

OPEN HEARING: SECURITY CLEARANCE REFORM

HEARING
BEFORE THE
SELECT COMMITTEE ON INTELLIGENCE
OF THE
UNITED STATES SENATE
ONE HUNDRED FIFTEENTH CONGRESS
SECOND SESSION

WEDNESDAY, MARCH 7, 2018

Printed for the use of the Select Committee on Intelligence



Available via the World Wide Web: <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

28-948 PDF

WASHINGTON : 2018

SELECT COMMITTEE ON INTELLIGENCE

[Established by S. Res. 400, 94th Cong., 2d Sess.]

RICHARD BURR, North Carolina, *Chairman*

MARK R. WARNER, Virginia, *Vice Chairman*

JAMES E. RISCH, Idaho

MARCO RUBIO, Florida

SUSAN COLLINS, Maine

ROY BLUNT, Missouri

JAMES LANKFORD, Oklahoma

TOM COTTON, Arkansas

JOHN CORNYN, Texas

DIANNE FEINSTEIN, California

RON WYDEN, Oregon

MARTIN HEINRICH, New Mexico

ANGUS KING, Maine

JOE MANCHIN III, West Virginia

KAMALA HARRIS, California

MITCH McCONNELL, Kentucky, *Ex Officio*

CHUCK SCHUMER, New York, *Ex Officio*

JOHN McCain, Arizona, *Ex Officio*

JACK REED, Rhode Island, *Ex Officio*

CHRIS JOYNER, *Staff Director*

MICHAEL CASEY, *Minority Staff Director*

KELSEY STROUD BAILEY, *Chief Clerk*

CONTENTS

MARCH 7, 2018

OPENING STATEMENTS

Burr, Hon. Richard, Chairman, a U.S. Senator from North Carolina	1
Warner, Hon. Mark R., Vice Chairman, a U.S. Senator from Virginia	2

WITNESSES

Panel 1

Farrell, Brenda, Director, DOD Strategic Human Capital Management, Government Accountability Office	4
Prepared statement	6
Phillips, Kevin, President and Chief Executive Officer, Mantech International Corporation	23
Prepared statement	25
Chappell, Jane, Vice President for Global Intelligence Solutions, Raytheon Corporation	32
Prepared statement	34
Berteau, David, President and Chief Executive Officer, Professional Services Council	44
Prepared statement	46

Panel 2

Dunbar, Brian, Assistant Director, Special Security Directorate, National Counter-Intelligence and Security Center, Office of the Director of National Intelligence	76
Prepared statement	79
Phalen, Jr., Charles S., Director, National Background Investigations Bureau, U.S. Office of Personnel Management	83
Prepared statement	85
Reid, Garry P., Director for Defense Intelligence (Intelligence and Security), Department of Defense	90
Prepared statement	93
Payne, Daniel E., Director, Defense Security Service, Department of Defense ..	97
Prepared statement	99

SUPPLEMENTAL MATERIAL

Responses to Questions for the Record by:	
Ms. Farrell	118
Mr. Phillips	121
Mr. Phalen	124
Mr. Dunbar	131
Mr. Reid and Mr. Payne	142

OPEN HEARING: SECURITY CLEARANCE REFORM

WEDNESDAY, MARCH 7, 2018

U.S. SENATE,
SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The Committee met, pursuant to notice, at 9:35 a.m. in Room SD-106, Dirksen Senate Office Building, Hon. Richard Burr (Chairman of the Committee) presiding.

Present: Senators Burr, Warner, Risch, Rubio, Collins, Blunt, Lankford, Cotton, Cornyn, Feinstein, Wyden, Heinrich, King, Manchin, Harris, and Reed.

OPENING STATEMENT OF HON. RICHARD BURR, CHAIRMAN, A U.S. SENATOR FROM NORTH CAROLINA

Chairman BURR. Good morning. I'd like to thank our witnesses for appearing today to discuss our government's security clearance process and potential areas of reform. The intelligence community, Department of Defense, and defense industrial base trust cleared personnel with our Nation's most sensitive projects and most important secrets. Ensuring a modern, efficient, and secure clearance process is paramount and necessary to maintain our national security.

The committee will first hear from industry representatives on their perspective on the process and how it affects their ability to support the U.S. Government. Our first panel includes: Mr. Kevin Phillips, President and CEO of ManTech; Ms. Jane Chappell, Vice President of Intelligence, Information, and Services at Raytheon; Mr. David Berteau, President of the Professional Services Council; and Ms. Brenda Farrell from the Government Accountability Office. Welcome to all of you. We appreciate your willingness to appear and, more importantly, thank you for the thousands of employees you represent, who work every day to support the whole of the U.S. Government. Many of our Nation's most sensitive programs and operations would not be possible without your work.

I look forward to hearing from you on how your respective companies view the security clearance process and how it affects your operations, your hiring, your retention, and your competitiveness. I also hope you've come today prepared with ideas for reform where necessary.

Our second panel will include representatives from the Executive Branch: Mr. Charlie Phalen, the Director of the National Background Investigation Bureau; Mr. Brian Dunbar, Assistant Director of National Counterintelligence and Security Center at the ODNI;

Mr. Garry Reid, Director for Security and Intelligence at the Office of the Under Secretary of Defense for Intelligence; and Mr. Dan Payne, Director of Defense Security Service at the Department of Defense. They'll provide the government's perspective on this issue and will update us on their efforts to improve the efficiency and effectiveness of the current system.

The purpose of this hearing is to explore the process for granting Secret and Top Secret clearances to both government and industry personnel, and to consider potential better ways forward. The government's approach to issuing national security clearances is largely unchanged since it was established in 1947, and the net result is a growing backlog of investigations, which now reaches 547,000, and inefficiencies that could result in our missing information necessary to thwart insider threats or workplace violence.

We should also consider new technologies that could increase the efficiency and effectiveness of our vetting process while also providing greater real-time situational awareness of potential threats to sensitive information. Furthermore, the system of reciprocity, whereby a clearance granted by one agency is also recognized by another, simply does not work.

We would all agree that the clearance process should be demanding on candidates and should effectively uncover potential issues before one is granted access to sensitive information. But clearly, the current system is not optimal and we must do better. I'm hopeful that today's discussion will have some good ideas and strategies that we can put into action to reform the process.

Again, I want to thank each of our witnesses for your testimony today, and I will now turn to the Vice Chairman for any comments he might have.

**OPENING STATEMENT OF HON. MARK R. WARNER, VICE
CHAIRMAN, A U.S. SENATOR FROM VIRGINIA**

Vice Chairman WARNER. Thank you, Mr. Chairman, and welcome to our witnesses. I want to first thank the Chairman for holding this hearing, particularly in an unclassified setting.

I believe that the way our government protects our secrets is a critical area for oversight of this committee. As the Chairman has already mentioned, in many ways the system that is in place, which was born in 1947—and I remind everybody, that's when classified cables were sent by typewriter and telex—really hasn't changed very much.

I believe that the clearance process today is a duplicative, manually intensive process. It relies on shoe leather field investigations that would be familiar to fans of spy films. It was built for a time when there was a small industry component and government workers stayed in their agency for their entire career. The principal risk was that someone would share pages from classified reports with an identifiable foreign adversary.

Today in many ways we worry more about insider threats, someone who can remove an external hard drive and provide petabytes of data online to an adversary or, for that matter, to a global audience. And industry—and much of that industry I'm proud to have in my State. And industry is a much larger partner. Workers are highly mobile across careers, sectors, and location. Technologies

such as big data and AI can help assess people's trustworthiness in a far more efficient and dynamic way. But we've not taken advantage of these advances.

Just last month, at an open hearing the Director of National intelligence, Director Coats, said that our security clearance process is, in his words, "broken and needs to be reformed." In January of this year—and I again appreciate the GAO witness today—placed the security clearance process on its, quote, "high-risk list" of areas that the government needs broad-based transformation or reforms.

The problems with our security clearance process are clear. The investigation inventory has more than doubled in the last three years, with, as the Chairman has mentioned, 700,000 people currently waiting on a background check. Despite recent headlines, the overwhelming majority of those waiting don't have unusually complex backgrounds or finances to untangle. Nevertheless, the cost to run a background check have nearly doubled. Timelines to process clearance are far in excess of standards set in law.

These failures in our security clearance process impact individual individuals, companies, government agencies, and even our own military's readiness. Again, as I mentioned, in the Commonwealth of Virginia I hear again and again from contractors, particularly from cutting-edge technology companies, and government agencies that they cannot hire the people they need in a timely manner. I hear from individuals who must wait for months and sometimes even a year to start jobs that they were hired for. And I've heard from a lot of folks who ultimately had to take other jobs because the process took too long and they couldn't afford to wait.

To compete globally, economically, and militarily, the status quo of continued delays and convoluted systems cannot continue. No doubt we face real threats to our security that we have to address. Insider threats like Ed Snowden and Harold Martin compromised vast amounts of sensitive data. And obviously the tragedy of the shootings at Washington Naval Yard and Fort Hood took innocent lives. The impacts of these lapses on national security are too big to think that incremental reforms will suffice.

Again referring back to Dan Coats's testimony, we need a revolution to our system. I believe we can assess the trustworthiness of our cleared workforce in a dramatically faster and more effective manner than we do today.

We have two great panels here that will help us, both from the government's perspective and from our national security partners in the private sector. I'd like again to thank you all for appearing. I hope that at our next meeting—and I hope some are listening downtown—that the OMB, which chairs the inter-agency efforts to address clearances, which declined to appear before us today, will actually participate in this process.

I want to be a partner in rethinking our entire security clearance architecture. I want to work with you to devise a model that reflects a dynamic workforce and embraces the needs of both our government and industry partners.

Thank you, Mr. Chairman. I look forward to this hearing.

Chairman BARR. I thank the Vice Chairman.

To members, when we have finished receiving testimony I'll recognize members based upon seniority for up to five minutes.

With that, Ms. Farrell, I understand you're going to go first, and then we'll work right down to your left, my right, all the way down the line. The floor is yours.

STATEMENT OF BRENDA FARRELL, DIRECTOR, DOD STRATEGIC HUMAN CAPITAL MANAGEMENT, GOVERNMENT ACCOUNTABILITY OFFICE

Ms. FARRELL. Thank you very much, Mr. Chairman. Chairman Burr, Vice Chairman Warner, and members of the committee: Thank you for the opportunity to be here today to discuss our recent work on the serious challenges associated with the personnel security clearance process. We designated the government-wide security clearance process as a high-risk area in January 2018 because it represents a significant management risk. A high-quality security clearance process is necessary to minimize the risk of unauthorized disclosures of classified information and to help ensure that information about individuals with criminal histories or other questionable behavior is identified and assessed.

My written statement today summarizes some of the findings in our reports issued in November and December 2017 on this topic. Now I will briefly discuss my written statement that is provided in three parts.

First, we found that the Executive Branch agencies have made progress reforming the clearance process, but key longstanding initiatives remain incomplete. For example, agencies still face challenges in implementing aspects of the 2012 Federal Investigative Standards that are criteria for conducting background investigations and in fully implementing a continuous evaluation program for clearance holders. Efforts to implement such a program go back ten years.

We found that, while the ODNI has taken an initial step to implement continuous evaluation in a phased approach, it had not determined what the future phases will consist of or occur. We recommended that the DNI develop an implementation plan.

Also, while agencies have taken steps to establish government-wide performance measures for the quality of investigations, the original milestone for completion was missed in fiscal year 2010. No revised milestone currently has been set for their completion. We recommended that the DNI establish a milestone for completion of such measures.

Second, we found that the number of agencies meeting timeliness objectives for initial Secret and Top Secret clearances, as well as periodic reinvestigations, decreased from fiscal years 2012 through 2016. For example, while 73 percent of agencies did not meet timeliness objectives for initial clearances for most of fiscal year 2012, 98 percent of agencies did not meet these objectives in fiscal year 2016. Lack of timely processing for clearances has contributed to a significant backlog of background investigations at the agency that is currently responsible for conducting most of the government's background investigations, that is the National Background Investigations Bureau. The Bureau's documentation shows that the backlog of pending investigations increased from about 190,000 in August 2014 to more than 710,000 as of February 2018. We found that the Bureau did not have a plan for reducing the backlog.

Finally, we found that potential effects of continuous evaluation on agencies are unknown because the future phases of the program and the effect on agency resources have not yet been determined. Agencies have identified increased resources as a risk to the program. For example, DOD officials told us that, with workload and funding issues, they see no alternative but to replace periodic reinvestigations for certain clearance holders with continuous evaluation. DOD believes that more frequent reinvestigations for certain clearance holders could cost \$1.8 billion for fiscal year 2018 through 2022. However, the DNI's recently issued directive for continuous evaluation clarified that continuous evaluation is intended to supplement, but not replace, periodic reinvestigations.

In summary, Mr. Chairman, several agencies have key roles and responsibilities in the multi-phase clearance process, including ODNI, OMB, DOD, and OPM. Also, the top leadership from these agencies comprises the Performance Accountability Council that is responsible for driving implementation of and overseeing the reform efforts government-wide.

We look forward to working with them to discuss our plans for assessing their progress in addressing this high-risk area.

Now is the time for strong top leadership to focus on implementing GAO's recommended actions to complete the reform efforts, improve timeliness, and reduce the backlog. Failure to do so increases the risk of damaging unauthorized disclosures of classified information.

Mr. Chairman, that concludes my remarks.

[The prepared statement of Ms. Farrell follows:]



United States Government Accountability Office

Testimony
Before the Select Committee on
Intelligence, U.S. Senate

For Release on Delivery
Expected at 9:30 am ET
Wednesday, March 7, 2018

PERSONNEL SECURITY CLEARANCES

Additional Actions Needed to Implement Key Reforms and Improve Timely Processing of Investigations

Statement of Brenda S. Farrell, Director, Defense
Capabilities and Management

GAO Highlights

Highlights of GAO-18-431T, a testimony before the Select Committee on Intelligence, U.S. Senate

Why GAO Did This Study

The government-wide personnel security clearance process was designated as a high-risk area in January 2018 because it represents one of the highest management risks in government.

This testimony focuses on, among other things, the extent to which executive branch agencies (1) made progress reforming the security clearance process, and (2) are meeting timeliness objectives and reducing NBIB's investigative backlog.

GAO's statement is based on information from public versions of its reports issued in November 2017 on continuous evaluation of clearance holders and in December 2017 on clearance reform efforts. Information that ODN and OPM deemed sensitive was omitted. For those reports, GAO reviewed Executive Orders and PAC strategic documents; obtained data from the Office of the Director of National Intelligence (ODNI) on the timeliness of initial clearances and periodic reinvestigations; and interviewed officials from ODNI, NBIB, and other agencies.

What GAO Recommends

In November 2017 and December 2017, GAO made 12 recommendations to the DNI and the Director of NBIB, including setting a milestone for establishing measures for investigation quality, developing a plan to meet background investigation timeliness objectives, and developing a plan for reducing the backlog. NBIB concurred with the recommendations. The DNI concurred with some, but not all, of GAO's recommendations. GAO continues to believe they are valid.

View GAO-18-431T. For more information, contact Brenda S. Farrell at (202) 512-3604 or farrellb@gao.gov.

March 2018

PERSONNEL SECURITY CLEARANCES

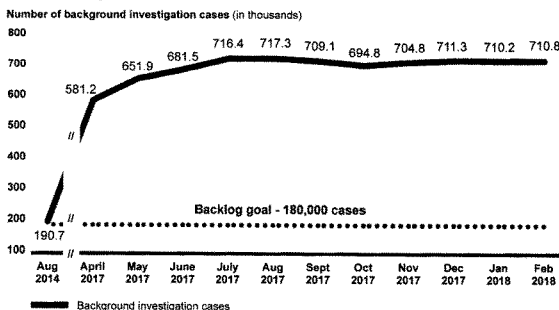
Additional Actions Needed to Implement Key Reforms and Improve Timely Processing of Investigations

What GAO Found

Executive branch agencies have made progress reforming the security clearance process, but long-standing key initiatives remain incomplete. Progress includes the issuance of federal adjudicative guidelines and updated strategic documents to help sustain the reform effort. However, agencies still face challenges in implementing aspects of the 2012 Federal Investigative Standards—criteria for conducting background investigations—and in implementing a continuous evaluation program. In addition, while agencies have taken steps to establish government-wide performance measures for the quality of investigations, neither the Director of National Intelligence (DNI) nor the interagency Security, Suitability, and Credentialing Performance Accountability Council (PAC) have set a milestone for completing their establishment.

GAO's analysis of timeliness data for specific executive branch agencies showed that the number of agencies meeting investigation and adjudication timeliness objectives for initial secret and top secret security clearances and periodic reinvestigations decreased from fiscal years 2012 through 2016. For example, while 73 percent of agencies did not meet timeliness objectives for initial clearances for three of four quarters in fiscal year 2012, 98 percent of agencies did not meet these objectives in fiscal year 2016. The DNI has not developed a government-wide plan, including goals and milestones, to help agencies improve timeliness. Agencies' challenges in meeting timeliness objectives have contributed to a significant backlog of background investigations at the agency that is responsible for conducting the majority of investigations, the National Background Investigations Bureau (NBIB). NBIB documentation shows that the backlog of pending investigations increased from about 190,000 in August 2014 to more than 710,000 as of February 2018, as shown below. NBIB leadership has not developed a plan to reduce the backlog to a manageable level.

National Background Investigations Bureau's Backlog of Background Investigations, August 2014 to February 2018



Source: GAO analysis of National Background Investigations Bureau information. | GAO-18-431T

Chairman Burr, Vice Chairman Warner, and Members of the Committee:

Thank you for the opportunity to be here today to discuss personnel security clearance reforms. The government-wide personnel security clearance process was designated as a high-risk area in January 2018 because it represents one of the highest management risks in government. A high-quality personnel security process is necessary to minimize the risks of unauthorized disclosures of classified information and to help ensure that information about individuals with criminal histories or other questionable behavior is identified and assessed. In 2014, emphasis on security clearance reform was renewed following high-profile events such as the September 2013 shooting at the Washington Navy Yard by an individual who had both access to the facility and a security clearance. In November and December 2017, we reported, among other things, that the executive branch faces challenges completing key reform efforts, processing security clearances, and reducing a significant backlog in background investigations.¹

In January 2018, in light of the serious challenges facing the interagency Security, Suitability, and Credentialing Performance Accountability Council (PAC), the entity responsible for driving the implementation of and overseeing the reform efforts, we placed the government-wide personnel security clearance process on GAO's High-Risk List. We made this designation out-of-cycle because it was important to call attention to these challenges now.² My testimony today focuses on three of the key challenges that led to the high-risk designation, including: (1) the extent to which executive branch agencies made progress reforming the security clearance process; (2) the extent to which executive branch agencies are meeting timeliness objectives and reducing the National Background Investigations Bureau's (NBIB) investigative backlog; and (3) the potential effects of continuous evaluation—a process to review the background of clearance holders and individuals in sensitive positions at any time during the eligibility period—on executive branch agencies.

¹GAO, *Personnel Security Clearances: Plans Needed to Fully Implement and Oversee Continuous Evaluation of Clearance Holders*, GAO-18-117 (Washington, D.C.: Nov. 21, 2017) and *Personnel Security Clearances: Additional Actions Needed to Ensure Quality, Address Timeliness, and Reduce Investigation Backlog*, GAO-18-29 (Washington, D.C.: Dec. 12, 2017).

²GAO updates the High-Risk List every 2 years near the start of each new Congress to help set oversight agendas. Our next update will be in 2019.

My testimony is primarily based on our November and December reports on these topics.³ For those reports, we reviewed relevant statutes, Executive Orders, and PAC strategic documents; obtained data from the Office of the Director of National Intelligence (ODNI) on the timeliness of initial personnel security clearances and periodic reinvestigations for fiscal years 2012 through 2016 for specific executive branch agencies; and interviewed PAC, Office of Personnel Management (OPM), NBIB, ODNI, and Department of Defense (DOD) officials.⁴ Our November and December 2017 reports include a detailed explanation of our scope and methodology. In these reports, we made 12 recommendations to the Director of National Intelligence and the Director of NBIB, some of which I will discuss today. NBIB concurred with the recommendations. The Director of National Intelligence concurred with some, but not all, of our recommendations. We continue to believe these recommendations are valid. Information that ODNI and OPM deemed sensitive was omitted. We conducted the work on which this statement is based in accordance with generally accepted government auditing standards.

³GAO-18-117 and GAO-18-29.

⁴For this statement, we followed up with OMB and NBIB officials to obtain updated backlog data and other key performance indicators.

**Executive Branch
Agencies Have Made
Progress Reforming
the Security
Clearance Process,
but Long-Standing
Key Initiatives
Remain Incomplete**

**The PAC Has Made
Progress Reforming the
Personnel Security
Clearance Process**

The PAC has made progress in reforming the personnel security clearance process and implementing various security clearance reform initiatives. For example, the PAC has taken action on 73 percent of the recommendations of a February 2014 review conducted in the wake of the Washington Navy Yard shooting.⁵ Actions in response to these recommendations included ODNI and OPM jointly issuing Quality Assessment Standards in January 2015, which establish federal guidelines for assessing the quality of investigations. Additionally, ODNI developed the Quality Assessment Reporting Tool, through which agencies will report on the completeness of investigations.

Similarly, the PAC reported quarterly on the status and progress of key initiatives, as part of the Insider Threat and Security Clearance Reform cross-agency priority goal.⁶ This reporting included the milestone due date and status for each initiative.⁷ According to PAC Program Management Office officials, although the data are no longer publicly

⁵Office of Management and Budget, *February 2014 Suitability and security Processes Review—Report to the President* (February 2014).

⁶The PAC reports began in the second quarter of fiscal year 2014 and continued through the end of fiscal year 2016.

⁷The PAC has not reported publicly on the status of the reform effort since the fourth quarter of fiscal year 2016 as the content on performance.gov, the vehicle through which the PAC previously issued its quarterly updates, was being reviewed based on the presidential transition. As of August 2017, it was undergoing revision as agencies developed updated goals and objectives for release in February 2018 with the President's budget submission to Congress. As of February 2018, the PAC is not reporting on the status of the reform effort via performance.gov.

reported, they have continued to track the status of these milestones internally, and identified almost half of the initiatives—16 of 33—as complete as of the third quarter of fiscal year 2017.

Additionally, the PAC has issued three documents that serve as its updated strategic framework for the next 5 years. In July 2016, it issued its Strategic Intent for Fiscal Years 2017 through 2021, which identifies the overall vision, goals, and 5-year business direction to achieve an entrusted workforce. In October 2016, it issued an updated PAC Enterprise IT Strategy, which provides the technical direction to provide mission-capable and secure security, suitability, and credentialing IT systems. According to PAC program management officials, the third document—PAC Strategic Intent and Enterprise IT Strategy Implementation Plan—was distributed to executive branch agencies in February 2017.⁸ Further, we reported in December 2017 that PAC members noted additional progress in reforming the personnel security clearance process, such as the development of Security Executive Agent Directives, the identification of executive branch—wide IT shared service capabilities, and the standardization of adjudicative criteria.

**Long-Standing Key
Reform Initiatives Remain
Incomplete**

Although the PAC has reformed many parts of the personnel security clearance process, the implementation of certain key initiatives, including the full implementation of the 2012 Federal Investigative Standards and the development of government-wide performance measures for the quality of investigations, remain incomplete. The Federal Investigative Standards outline criteria for conducting background investigations to determine eligibility for a security clearance, and are intended to ensure cost-effective, timely, and efficient protection of national interests and to facilitate reciprocal recognition of the resulting investigations.⁹

However, the standards also changed the frequency of periodic reinvestigations for certain clearance holders and include continuous evaluation as a new requirement for certain clearance holders.

⁸Security, Suitability, and Credentialing Performance Accountability Council, *Strategic Intent Fiscal Years 2017-2021* (July 2016); and *Enterprise Information Technology Strategy Fiscal Years 2017-2021* (October 2016).

⁹In addition to eligibility for access to classified information, the standards cover investigations to determine eligibility for logical and physical access, suitability for government employment, eligibility to hold a sensitive position, and fitness to perform work for or on behalf of the government as a contractor employee.

Continuous evaluation is a key executive branch initiative to more frequently identify and assess security-relevant information, such as criminal activity, between periodic reinvestigations. Continuous evaluation is a process to review the background of an individual who has been determined to be eligible for access to classified information or to hold a sensitive position at any time during the period of eligibility. Continuous evaluation involves automated record checks conducted on a more frequent basis, whereas periodic reinvestigations are conducted less frequently and may include, among other things, subject and reference interviews. The types of records checked as part of continuous evaluation are the same as those checked for other personnel security purposes. Security-relevant information discovered in the course of continuous evaluation is to be investigated and adjudicated under the existing standards.

Efforts to implement an executive branch continuous evaluation program go back to at least 2008, with a milestone for full implementation by the fourth quarter of fiscal year 2010. In November 2017, we reported that while ODNI has taken an initial step to implement continuous evaluation in a phased approach across the executive branch, it had not determined when the future phases of implementation will occur. We recommended, among other things, that the Director of National Intelligence develop an implementation plan. ODNI generally concurred with that recommendation.¹⁰

Regarding government-wide measures for the quality of background investigations, as noted earlier, ODNI and OPM issued the Quality Assessment Standards and ODNI issued the Quality Assessment Reporting Tool. The Quality Assessment Standards established federal guidelines for assessing the quality of investigations. The Quality Assessment Reporting Tool is a tool through which agencies will report on the completeness of investigations. However, measures for quality have not been developed, and it is unclear when this key effort will be completed. The original milestone for completing government-wide measures was fiscal year 2010, and no new milestone has been established. In our December 2017 report, we recommended that the Director of National Intelligence, in his capacity as the Security Executive Agent, and in coordination with the other PAC Principals, establish a milestone for the completion of government-wide performance measures

¹⁰GAO-18-117.

for the quality of investigations. ODNI disagreed with the recommendation, stating that it is premature to establish such a milestone and that it will do so once the Quality Assessment Reporting Tool metrics have been fully analyzed. We continue to believe that setting a milestone, which takes into consideration the amount of time needed to analyze Quality Assessment Reporting Tool data, will help to ensure that the analysis of the data is completed, initial performance measures are developed, and agencies have a greater understanding of what they are being measured against.

**Agencies Meeting
Timeliness Objectives
for Clearances
Decreased, and a
Government-Wide
Approach Has Not
Been Developed to
Improve Timeliness or
Address the Backlog**

Our analysis of government-wide and agency-specific data shows a decline in the number of executive branch agencies meeting the timeliness objectives for processing clearances. While ODNI has taken steps to address timeliness challenges, it has not developed a government-wide approach to help agencies improve the timeliness of initial personnel security clearances. Additionally, the backlog of background investigations conducted by NBIB—the primary entity responsible for conducting background investigations—has steadily increased since 2014 and as of February 2018 exceeds 710,000 cases. NBIB personnel are attempting to decrease the backlog by making the background investigation process more effective and efficient and increasing investigator capacity. However, NBIB faces challenges in developing a plan to reduce the size of the investigation backlog to a manageable level.

**Agencies Meeting
Timeliness Objectives
Decreased**

Our analysis showed that the percentage of executive branch agencies meeting timeliness objectives for investigations and adjudications decreased from fiscal years 2012 through 2016. The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)¹¹ established an objective for each authorized adjudicative agency to make a determination on at least 90 percent of all applications for a personnel security clearance within an average of 60 days after the date of receipt of the completed application by an authorized investigative agency. The objective includes no longer than 40 days to complete the investigative phase and 20 days

¹¹Pub. L. No. 108-458, § 3001 (2004) (codified in relevant part at 50 U.S.C. § 3341). While IRTPA was a far-reaching act with many broad implications, our references to it throughout this statement pertain solely to section 3001, unless otherwise specified.

to complete the adjudicative phase.¹² In assessing timeliness under these objectives, executive branch agencies exclude the slowest 10 percent and report on the average of the remaining 90 percent (referred to as the fastest 90 percent).¹³

As part of the Insider Threat and Security Clearance Reform cross-agency priority goal, the PAC reported quarterly on the average number of days to initiate, investigate, adjudicate, and complete the end-to-end process for initial secret and initial top secret cases and periodic reinvestigations for the executive branch as a whole from fiscal year 2014 through 2016.¹⁴ For fiscal year 2016, the PAC reported that the government-wide average for executive branch agencies¹⁵

- did not meet the 40-day investigation objective for the fastest 90 percent of initial secret clearances for any quarter; the averages ranged from 92 days to 135 days;
- did not meet ODNI's revised investigation objective for the fastest 90 percent of initial top secret clearances for any quarter; the averages ranged from 168 days to 208 days;
- did not meet the goal of conducting the investigative portion of periodic reinvestigations within 150 days for the fastest 90 percent of cases for any quarter; the averages ranged from 175 days to 192 days; and

¹²Specifically, IRTPA required the development of a plan to reduce the length of the personnel security clearance process that included, to the extent practical, the above time frames. See Pub. L. No. 108-458, § 3001(g) (2004) (codified as amended at 50 U.S.C. § 3341(g)).

¹³In 2012, ODNI, in coordination with interagency participation, modified the timeliness goals for certain background investigations.

¹⁴However, the timeliness goals on which the PAC currently reports for periodic reinvestigations are the same as those identified in a 2008 report that included government-wide processing goals for security clearances for calendar year 2008. The calendar year 2008 government-wide goal for the fastest 90 percent of periodic reinvestigations is the same as the goal currently in place: 195 days to complete the end-to-end processing of the periodic reinvestigations. Joint Security and Suitability Reform Team, *Security and Suitability Process Reform* (December 2008).

¹⁵Of the agencies we reviewed, we found that agencies that use NBIB as their investigative service provider and agencies with delegated authority to conduct their own investigations both experienced challenges in meeting established timeliness goals. Data provided by ODNI identified the agencies with delegated authority to conduct their own investigations.

-
- did not meet the goal of completing periodic reinvestigations—the end-to-end goal—within 195 days for any quarter of fiscal year 2016; the averages ranged from 209 days to 227 days.

Our analysis of timeliness data for specific executive branch agencies showed that the percentage of agencies meeting established investigation and adjudication timeliness objectives for initial secret and top secret personnel security clearances and periodic reinvestigations decreased from fiscal year 2012 through 2016. We found that agencies with delegated authority to conduct their own investigations and those that use NBIB as their investigative provider experienced challenges in meeting established investigative timeliness objectives. Specifically, in fiscal year 2012, we found that

- 73 percent of the agencies, for which we obtained data, did not meet investigation and adjudication objectives for at least three of four quarters for initial secret clearances,
- 41 percent did not meet those objectives for initial top secret clearances, and
- 16 percent did not meet the investigative goal for at least three of four quarters for the fastest 90 percent of periodic reinvestigations.

By fiscal year 2016, the percentage of agencies that did not meet these same objectives had increased to 98 percent, 90 percent, and 82 percent, respectively.

Furthermore, ODNi requests individual corrective action plans from agencies not meeting security clearance timeliness objectives. However, the executive branch has not developed a government-wide plan, with goals and interim milestones, to meet established timeliness objectives for initial security clearances that takes into consideration increased investigative requirements and other stated challenges. In our December 2017 report, we recommended that the Director of National Intelligence, as Security Executive Agent, develop a government-wide plan, including goals and interim milestones, to meet timeliness objectives for initial personnel security clearance investigations and adjudications. Although the DNI did not specifically comment on this recommendation, we continue to believe a government-wide plan would better position ODNi to identify and address any systemic government-wide issues.

We also recommended that the Director of National Intelligence conduct an evidence-based review of the investigation and adjudication timeliness objectives and take action to adjust the objectives if appropriate. He did

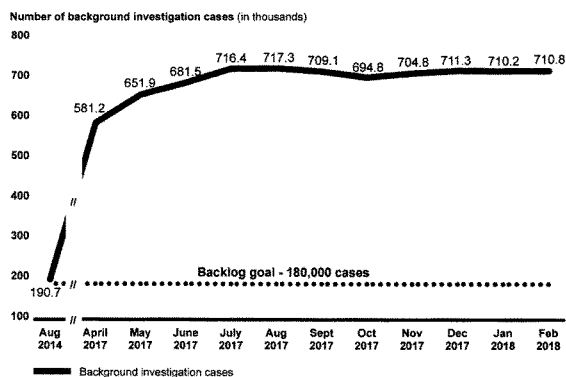
not agree with this recommendation and stated that it is premature to revise the existing timeliness goals until NBIB's backlog is resolved. We continue to believe that our recommendation to conduct an evidence-based review, using relevant data, is valid. As we noted in our report, even agencies with delegated authority to conduct their own investigations are experiencing challenges meeting established timeliness objectives. We also noted that ODNI has not comprehensively revisited the investigation or adjudication timeliness objectives for initial security stemming from the implementation of the 2012 Federal Investigative Standards.

Backlog of Background Investigations Has Steadily Increased since 2014

The executive branch's challenges in meeting investigation timeliness objectives for initial personnel security clearances and periodic reinvestigations have contributed to a significant backlog of background investigations at the primary entity responsible for conducting background investigations, NBIB. NBIB personnel are attempting to decrease the backlog by making the background investigation process more effective and efficient. To do so, NBIB conducted a business process reengineering effort that was intended to identify challenges in the process and their root causes. Specifically, NBIB officials cited efforts that have been implemented to reduce the number of personnel hours necessary to complete an investigation, such as centralizing interviews and using video-teleconferencing for overseas investigations (to decrease travel time), automated record checks, and focused writing (to make reports more succinct and less time-consuming to prepare). However, NBIB has not identified how the implementation of the business process reengineering effort will affect the backlog or the need for additional investigators in the future. In December 2017, we recommended that the Director of NBIB develop a plan, including goals and milestones, that includes a determination of the effect of the business process reengineering efforts on reducing the backlog to a "healthy" inventory of work, representing approximately 6 weeks of work. NBIB concurred with this recommendation.

NBIB documentation shows that the backlog of pending investigations increased from about 190,000 in August 2014 to more than 710,000 as of February 2018, as shown in figure 1. NBIB's Key Performance Indicators report states that a "healthy" inventory of work is around 180,000 pending investigations, representing approximately 6 weeks of work, and would allow NBIB to meet timeliness objectives.

Figure 1: National Background Investigations Bureau's Backlog of Background Investigations, August 2014 to February 2018



Source: GAO analysis of National Background Investigations Bureau information. | GAO-18-431T

ODNI officials stated that several significant events contributed to agency challenges in meeting timeliness objectives over the past 5 fiscal years, including a government shutdown, the 2015 OPM data breach, a loss of OPM contractor support, and OPM's review of the security of its IT systems, which resulted in the temporary suspension of the web-based platform used to complete and submit background investigation forms. In addition, executive branch agencies noted the increased investigative requirements stemming from the 2012 Federal Investigative Standards as a further challenge to meeting established timeliness objectives in the future.

While NBIB has taken steps to increase its capacity to conduct background investigations by increasing its own investigator staff as well as awarding new contracts, in our December 2017 report we noted that NBIB officials have assessed four scenarios, from the status quo—assuming no additional contractor or federal investigator hires—to an

aggressive contractor staffing plan beyond January 2018.¹⁶ The two scenarios that NBIB identified as most feasible would not result in a "healthy" inventory level until fiscal year 2022 at the earliest. In our December 2017 report, we recommended that the Director of NBIB establish goals for increasing total investigator capacity—federal employees and contractor personnel—in accordance with the plan for reducing the backlog of investigations, as noted above. NBIB concurred with this recommendation.

The Potential Effects of Continuous Evaluation on Executive Branch Agencies Are Unknown

We reported in November 2017 that the potential effects of continuous evaluation on executive branch agencies are unknown because future phases of the program and the effect on agency resources have not yet been determined.¹⁷ ODNI has not yet determined key aspects of its continuous evaluation program, which has limited the ability of executive branch agencies to plan for implementation in accordance with ODNI's phased approach. For example, while ODNI has initiated the first phase of continuous evaluation in coordination with implementing executive branch agencies, it has not yet determined what the future phases of implementation will entail, or when they will occur. As we reported in November 2017, the uncertainty regarding the requirements and time frames for the future phases of the program has affected the ability of executive branch agencies to plan to implement continuous evaluation and estimate the associated costs.

Although executive branch agencies have identified increased resources as a risk associated with implementing continuous evaluation, and ODNI has acknowledged that risk, ODNI, in coordination with the PAC, has not assessed the potential effects of continuous evaluation on an agency's resources. Further, ODNI has not developed a plan, in consultation with implementing agencies, to address such effects, including modifying the scope or frequency of periodic reinvestigations or replacing periodic reinvestigations for certain clearance holders.

Moreover, the potential effect of continuous evaluation on periodic reinvestigations is unknown. Executive branch agencies have expressed varying views about potential changes to the periodic reinvestigation model:

¹⁶GAO-18-29.

¹⁷GAO-18-117.

-
- DOD officials stated that with workload and funding issues, they see no alternative but to replace periodic reinvestigations for certain clearance holders with continuous evaluation, as the record checks conducted are the same for both processes.
 - State Department officials expressed concerns that relevant information, such as state and local law-enforcement records that are not yet automated, would be missed if it did not conduct periodic reinvestigations.
 - State Department officials, along with officials from the Departments of Justice and Homeland Security, stated it may be possible to change the frequency or scope of periodic reinvestigations at some point in the future.
 - The Security Executive Agent Directive for continuous evaluation, issued since our report, clarified that continuous evaluation is intended to supplement but not replace periodic reinvestigations.

In our November 2017 report, ODNI officials stated that ODNI is not opposed to further improving the security clearance process, and that once continuous evaluation is operational, it plans to determine the efficiencies and mitigation of risks associated with the approach. Specifically, these officials stated that once continuous evaluation is further implemented and ODNI has gathered sufficient data—which they estimated would take about a year from May 2017—they can perform analysis and research to determine whether any changes are needed to the periodic reinvestigation model.

We recommended that the Director of National Intelligence assess the potential effects of continuous evaluation on agency resources and develop a plan, in consultation with implementing agencies, to address those effects, such as modifying the scope of periodic reinvestigations, changing the frequency of periodic reinvestigations, or replacing periodic reinvestigations for certain clearance holders. ODNI generally concurred with this recommendation.

Finally, the National Defense Authorization Act for Fiscal Year 2018, enacted in December 2017, will have a significant impact on the personnel security clearance process. Among other things, the act authorized DOD to conduct its own background investigations and

requires DOD to begin carrying out a related implementation plan by October 1, 2020.¹⁸ It also requires the Secretary of Defense, in consultation with the Director of OPM, to provide for a phased transition.¹⁹ These changes could potentially affect timeliness, the backlog, and other reform initiatives but the effect is unknown at this time. DOD's investigations represent the majority of the background investigations conducted by NBIB.

Chairman Burr, Vice Chairman Warner and Members of the committee, this concludes my prepared testimony. I look forward to answering any questions.

GAO Contact and Staff Acknowledgements

If you or your staff have any questions about this testimony, please contact Brenda S. Farrell at (202) 512-3604 or at farrellb@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this testimony. GAO staff who made key contributions to this testimony are Kimberly Seay (Assistant Director), James Krustapentus, Michael Shaughnessy, and John Van Schaik.

¹⁸See Pub. L. No. 115-91, § 925(a), (b) (2017). Section 925(b) requires DOD to begin carrying out the implementation plan developed in response to section 951(a)(1) of the National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328 (2016).

¹⁹§ 925(a)(2).

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<https://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <https://www.gao.gov> and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <https://www.gao.gov/fraudnet/fraudnet.htm>
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149, Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707, U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548



Please Print on Recycled Paper.

Chairman BURR. Thank you, Ms. Farrell.
Mr. Phillips, the floor is yours.

STATEMENT OF KEVIN PHILLIPS, PRESIDENT AND CHIEF EXECUTIVE OFFICER, MANTECH INTERNATIONAL CORPORATION

Mr. PHILLIPS. Mr. Chairman, Vice Chairman, and members of the committee: My name is Kevin Phillips. I'm the President and CEO of ManTech International. ManTech has 7,800 employees who support national security and homeland security. I appreciate the opportunity to participate in this industry panel and ask that my written statement be entered as part of the hearing record.

Senator Warner, including our initial outreach through NVTC, 15 companies and 6 industry associations have worked collectively over the last 6 to 9 months to increase the visibility and importance of this matter and to propose solutions to help improve the process. Put simply, the backlog of 700,000 security clearance cases is our industry's number one priority. Given the increasing challenges that we face in providing qualified, cleared talent to meet the mission demands, we consider it a national security issue and an all-of-government issue because it impacts every agency we support.

Some quick facts. Since 2014, the time it takes to obtain a clearance has more than doubled in our industry. The average time it takes to get a TS-SCI clearance, a Top Secret clearance, is over a year. The time it takes to get a Secret clearance is eight months. Top professionals are in high demand across the Nation. They do not have time to wait over a year to get a job. And increasingly, they are unwilling to deal with the uncertainty associated with this process.

As a result of this issue, the key support for weapons development, cyber security, analytics, maintenance and sustainment, space resilience support, as well as the use of transformational technologies across all of government, is being underserved. Since the end of 2014, we estimate that approximately 10,000 positions required from the contractor community in support of the intelligence community have gone unfilled due to these delays.

We offer the following recommendations to help improve the backlog: first, enable reciprocity; allow for crossover clearances to be done routinely and automatically. Today 23 different agencies provide different processes and standards in order to determine who is trustworthy and suitable to be employed within their agency. One universally accepted and enforced standard across all of government is needed.

Second, increase funding. The current backlog shows no signs of improvement. We need funding to increase processing capacity, to reduce the backlog we have today, while our government partners, who are working diligently to develop and implement a new system, work to develop the system of tomorrow.

Third, prioritize existing cases. The amount of backlog of 700,000 cases has not gone down. The timelines have not improved, and we may be at a point where we have to prioritize within that backlog the cases that have the greatest mission impact or that may have

the highest or pose the highest risks to national security based on the access to data.

Fourth, adopt continuous evaluation, adopt new systems that can be used across all of government, and establish a framework for which government and industry can better share information about individuals holding positions of public trust that is derogatory, so that we can better protect the Nation against threats from insiders.

Fifth, from a legislative standpoint we consider this a whole-of-government issue. Accordingly, we believe that a concerted focus from Congress is required and the oversight is needed. We support the reinstatement of the IRTPA timelines with incremental milestones. "IRTPA" is the Intelligence Reform and Terrorism Prevention Act.

Finally, we offer that mobility and portability for clearances among the contractor community are needed. We in industry fully understand the importance of a strong security clearance process. That said, slow security does not constitute good security. Time matters to mission.

The industry is committed to take the actions needed to hire trustworthy individuals and to help protect the Nation from outside threats. We appreciate the committee's leadership and the focus on this important matter. Thank you.

[The prepared statement of Mr. Phillips follows:]

**Statement of Kevin Phillips, CEO ManTech Inc.
Hearing on Security Reform
Senate Select Committee on Intelligence
7 March 2018**

Introduction

Mr. Chairman, Vice Chairman, and Members of the Committee. I am honored to present to you our industry and association partners' views on security clearance reform. I want to express appreciation for the Committee's leadership on this issue which recently led GAO to elevate this issue to its "High Risk" list. We also appreciate the very helpful legislation in Section 603 of your FY 2018 Intelligence Authorization bill.

I speak today not only for my company, ManTech, but am also reflecting the input of a group of 15 major professional services companies and six industry associations who support national and homeland security with whom I coordinated my testimony. I would like to address five areas:

- 1) Industry experience with the clearance backlog
- 2) The impact of the backlog on national security
- 3) Goals for reform
- 4) Views on government progress
- 5) Recommendations

Industry Experience with the Clearance Backlog

Since 2014, the time required for receiving security clearances has more than doubled. To put it in perspective, consider how much time this process consumed in 2017, the most recent year for which we in industry have data:

- ☐ In 2017, the average time to complete initial TS/SCI clearances was 400 days – with timelines ranging from 325 days to as many as 598 days.
- ☐ The average timeline for adjudicating a SECRET clearance was 231 days.
- ☐ Cross-over clearances (when a contractor moves from providing services at one agency to another) averaged 21 days and varied widely by agency – an average range of 12 days for the Intelligence Community to up to 97 days for the Department of Homeland Security.

While three weeks might not appear excessive to process cross-over clearances, any delay disrupts industry's support for the government mission. The problem is the process itself. As a point of reference, consider that 23 different agencies within the Federal Government possess delegated authority from the DNI to perform either background investigations or adjudications.

This increases the complexity and variation of practices for cross-over clearances and background investigation processing.

In addition to performing clearance determinations, many agencies apply additional, sometimes unique hiring standards referred to as “suitability” or “fitness.” In the services support industry we know from experience that agency-specific “suitability” or “fitness” requirements sometimes delay approval of cross-over clearances and create additional requirements in the contractor’s security clearance process. (“Suitability” standards apply to federal employees and “fitness” standards apply to contractors.) Yet agencies do not typically reveal to industry the specific standards associated with suitability or fitness that they apply. As the Suitability Executive Agent, OPM has responsibility for suitability, fitness policy and standards across the government. As the Security Executive Agent, the DNI has responsibility for policy and standards for security background investigations. Having two entities share policy-making responsibilities for trust functions across various government agencies adds to complexity and delays in agency execution.

The Impact of the Backlog on National Security

We believe that the current backlog of over 700,000 clearance cases constitutes a major national security issue — it is not a “back-office” administrative function. The slow pace of the security clearance process prevents us from recruiting and hiring the talented individuals critical to national security. Specific areas impacted include weapon systems, space missions and operations, cyber network operations and cyber security, cloud computing, data science and analytics, and hardware manufacturing. Nationwide, technology professionals are in high demand. They will not wait for a year or longer to obtain a clearance to begin the meaningful work which contributes to the innovations demanded by national security priorities.

This problem threatens the nation’s ability to achieve a top objective in the Pentagon’s recently-released National Defense Strategy: *“Establishing an unmatched twenty-first century National Security Innovation Base that effectively supports Department operations and sustains security and solvency.”* It also constrains our nation’s ability to lead in research, technology, invention, and innovation — integral components of the second Pillar of the President’s National Security Strategy.

The backlog impacts mission, efficiency and jobs. As a result of the security clearance delays from 2014-2017, we estimate that approximately 10,000 contract positions critical to the Intelligence Community remained unfilled. The inability of the government and industry to hire private sector talent has negatively affected the government’s ability to perform critical national security missions. These unfilled positions also represented roughly \$1.8 billion of lost services contract support for critical missions out of the \$71 billion annual intelligence budget—a direct result of the lack of cleared talent. Additionally, we estimate that due to the increased investigation backlog the vast majority of industry’s recruiting efforts for intelligence community positions in 2017 focused on personnel who already held a clearance. This means that Government and industry effort was directed toward reciprocity requests and periodic

reinvestigation submissions. The time and effort spent on lengthy reinvestigations significantly undercuts the ability to hire the new contractor talent necessary to support missions, such as cybersecurity and the introduction of new technologies and innovation. Moreover, the increasing gap between cleared contractor talent and mission needs drives up demand, and subsequently increases contractor salaries, thus increasing the cost the Government pays for classified services.

For all these reasons, reducing the 700,000 security clearance backlog is our industry's number one issue and is why we are working with the Federal Government to resolve this challenging problem.

Goals for Reform

We offer three simple but not easily achievable goals for government security clearance reform. They are that the:

- 1) Government should immediately implement an effective course of action to substantially reduce the backlog of security clearances to a healthier and more sustainable level (similar to those in 2014) in the next two years, and ultimately to the much lower levels implied by the ambitious timeline goals in IRTPA. Achieving these goals will allow us to more rapidly hire and retain the required, trusted workforce;
- 2) Government should reform clearance standards and cross-agency reciprocity practices which will substantially reduce the time to clear a contractor moving from one agency or job to another, thus improving the ability to place cleared talent on critical contracts;
- 3) Government and Industry should make available information to each other in a timely manner to improve our collective ability to detect and deter insider threats that may compromise classified information.

Views on Government Progress

To help advance these goals, our industry partners actively interact with our government customers at all levels, and (at their invitation) with the senior members of the interagency Performance Accountability Council (PAC) chaired by OMB. In addition to the OMB, PAC Principals include senior executives from the OPM, ODNI, and DoD.

Federal officials recognize the need to reduce the current clearance backlog and are working toward changes that will improve the process in the long term. We applaud the efforts by PAC Principals, NBIB, and DSS to implement business process improvements in tandem with investment plans for new IT systems. We believe that Congressional oversight can help keep this progress on track. We are also encouraged by preliminary government consideration of an information sharing program with Industry, as well as by the Government's intention to treat

contractors moving from one agency to another on par with government employees. Finally, we also believe that DoD's continuous evaluation (CE) pilot is an important step toward primary reliance on CE.

Recommendations

Despite significant movement, there is still much that needs to be done particularly while we await the arrival and impact of new IT systems and more uniform processes and standards. Because these delays impact our ability to meet our customers' mission requirements now, we offer five near-term recommendations for your consideration, as well as two additional suggestions for long-term reform.

- 1) **Funding**: We urge Congress to invest near-term resources to increase the Government's capacity to investigate and adjudicate cases. In our experience, over the last few years our government customers' field investigative teams have not been able to meet the needed case load due to funding constraints. Therefore, we seek Congressional support for additional funding in Fiscal Year 2018 and 2019 to reduce the current 700,000 case load. We recommend that agencies present budgets in a clear and transparent fashion that will permit Congress to track whether funds authorized and appropriated for security clearance processing get reprogrammed "below threshold" for other purposes in the year of execution. Additionally, given the sheer volume of background cases involved, as DoD assumes responsibility for its own clearance investigations, we believe it will require strong program management to implement and coordinate the transformation. Talented people are critical for the development, sustainment, and enhancement of major ship, plane, satellite, armored, IT, and mission systems. Indeed, in the cyber domain top trained people are our ships, planes, and satellites. Until new systems, standards, and automation improve the speed and accuracy of clearance processing, increased funding for investigations and adjudications will remain critical to reduce and reverse the increasing backlog. It is also paramount to ensure the continuity and productivity of the current investigative workforce in order to reduce the backlog.
- 2) **Prioritization and Continuous Evaluation**: Irrespective of funding levels, we recommend that the agencies prioritize the backlog to devote resources to those cases having the greatest mission need -- regardless of whether such cases originate from the Government or from industry. The current "First in, First out" efforts to complete cases, versus mission impact or insider threat risk, reduce the ability to apply investigative resources toward cases with higher security risk as well as cases of greater mission need. This approach may mean suspending time-based periodic reinvestigations for lower tiered clearance level cases in favor of reliance on CE -- an action this Committee's own FY 2018 Intelligence Authorization bill suggests. We strongly support a shift to CE as the primary means for verifying trustworthiness as part of the risk assessment for continued access to information.
- 3) **Reciprocity and Portability**: First, a uniformly applied set of standards and procedures is needed across the entire Government to guide "suitability" and "fitness" determinations

that currently slow many cross-over clearances. These standards should be made public and require the Suitability Executive Agent to approve the special needs of individual agencies in advance. With these standards in place, agencies could then immediately grant provisional cross-over access for individuals who possess the same or higher level clearance required by the new position. This would be the norm, not the exception — such moves across agencies could then be implemented by notification as opposed to formal approval. Second, the Government should enforce the good, existing reciprocity policies — the DNI, as the Security Executive Agent, and Congress can hold agencies accountable for complying with these policies. Third, we support a paradigm shift to make clearances “portable” for contractors based on personal trustworthiness, and not the particular contract on which they happen to work. These reforms should reduce typical cross-over times from weeks or months to days, or even hours. These policy actions are extremely important because they would help reduce the clearance backlog and re-direct investigative resources toward higher risk and higher mission needs, thus bringing critical new talent within the cleared workforce. The improvements we seek in this area should not require additional resources, only process improvements.

- 4) Information Sharing: We understand the ODNI has developed a plan for a government information-sharing program that this Committee urged in its FY 2018 Intelligence Authorization bill. This program would make available personnel security information (stored in a central repository) among Government and Industry, and even between companies for employees who have applied to positions requiring security clearances. We urge establishing such a program as soon as possible. This would enable all of the public and private sector to identify and respond appropriately to insider threat security warnings.
- 5) Reinstituted IRTPA Timelines: We strongly support the GAO recommendation to construct a government-wide plan, including milestones, to meet timeliness objectives for the completion of security clearance investigations and adjudications. Such timelines would cover the entire clearance lifecycle, and would enable the Executive Branch to drive towards near, mid, and long-term objectives. It would also permit Congress to hold the Executive Branch accountable to quantifiable performance metrics. This approach worked in the last decade to help reduce an exploding case backlog. As GAO noted, the expiration of IRTPA reporting timelines in 2011 makes it difficult to evaluate and identify where and why delays exist, or to direct corrections where necessary.

In the long term, we need to radically simplify the clearance process by creating one set of uniform, simplified, and transparent standards to determine who is trustworthy. These standards would effectively streamline the numerous independent categories of “suitability,” “fitness,” and “security,” and eliminate disparate individual agency practices. Such a construct would require much stronger coordination and streamlining of standards within the multitude of government authorities and may benefit from one single trust authority.

In addition, we recommend that the government leverage and exploit new, ever-advancing digital technologies, including social media analytics, to create a modern, all-digital and

electronic security clearance process. This will drastically reduce costs and cycle times, while achieving improved security standards and outcomes. Such a process would utilize the exponentially growing, publicly-available, digital profile that we all generate, thereby providing investigators real, direct information about behaviors bearing on trust. Although this is a vision for long-term transformation, we need to begin moving toward it now.

Conclusion

On behalf of our industry and association partners we appreciate this opportunity to present our experience and recommendations on the security clearance backlog and those issues affecting it.

We are acutely aware of the enormous harm that can result from intentional or unintentional compromises of highly-classified information by employees unworthy of the Government's sacred trust. The Administration and the Congress correctly focus on these dangers. We do as well. In no way do we suggest weakening rigorous personnel vetting to improve processing speed. This said, **slow security is not good security**. The critical need for an improved security clearance process further highlights the need to protect and monitor our classified environments. We must weigh the risks of security compromise from untrustworthy personnel **within** our networks against the risk of compromises to our networks from attackers **outside** of them. We weaken the collective defense of our cyber domain if we cannot bring top talent into this fight. Our inability to vet talent, new or existing, in a timely manner within a fully funded security clearance process impacts our efforts and effectiveness.

Industry strongly believes that the focus of Congress, and of this committee in particular, will be key in determining the Government's ability to reduce the backlog to normal, healthy levels, and to do so in a way that makes our nation's security stronger through a faster, more effective security clearance process.

The following Companies and Associations have reviewed and agree to this testimony:

Industry	Associations
ManTech International Corporation	Aerospace Industries Association (AIA)
Amazon	Intelligence & National Security Alliance (INSA)
BDO	Industrial Security Working Group (ISWG)
Booz Allen Hamilton	National Defense Industrial Association (NDIA)
CACI	Northern Virginia Technology Council (NVTC)
CSRA	Professional Services Council (PSC)
DXC	
Engility	
Leidos	
Microsoft	
PAE	
SAIC	
Salient CRGT	
Telos	
Vencore	

Chairman BURR. Thank you, Mr. Phillips.
Ms. Chappell.

**STATEMENT OF JANE CHAPPELL, VICE PRESIDENT FOR
GLOBAL INTELLIGENCE SOLUTIONS, RAYTHEON CORPORATION**

Ms. CHAPPELL. Chairman Burr, Vice Chairman Warner, members of the committee: I'm honored to represent Raytheon today before the Select Committee on Intelligence. Raytheon and our employees understand and take very seriously our obligation to protect the Nation's secrets. We submit to the same clearance process that governs our government and military partners and we take the same oath to protect the information established and entrusted to us. Every day our number one priority is honoring that oath while meeting the needs of our customers.

As Vice President of Raytheon's Global Intelligence Solutions business unit, I navigate the disruptions that backlogs in the security clearance process cause on a daily basis, not just for Raytheon, but for our suppliers and our industry peers, but ultimately for the warfighters, intelligence officers, and homeland security officials who rely on our products and services to protect the United States.

The magnitude of the backlog and the associated delays is well documented, and the metrics speak for themselves. But what metrics fail to capture are the real-world impacts of the backlog: new careers put on hold, top talent lost to non-defense industries, and programs that provide critical warfighter capabilities suffer delay and cost increases. The delays also come with a real-world price tag. Those new hires run up overhead costs while they wait for their clearances, resulting in significant program cost increases and inefficient use of taxpayer dollars.

Reducing the current backlog will require immediate and aggressive interim steps, some of which are already being addressed. Raytheon supports the government's efforts to add resources and ease requirements for periodic reinvestigations. We also appreciate efforts to streamline the application process, automate and digitize information collection, provide for secure data storage, and improve the related processes.

Beyond these actions, we recommend eliminating the first-in, first-out approach to the investigation workflow, focusing immediate resources on high-priority clearance and low-risk investigations.

It's also critical that Congress and the Executive Branch implement fundamental reforms that streamline the clearance process and increase our Nation's security by leveraging advances in technology. This effort should be guided by what our industry calls "the four ones." The first one is one application, which is a digital permanent record forming the basis of all clearance investigations, updated continuously and stored securely.

The second is one investigation, which would implement continuous evaluation and the appropriate use of robust user activity monitoring tools to facilitate a dynamic ongoing assessment of individual risk while securing sensitive information on protected systems.

The third one is one adjudication, which calls for streamlining and standardizing the adjudication system so the agency's clearance decision is respected by other departments and agencies. This would increase efficiency and promote reciprocity based on a consistent set of standards for access, suitability, and fitness.

The fourth and final one is one clearance, that is recognized across the entire government that is transferable between departments, agencies, and contracts.

We believe the implementation of these reforms will help eliminate the inefficiencies that hamstring the current clearance system while promoting more effective recruitment, retention, and utilization of government employees and contractors. And most critically, these reforms will help close the security gaps that threaten our Nation's secrets and personnel.

The modern threat environment can no longer be addressed using outdated and infrequent security snapshots. But even the most well-intended reporting requirements, working groups, and legislative deadlines have not and will not overcome the fear of change or the comfort of the status quo. Strong, sustained leadership from both Congress and the White House will be crucial to the success of these efforts.

Thank you for the opportunity to be here today and I look forward to answering your questions.

[The prepared statement of Ms. Chappell follows:]

STATEMENT OF
JANE CHAPPELL,
VICE PRESIDENT, GLOBAL INTELLIGENCE SOLUTIONS,
INTELLIGENCE, INFORMATION AND SERVICES,
RAYTHEON COMPANY
before the
UNITED STATES SENATE
SELECT COMMITTEE ON INTELLIGENCE

—

March 7, 2018

Chairman Burr, Vice Chairman Warner, Members of the Committee, I am honored to represent Raytheon today before the Select Committee on Intelligence.

Raytheon and our employees understand — and take very seriously — our obligation to protect the Nation's secrets. We submit to the same clearance process that governs our Government and military partners, and we take the same oath to protect the information entrusted to us. Our number one priority every day is meeting the needs of our customers.

As Vice President of Raytheon's Global Intelligence Solutions mission area within our Intelligence, Information, and Services business, I navigate the disruptions that backlogs in the security clearance process cause every day — not just for Raytheon, our suppliers, and our industry peers, but ultimately for the warfighters, intelligence officers, and homeland security officials who rely on our products and services to protect the United States and our allies.

The magnitude of the backlog and associated delays speaks for itself. In September of 2017, the National Background Investigations Bureau (NBIB) faced a backlog of around 709,000 investigations. Delays in the initiation, investigation, and adjudication process for both secret and top secret clearances were two to three times longer than the timelines set by Congress in the Intelligence Reform and Terrorism Prevention Act of 2004.

But what those numbers fail to capture are the real-world impacts of the backlog. New careers are put on hold, top talent is lost to non-defense industries, and programs that will provide critical warfighter capabilities are delayed. And these impacts come with a real-world price tag, resulting in otherwise-unnecessary increases in program costs and inefficient use of taxpayer dollars.

We would gladly accept these costs if the clearance process delivered significant improvements in the security of our Nation's most sensitive

information, facilities, and personnel. Unfortunately, we have seen little evidence that the decades-old clearance process achieves that goal, especially when considering the threat posed by trusted insiders to classified computer networks. The modern threat environment can no longer be addressed using outdated and infrequent security snapshots.

To address the costs of the backlog, we ask Congress and the Executive Branch to implement fundamental reforms that streamline the clearance process and increase our Nation's security by leveraging advances in technology.

The Backlog

Raytheon is a technology and innovation leader specializing in defense, security, and civil markets throughout the world, and a world leader in advanced cybersecurity solutions for both the public and private sector. We have a workforce of approximately 64,000 employees, 68% of whom hold some level of security clearance. As these numbers demonstrate, Raytheon's ability to meet the needs of our customers depends on both our ability to attract and retain top talent, and our ability to get our employees the clearances needed to do their jobs.

With current backlogs, we have nearly 4,300 employees awaiting clearances, and almost 5,000 more awaiting the completion of a periodic reinvestigation — almost 15% of our total workforce.

In 2017, the average length of time it took a Raytheon employee to get an initial clearance was:

- 225 days for Confidential,
- 252 days for Secret,
- 500 days for Top Secret, and
- 328 days for Top Secret/Sensitive Compartmented Information (TS/SCI).

Surprisingly, the timelines for periodic reinvestigations were even longer, exceeding 615 days for a Top Secret clearance holder.

Our Missile Systems business has a rolling backlog of between 400 and 500 new hires who are unable to start their jobs because of delays in processing their clearances. And in the business unit I oversee, almost 300 software and systems engineers are also waiting.

These candidates have high-demand technical skills. They are enthusiastic about supporting our customers, and they meet the stringent pre-

qualifications we impose on anyone applying for a clearance. In short, they are "unicorns." We do what we can to keep them interested while they wait for their clearance, but a candidate's patience only lasts so long, especially when they have other options.

The Job Market

To truly understand the impact of clearance delays on the defense industry, you have to start with the job market. Our customers demand the most advanced technologies that Raytheon and the defense industry can produce — particularly on the most sensitive programs. This requires a continuous and persistent effort to recruit and retain top technical talent. And, our pool for positions requiring clearances is further restricted to U.S. citizens.

Faced with these customer requirements, the demand for cleared talent has dramatically increased. Currently, more than 120,000 job openings in the United States require a Secret clearance, and another 30,000 require a TS/SCI.

By our estimates, 480,000 people in the contractor community hold a Secret clearance, and 446,000 hold a Top Secret clearance. But most of these candidates are already employed, which means there are far more open roles than cleared candidates to fill them. This has led to a dire imbalance in the market for cleared talent. As a result, employers are paying cleared candidates an extra 10-15% in base pay and sign-on bonuses that *start* at \$15,000.

In the last few years, non-traditional commercial competitors have also entered the market, driving these premiums to unprecedented levels. A recent example of this involved an entry-level software engineer who left Raytheon after receiving his TS/SCI clearance. A commercial competitor offered him a \$20,000 sign-on bonus, a 15% increase in base pay, a 20% annual performance bonus, a \$25,000 annual bonus for maintaining a TS/SCI clearance, and \$20,000 in company stock.

And this offer was not a one-off. We often find ourselves choosing between matching these lucrative competitive offers and losing our cleared talent.

While preparing for this hearing, a Vice President from our missile business recounted a disappointing story. While he was pumping gas, he started a conversation with the gas station clerk, who turned out to be a recent college graduate who had accepted an offer to join Raytheon pending the outcome of his clearance. The candidate moved across the country to Tucson for his new job, but as his start date at Raytheon was delayed by the clearance process, he was forced to work at the gas station to make ends meet. While we are certainly proud he was willing to wait for the job of his dreams, many other

candidates are not as patient. And, when you add the pressing weight of college debt and the desire to keep technical skills current, the impact of delays on new college graduates is only amplified.

The impact of clearance delays is not confined to our highly-skilled technical workforce. They also affect candidates who we would like to hire for stable and well-paid manufacturing jobs. Many of these candidates come from lower- or middle-class backgrounds, and they simply cannot afford to wait — unemployed and without pay — for months while a clearance is received. Far too often, these candidates will accept another job well before we are able to bring them on following a months-long delay in the adjudication of even an interim Secret clearance.

To avoid stories like this, Raytheon often starts employees before they are cleared. They are assigned as much unclassified work as possible, but certainly not the kind of work they joined the company for, or what we hired them to do. And, while they wait, the associated overhead costs grow and grow. These costs ultimately work their way back into our products and services, eroding the buying power of our customers and delaying the delivery of critical capabilities.

Our subcontractors — particularly small businesses that cannot shift employees or other resources to manage their way through clearance delays — are also affected by the backlog. Recently, Raytheon identified a small, veteran-owned business to conduct a significant portion of the work on a sensitive Intelligence Community system designed to automate analysis for new sensors. After waiting through long delays to get their employees cleared, Raytheon was forced to give the subcontract to an alternative source to prevent program delays.

Even companies the size of Raytheon are not immune, and clearance delays have had real effects on our programs. To avoid the program delays and cost increases caused by the clearance backlog, we work diligently with our customers to leverage our cleared workforce across multiple programs to cover gaps.

These gap-filling personnel decisions — based primarily on clearance status instead of qualifications — have career consequences for everyone involved. High-performing employees can be stuck doing less important work, and program managers have to stretch cleared talent to cover critical tasks while the employee they need waits for a clearance.

Managing risk on our most sensitive compartmented programs or “Special Access Programs” (SAPs) is even more complicated because of the severe restrictions on the number of billets made available by the Government.

These restrictions can delay and limit workforce management decisions, and often prevent cross-pollination of lessons learned and efficiencies across our program portfolio. And reciprocity issues can sometimes prevent an employee with an active clearance at the same level needed on a different program from transferring between contracts without an additional investigation or adjudication.

These impacts negatively affect the lives of our employees, hinder Raytheon's ability to effectively manage complex programs vital to our national security, and add unnecessary costs that ultimately burden our customer's budgets and American taxpayers.

The Process

Despite various amendments to laws and executive orders, the security clearance process has gone largely unchanged since the 1940s. Applicants submit their background information and federal investigators (either federal employees or contractors) conduct an extensive investigation of the applicant.

Investigators operate on a five-tier system, with each successive tier mandating a more thorough background investigation based on the level of access granted. Tier 5 is reserved for the most sensitive access — to Sensitive Compartmented Information and other highly sensitive information or positions.

Periodic re-investigations are initiated, conducted, and adjudicated the same way as the initial clearance, and are required every 5 years for a top secret clearance, 10 years for a secret, and 15 years for confidential.

If the process looks complex on paper, I can assure you it is far worse in practice.

The intelligence reform act required each federal department and agency to honor the clearances of others (with certain limited exceptions) — a process known as “reciprocity.”

In practice, agencies do not always honor the investigations or adjudications of others. Some mandate differently tiered investigations for different types of suitability and access determinations. Some mandate a polygraph. If a polygraph is required, the scope can vary. Some agencies mandate a polygraph every three years before a contractor can access sensitive government systems — even if the contractor has an active TS/SCI clearance that does not yet require a periodic reinvestigation. Some elements of larger departments do not acknowledge clearances issued by components within the

same department. And, when these differences arise, a new investigation is often ordered and added to the backlog.

And recently, at least one of our customers has mandated a Secret-level clearance for access to Unclassified/For Official Use Only (U/FOUO) material. These additional applications also clog the clearance pipeline, and impede clearance applications for individuals that require access to information that is actually classified.

Though we have seen some progress on reciprocity — particularly across the Intelligence Community — the Government continues to struggle with the size and scope of the issue. From our standpoint, the theory of reciprocity exists, but in reality, reciprocity is managed to different risk levels across different agencies. Simply put, the reciprocity ideal is not a fully realized practice. It is our understanding that Government-wide reciprocity standards originally planned for September 2013 have yet to be issued, are continually challenged with effective interagency coordination, and have no proposed deadline for completion.

The Government has only recently begun to automate and streamline the investigation process. In 2003, the Office of Personnel Management (OPM) automated the collection of information needed for the initial clearance application. Since then, OPM has made progress on a digitized SF-86 — the form applicants submit to initiate a clearance investigation or periodic reinvestigation — as well as other improvements to information collection and adjudication. However, following the OPM data breaches in 2015, at least one Intelligence Community agency stopped using these web-based tools. While OPM's overall efforts are steps in the right direction, none of them represent the transformative change needed to reduce the current backlog and prevent future delays.

Interim Reforms

The magnitude of the current backlog and associated clearance delays demands immediate and aggressive interim actions. Raytheon supports the Government's efforts to add investigative resources and ease requirements for periodic reinvestigations, and we also appreciate efforts to streamline the application process, automate and digitize certain information collection, provide for secure data storage, and improve other related processes.

Despite these improvements, at investigative resource levels NBIB has identified as feasible, GAO indicates that a "healthy" backlog — around 180,000 pending investigations — would not be reached until fiscal year 2022 "at the earliest."

As an interim measure, Raytheon encourages the Government to reevaluate the “first-in/first-out” investigation approach and adopt a risk-based method that would quickly adjudicate low-risk investigations and prioritize mission-critical investigations. Higher-risk, time-consuming investigations would be delayed until additional investigative resources were available.

Adjusting the periodic reinvestigations process will also free investigative resources for initial reviews, but we urge the Government to reconcile the current extensions with inconsistent recognition of “expired” clearances. Despite a December 2016 Department of Defense (DoD) memorandum directing otherwise, employees with current, valid investigations are being denied access by some customers based on Government-directed delays to initiate a periodic reinvestigation. These inconsistent decisions exacerbate the backlog with no clear risk-based justification.

The Government should also consider recognizing background investigations conducted by private sector employers as the basis for lower-risk clearance and access determinations. Consistent with applicable laws, these employment-related investigations often entail the collection and review of publicly available and sensitive information on a candidate’s financial, criminal, residency, military and educational records. These records serve as the foundational components of all federal clearance investigations. If these investigations met Government-established standards for rigor, the results could serve as the basis for certain lower-risk clearance, access, or suitability determinations by an adjudicating agency.

Additional resources and thoughtful adoption of low-risk interim adjustments may marginally improve the current situation, but fundamental reforms to the clearance process are essential. Without these foundational efforts, inefficiencies will continue to frustrate progress with no real increase to the security of the Government’s information, facilities, or personnel.

Fundamental Reforms

In 2006 — with a clearance backlog of 300,000 investigations — a coalition of industry associations recommended a set of reforms known as the “Four Ones” (<https://www.itic.org/public-policy/SecurityClearanceReformCoalitionWhitePaper%28Final%292006.pdf> and https://oversight.house.gov/wp-content/uploads/2017/10/ITAPS_Hodgkins_Testimony_Security-Clearance-Investigations.pdf).

- One Application — one standardized and digitized application for all clearance determinations, updated continuously and stored securely,

to form the “permanent digital record” for the initial and any subsequent suitability, access, or clearance determinations.

- One Investigation — enabling a dynamic, ongoing examination of individual risk by implementing continuous evaluation.
- One Adjudication — streamlining and standardizing the overly complex adjudication system so that one agency’s clearance decision is respected by other departments and agencies, promoting reciprocity and efficiency.
- One Clearance — recognized across the entire Government, transferable from department-to-department, agency-to-agency, and contract-to-contract.

More than a decade after they were first proposed, the “Four Ones” continue to serve as a roadmap for needed reforms, and a reminder that progress has fallen far short of expectations.

To make immediate progress, Raytheon encourages the Government to prioritize and set incremental milestones for implementing Government-wide reciprocity, continuous evaluation, and information technology reforms.

Information technology reforms that enable automated application collection, incorporate new information derived from investigations or continuous evaluation, and provide secure, cross-domain mechanisms for accessing investigative information are vital to support each prong of the “Four Ones.” Technology forms the basis for automated applications and the establishment of a permanent, electronic investigative file. It underpins continuous evaluation, and is necessary to provide the confidence departments and agencies need to confidently implement Government-wide reciprocity.

We support the direction that the Department of Defense (DoD) and the Office of Personnel Management (OPM) are taking to establish the National Background Investigation System, but vigorous oversight and robust resources will be required to address integration and security risks that the system must overcome.

Effective implementation of a comprehensive continuous evaluation program will help eliminate the need for time-based periodic reinvestigations for all clearance holders, cutting the unnecessary costs incurred to fully investigate even low-risk individuals. More importantly, we strongly believe that this dynamic, ongoing approach to vetting will increase security and detect, deter, and mitigate insider threats.

As currently constructed, the periodic reinvestigation system only provides a risk snapshot for clearance holders when the initial investigation is conducted and at prescribed 5-, 10-, or 15-year intervals. In the intervening

periods, our Nation's security relies upon self-reporting and serendipity to identify risks.

Continuous evaluation fills this security gap, providing immediate reporting on security threats and allowing agency security officials to make real-time risk determinations. When necessary, these risks may be so significant that immediate personnel action is required. Alternatively, the risks may call for initiation of a risk-based, aperiodic reinvestigation. Any aperiodic reinvestigation, based on the continuous collection of investigative data since the initial clearance determination and informed by targeted investigations associated with significant security concerns, could be conducted more efficiently than the current process which basically recreates the initial investigation.

I would be remiss if I did not underscore Raytheon's belief that an effective continuous evaluation system must be accompanied by robust user activity monitoring (UAM) programs. With so much sensitive information contained in our Government's information technology systems, it is vital that security officials be able to quickly identify inappropriate user activity on their networks — both classified and unclassified. Context-aware UAM programs, when combined with data from other continuous vetting sources, will enable real-time, risk-based decision making about system users and clearance holders.

One tool informs the other, *and the combination promotes increased privacy protections*. Comprehensive, detailed monitoring of all users is unwieldy, impractical, and invasive. Modern, analytics-enabled UAM allows security officials to adjust the sensitivity of the tool based on the risk associated with particular users. So, a clearance holder with security risks identified in continuous evaluation could be more carefully monitored by UAM when using Government systems. Users with low-risk activity on Government systems may require less comprehensive continuous evaluation. The combination promotes efficient targeting of investigative resources toward higher risks, and protects the privacy interests of low-risk personnel or contractors.

The electronic availability of secure, up-to-date investigative records, clearance histories, and any security risks identified through continuous evaluation and UAM, should make the implementation of reciprocity that much easier. Agencies will be more willing to trust prior adjudications and will have access to any intervening derogatory information — not to make independent clearance decisions, but to promote a one-Government/one-individual approach to the clearance process.

Finally, I believe it is critical to note that sustained and relentless leadership — from both Congress and the White House — will be crucial to successfully implement reforms. Even the most well-intentioned reporting requirements, working groups, and legislative deadlines have not, and will not, outlast the fear of change or the comfort of the status quo.

The Committee's investments of time and resources to effectively implement this security framework will help eliminate the investigative inefficiencies, duplication, and stove-piped decision making that hamstring the current clearance system. They will promote the effective and dynamic recruitment, retention, and deployment of Government employees and contractors as dictated by skill and performance, not based merely on the availability of a current clearance. And, critically, they will help close the security gaps that threaten our Nation's secrets and personnel.

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

Chairman BURR. Thank you, Ms. Chappell.
Mr. Berteau.

**STATEMENT OF DAVID BERTEAU, PRESIDENT AND CHIEF
EXECUTIVE OFFICER, PROFESSIONAL SERVICES COUNCIL**

Mr. BERTEAU. Thank you, Mr. Chairman, Vice Chairman Warner, members of the committee. We really appreciate you having this hearing today. I would ask that my written statement be incorporated in the record in its entirety and I'll just make a few key points here.

You heard the description of the problems and the process solutions, the four ones: one application, one investigation, one adjudication, and one clearance. It highlights, I think, the fact that this is really a whole-of-government problem. Just look at the panel that you have following us. You don't have a whole-of-government representation on there.

As Vice Chairman Warner pointed out, the Office of Management and Budget plays a key role both in the Performance Accountability Council and in the fundamental process across the board. In the end, though, this is a set of processes that exercises judgment. It makes the decision of where to place trust. And in that decision is a calculus of how much risk are we willing to accept. If it's zero, then we'll never issue a clearance. So there's a whole level of dynamic that has to go on there, and the four ones helps get you there.

What, though, can this committee and the Congress do? First is keep that whole-of-government requirement in mind. Second is, within that there's a funding process. So all of those 23 agencies that have separate authorities here have to provide funding to somebody who's going to do the work. Typically today that's the National Background Investigation Bureau. We can't find, from where we sit outside, a record of where that funding stands for those 23 agencies, because it's across all the appropriations accounts. OMB used to track that and report that, but that's no longer available to us. It may be available to you. It should be available to you. And I think it's important as we look at the fiscal year 2018 funding bill that we'll see end of this week, early next week, make sure that that funding is in there, because these systems will not operate without adequate resources. You can't buy your way out of it, though. There's got to be substantial process improvement as well. My fellow panelists have talked about that.

But in the meantime, you have a requirement for part of this responsibility to be moved from the Office of Personnel Management, the National Background Investigations Bureau, over to the Defense Department, and you'll hear more about that in the second panel. While that movement's taking place—and the plan is it will take years—the system has to keep going as well. So there's got to be both funding for the ongoing work and funding for the new capabilities inside the Defense Department. So that makes it all the more important.

My fellow panelists have mentioned reciprocity. This is a critical, critical issue. How can it be that you're cleared and acceptable for one part of the government at a certain level and you're not cleared and acceptable at another part? The records show 23 different

agencies, but within those agencies there's lots of subcategories. DHS alone has more than a dozen separate individual reciprocity determiners who can say: You may be good enough for those guys, but you're not good enough for me. And they don't even have to tell us why, which makes it very hard for us to figure out how to get out of that.

So industry can quantify its impact. You've already heard some of that. We all know there's an impact on the government as well. Somewhere in the government, something's not being done or not being done as well as it ought to be or not being done as fast as it ought to be. We don't have that kind of information out of the government, but you've got to believe that in fact somewhere a backlog of 700,000 is going to have an impact, because this is not just contractors; this is government civilian personnel, this is military personnel, this is new recruits. All of those have effects as well.

So I think the single biggest thing is access to information about what's going on, what the results are. You've got a situation now where it used to be there was information made available to the public that we could rely on to prioritize our own resources. That's no longer there. We need you to help make that information not only visible to you in the committee—it might come to you in an FOUO kind of a status—but visible to the public and to those of us who have to operate within that system in order to do our job supporting the government.

So with that, Mr. Chairman, I'll conclude my remarks and turn back to you.

[The prepared statement of Mr. Berteau follows:]



Statement of David J. Berteau

President & CEO

Professional Services Council

"Security Clearance Reform"

Select Committee on Intelligence

United States Senate

March 7, 2018

***Statement of David J. Berteau, President & CEO, Professional Services Council,
before the Senate Select Committee on Intelligence***

March 7, 2018

Introduction

Chairman Burr, Vice Chairman Warner, and Members of the Committee, thank you for the invitation to testify on behalf of the Professional Services Council's (PSC) nearly 400 member companies and their hundreds of thousands of employees across the nation.¹ PSC is the voice of the government technology and services industry, supporting the full range and diversity of government missions and functions across all agencies. I appreciate the opportunity to discuss with you the current status of the personnel security clearance process, the impact of the current situation on industry, and the prospects for reform. These are issues of great significance for our member companies and their employees, as well as for the success of government missions and support functions.

Today, I will describe some of the opportunities and challenges for Congress and federal agencies and offer some recommendations to improve the process and reduce the negative impacts on contractors and our government partners.

I believe there is much this committee can do in legislation and oversight that will lead to practical and productive improvements.

Contractors Provide Significant Value to the Government

The contractor community plays a vital role in assisting the government in providing services to the American people. Contractor contributions are necessary to maintaining government operations. Many of the capabilities that contractors provide do not exist, or are insufficiently available, within the government, and contractors can quickly expand or adjust capacity to meet changing mission needs. Contractors draw from a strong, diversified national interest business base to support current and emerging requirements for every agency of the government.

To meet these demands, however, contractors need to be able to hire, retain, assign, and transfer qualified, skilled employees to the missions and functions with greatest need. Like the federal employees they work aside, contractors come to work every day to do a

¹ For over 45 years, PSC has been the leading national trade association of the government technology and professional services industry. PSC's member companies represent small, medium, and large businesses that provide federal agencies with services of all kinds, including information technology, engineering, logistics, facilities management, operations and maintenance, consulting, international development, scientific, social, environmental services, and more. Together, the association's members employ hundreds of thousands of Americans in all 50 states. See www.pscouncil.org.

job that is vital to the government's ability to achieve their missions. Both federal workers and contractors deserve a better system for background investigations and clearances.

Scope of the Problem

The Government Accountability Office (GAO) agrees on the need for a better system. On January 25, 2018, GAO added the government-wide personnel security clearance process to its High Risk List of federal areas in need of either broad-based transformation or specific reforms to prevent waste, fraud, abuse, and mismanagement.

Prior GAO studies highlight not only the extent on the problem but also how the backlog and wait times have increased within the past year alone.

According to OMB, at the end of FY17, the backlog covered 708,000 individuals. There are now over 700,000 military, civilian, and contractor personnel who remain in limbo awaiting a clearance to perform mission-critical work. In FY16, the backlog was 573,000.

In FY17, the average number of days to complete the fastest 90 percent of initial Secret clearances was 134 days, up from 108 days in FY16.

In FY17, the average number of days to complete the fastest 90 percent of Top Secret clearances was 331 days, up from 220 days in FY16.

The backlog and wait times are unacceptable and growing. PSC and the industry agree with GAO on the need for action now.

Industry Impact

The impacts of the security clearance process, the backlog of cases and the wait times associated with obtaining a clearance affect both government and industry. As other witnesses today have described, we can and have quantified these impacts on the contractor community. The government has not, to my knowledge, quantified the impact on the government workforce and government missions, but we know that it is real. I urge the committee to ask the leaders of the Department of Defense (DoD), and other national security agencies about these consequences. Only when they recognize the need to reduce negative impacts will they make improvements a sufficiently high priority.

From our industry's perspective, one of the biggest impacts is on our workforce. Recruitment and retention remain significant challenges. Contractors are often unable to fill positions requiring clearances, even when the positions are funded under existing contracts. Essential work goes unperformed, and contractors can even be penalized for contractual non-performance by the very agencies that are holding up the clearances. Some agencies have even enforced liquidated government damages on contractors who have missed staffing deadlines due to delayed processing of contract employees' clearances.

Neither government nor industry partners can recruit for critical national security missions or compete to hire the best and brightest when those individuals have to wait months or even years before being able to work.

False Dichotomies of Security Clearance Reform

There are two false dichotomies that may be raised when security clearance reform is discussed.

The first dichotomy is that a faster process means we are less secure, that applicants receive less scrutiny, and that risks are heightened. This is simply untrue. Process improvements can speed up the timelines of clearance approvals without cutting corners and because they can provide continuous monitoring of cleared personnel, can actually make us more secure, not less.

The second dichotomy is that a better system costs more. This is also untrue. Over time, a more efficient system will be more cost effective to operate and would also reduce money wasted when the government cannot meet mission needs as a result of the backlog.

Recommendations

The recommendations below include concrete actions that Congress can take and also includes steps for the executive branch to address deficiencies and risks, reduce the backlog and speed up processing times, and carry out effective oversight of initiatives at federal agencies.

Most broadly, PSC recommends adopting and implementing what we call the “four ones.” These principles can and should apply both to the government and to contractors. The federal government has made progress, but greater and more rapid results are necessary. These principles are:

- One application;
- One investigation;
- One adjudication;
- One clearance.

Adopting policies that will implement the “Four Ones” will provide remedial actions that touch on all aspects of this issue—including and especially—reciprocal recognition for existing clearance holders.

Adopt a Whole of Government Approach

The security clearance process is a government-wide problem that requires a government-wide solution. No one agency can fix this, and cabinet-level leadership and

White House engagement are crucial. This committee can help by focusing continuously on their roles.

Require Up-to-Date, Publicly Available Data

Unfortunately, as the problem has worsened, the government has made information less available. This helps no one.

Congress should legislate requirements for all relevant agencies to provide timely, accurate, publicly available, and up-to-date data on the size and scope of the backlog and the wait times for individuals seeking a security clearance. Without knowing the extent of the backlog or the causes, actions to reduce the number of individuals awaiting security clearances and implementation metrics risk being either insufficient or mistargeted. From my experience as an Assistant Secretary of Defense, I know that I paid greater attention to the responsibilities on which I was reporting regularly to Congress and the public.

On June 15, 2017, the Office of Management and Budget issued memorandum M-17-26 "Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda,"² removing outdated and unnecessary regulatory and administrative burdens on federal agencies, on government contractors, and on taxpayers. PSC supported the elimination or modification of many of these OMB burdens, but some removals were counterproductive.

Under the June 15 OMB Memo, agencies are to discontinue reporting on all previously covered priority goals for the remainder of fiscal year 2017, even when those goals align with the Administration's current priorities, as confirmed to PSC by OMB's Resource Management team.

In a June 22, 2017 letter to Director Mulvaney,³ we detailed our concerns about OMB's elimination of reporting requirements under the GPRA Modernization Act, under which agencies provide quarterly progress reports via performance.gov with respect to both individual agency and cross-agency priority goals.

These quarterly reports have provided PSC and our member companies with valuable insight into agency activities, including successes and remaining challenges. In the case of the cross-agency goal for security clearance, the quarterly reports have provided critical information on addressing key administration, congressional, and industry interests.

² Executive Office of the President, Office of Management and Budget. *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda* (M-17-26). Issued on June 25, 2017. Text from: <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-17-26.pdf>

³ Professional Services Council (PSC) letter to Office of Management and Budget Director Mick Mulvaney. June 22, 2017. Text from: <http://www.pscouncil.org/Downloads/documents/PSC%20Letter%20on%20OMB%20Memos%206.22.17.pdf>

Section 925 of the FY18 National Defense Authorization Act (NDAA) does include many reporting requirements on the size and scope of the backlog. Yet—unlike previous government reporting—under current practice, this information will be seen only by the congressional committees of jurisdiction—leaving the heavily-impacted contractor community in the dark, along with many of their government customers, as well as state and local officials. PSC believes the best way to fix this is to expand statutory reporting requirements and to make the information public.

Speed up Vetting and Clearance Process

The vetting and clearance process can be accelerated while maintaining system integrity and without cutting corners. Let's look at how it is now. Currently, to verify an applicant's educational background, an investigator must draft, print and hard mail a letter to the college or university cited. The investigator then waits for the college or university to respond—again via hard mail—with a verification of the applicant's information. Once the verification letter is received, the investigator scans it into their system and adds it to the applicant's file. This example highlights the outdated, cumbersome, and lengthy process now used to simply confirm that an applicant attended the college they claim to have attended. There are much faster and more reliable ways to do this.

Much of the backlog problem comes from using an antiquated, time-consuming background investigations process. Investigators ask basically the same questions they did 40 years ago, often going door-to-door and relying on face-to-face meetings with neighbors and friends. The government still relies too much on paper records and closed systems for collecting and sharing information. Investigators are often required to take notes on paper, then type those notes into an antiquated computer system. They are not even allowed to use a computer or electronic tablet.

The amount of manual effort required in the investigation process for a majority of personnel can be dramatically and significantly reduced through the use of technology that automatically pulls in previously verified information and other publicly available information.

Provide the Necessary Resources for Federal Agencies

OPM's NBIB operates under a revolving fund, which is replenished by the transferring funds appropriated to each of the 20-plus agencies that use NBIB. There is often no specifically identified request or justification for those funds in the President's budget, making it unclear for Congress to be sure adequate funding is provided. This makes it more important that Congress provide the agencies conducting the investigations and the adjudications the necessary resources.

Right now, there are too few well-trained people processing clearances and too little money to meet the demand. As a result, PSC member companies regularly report that cases are delayed further by lost forms, communication disconnects, failure by agencies to process responses, and inadequate tracking of cases or reporting of their status.

The entire system across the federal government needs a workforce that is trained and appropriately sized with the necessary funding for investigations and adjudications, as well as the authorities to prioritize and allocate resources based on risk. They also need a strategic implementation plan that will improve overall performance through predetermined metrics and milestones with strong accountability mechanisms.

For the FY18 and FY19 appropriations bills, Congress should account for and support full funding for all of the relevant components.

Conduct Aggressive Oversight of the Sec. 925 Transfer

Section 925 of the FY18 NDAA requires DoD to conduct its own background and security investigations by transferring certain clearances from the National Background Investigations Bureau (NBIB).

This will require the Committee to participate with the other committees of jurisdiction in regular, detailed oversight of the three-year process to transfer authority. The timeline is demanding, and detailed plans are not yet available, at least to us, which we see as increasing risk. Congress can and should ensure that DoD stays on track, while funding and processing the remaining clearance requests at NBIB must remain a priority. We also recommend that, as Senators, you should also raise these issues with every nominee and every witness in the affected agencies.

Prioritize Continuous Evaluations

Congress should require that agencies prioritize continuous evaluations, both as a timely response to insider threats and to reduce the burden of periodic reinvestigations. This is where process improvements offer the greatest payoff.

PSC strongly supports the continuous evaluations (CE) approach and urges Congress—through regular reports and oversight—to incentivize and reward government-wide moves toward more robust CE. The current process of reevaluations is based on the calendar, not on risk or need. To be successful, CE must be part of the personnel system as well as security clearance, suitability, and credentialing procedures. Moving to CE will significantly reduce current and future backlogs by removing periodic reevaluations from the queue. Moving from a timeline-based process to continuous monitoring will also increase security and reduce insider threats in a timely manner.

The Departments of Homeland Security and Defense are currently operating CE pilot programs that monitor available databases for information on security clearance holders. Although the results of these pilots have not been made public, we believe they show that the technologies and processes already exist and are in use by federal government agencies—making it practical to expand CE government-wide.

Implement True Reciprocity among Federal Agencies

Perhaps the problem that should be easiest to fix, is the delay in granting reciprocal recognition of clearances to contractors and government personnel who move from agency to agency (or even in some cases from contract to contract within the same agency.)

At the government-wide level, the NBIB, established on October 1, 2016, is currently the primary provider of background investigations (BIs), including processing of electronic questionnaires, conducting national agency record checks, and maintaining a central clearance repository. In most cases, the NBIB processes the forms, schedules and conducts BIs, and delivers results to the agencies to adjudicate employee suitability, contractor fitness, and, when needed, a security clearance determination. Agencies can and do impose unique requirements on personnel who have already been granted a clearance by another federal agency, delaying and sometimes denying the transfer of a clearance.

Existing regulations already provide guidance for implementing reciprocal recognition. These include language in the January 17, 2017, executive order to modernize the executive branch-wide governance structure and processes for security clearances, suitability and fitness for employment and credentialing, and the Director of National Intelligence's (DNI) Strategy and Schedule for Security Clearances Reciprocity.

Legislatively, Congress should task the head of each federal Department and the Director of the Office of the Director of National Intelligence to account for, and then justify, each distinct exception among components within their jurisdiction. PSC understands that reciprocity is culturally hard, but implementation would be easy to implement with big payoff.

Reciprocity is another area where data are lacking—we do not know the extent of the problem, its contribution to the backlog and wait time estimates, and the reasoning behind why certain adjudications may take one day, one month, longer or never granted at all.

Executive Order 13764 states: "Any additional requirements approved by the appropriate Executive Agent shall be limited to those that are necessary to address significant needs unique to the agency involved, to protect national security, or to satisfy a requirement imposed by law."⁴

PSC agrees with the criteria but urges the committee to better define when the situations occur. Currently, there is no central tracking of compliance with existing regulations or documentation on the justification for exceptions to reciprocity guidelines and the frequency of their use.

⁴ Federal Register. *Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters* (Executive Order 13764). Issued on January 17, 2017. Text from: <https://www.gpo.gov/fdsys/pkg/FR-2017-01-23/pdf/2017-01623.pdf>

For example, at a Professional Services Council event, the Department of Justice (DOJ) alone cited at least five different required sets of background information, with each of those DOJ agencies failing to recognize the validity of similar investigations from any of the others, even within the same department.

There is a related problem under which personnel with active clearances are delayed for months or even a year or more when being considered for a separate determination of suitability or fitness for a position. Fixing that may also require Congress to act.

These actions would focus attention on risk to the government rather than on rote application of rules. Further, they may lead to efficiencies in the process and synchronization of requirements Department-wide or Intelligence Community-wide.

Conclusion

As you will hear from the second panel today, NBIB has plans for process changes that offer hope for improvement. DoD, implementing Sec. 925, is working on similar plans. Nevertheless, the failures and shortcomings of the current personnel security process impact uniformed personnel, civilian employees, and contractors across the country—in every state and congressional district—and weaken our national security.

The backlog and wait times add risk to government missions, contract performance, and the ability to recruit and hire. Security clearance processes need to be better and faster.

PSC applauds the committee for holding this hearing and for emphasizing the need to improve the security clearance systems. Yet one hearing is simply not enough to address the scope and scale of this problem. These issues have arisen time and again. While the recommendations above can help address the problems, only Congress, through sustained oversight, can produce agency implementation of these reforms.

On behalf of PSC and our members, I thank you for your time and consideration of these matters. As always, PSC is available at your convenience to address any questions or concerns you have, now and in the future.

Chairman BURR. Thank you, Mr. Berteau.

The Chair would recognize himself, and then we'll go by seniority for up to five minutes.

My question is very simple, and it's this. Let's make an assumption that funding is not an issue. Why does it take so damn long? Give me the three things that make this process be so long?

Mr. PHILLIPS. Let's start, sir, with we have from history a number of agencies who have their own processes set up and they have to go through those processes, and they're very manual. As mentioned before, the process was established during the Eisenhower administration. It's very manual.

Investigators have to go in person and write notes, rather than use tablets. They have to go through the mail to send a request to get an education check. They physically have to visit a person, versus using social media or other access points to get things done, when today's technology allows for a much more rapid way of getting decisions done without, in our view, changing the trustworthiness of the individual. That can be done greatly and significantly.

I think the second part is that people want to walk through the process and make sure in this environment that people are trustworthy, and the timeline is taking longer because the assurance is needed and it's impacting the mission. We want to make sure time is factored in to the decisions or we will not be able to defend the digital walls from outside threats.

So I think it's the process and I think it's the need to have a more risk-based review against the mission requirements and the need to protect our Nation combined from insider threats.

Thank you.

Chairman BURR. Ms. Chappell.

Ms. CHAPPELL. I would echo his comments, but I would say it a little different. We are a Nation blessed with very high technology. We are just not using that technology in this process.

We talked about people having to physically go and meet with people. I think that, while that gives us some level of assurance, I think the continuous evaluation gives us a whole other level of insurance, and we should use that technology to give us more confidence in the results as well as decrease the time lines.

Chairman BURR. Basically, what you've told me is I put more effort into understanding who my interns are than potentially the process does for security clearances, because you go to the areas that you learn the most about them, which social media is right at the top of the list. I can't envision anybody coming into the office that you haven't thoroughly checked out everything that they've said online, which is to them a protected space. And we all know that it's a public space.

I think what you've done is you've confirmed our biggest fear, that we're so obsessed with process and very little consumption of outcome. I think that's how you get a backlog. And you can let that continue to be the norm and nobody's outraged.

What's the single change that you'd make to the security clearance process if you only were limited to one?

Ms. Farrell.

Ms. FARRELL. I think prompt action. This needs to be, as some of the colleagues here have said, a high priority. We keep hearing the words "top leadership." There was top leadership involvement when the DOD program was on the high-risk list from 2005 and 2011. We saw that top leadership driving efforts from OMB, DOD, the DNI. That's what we're going to be looking for as we measure their progress going forward to take actions to come off of the high-risk list: top leadership actions engaging with Congress to show that reducing the backlog is a top priority, as well as taking action to communicate that to the other members of the personnel strategic clearance community, as well as my colleagues on the panel here. But leadership is desperately needed in this area.

Chairman BURR. Mr. Phillips.

Mr. PHILLIPS. Sir, immediately it's funding. But putting that aside, I think long-term it's one uniform standard and reciprocity. It's a big deal.

Chairman BURR. Ms. Chappell.

Ms. CHAPPELL. I would say continuous evaluation monitoring, doing that on a continuous basis, which reduces the periodic investigations, which allows those people to spend more time reducing the current backlog.

Chairman BURR. Mr. Berteau.

Mr. BERTEAU. Do I get to use the three that they've already used and add a fourth one to it?

Chairman BURR. Absolutely.

Mr. BERTEAU. Because I do think reciprocity is the top priority in that process. But I think using technology, not just in continuous evaluation, but in the investigations process itself. I've had a clearance for nearly 40 years and the guy still shows up with a pencil and a piece of paper and makes sure that the questions I've entered into the form, which are in many cases the same answers I've given for almost 40 years, are still what I believe, and he writes it down with a pencil, and then he takes it off and puts it into a computer system that's not compatible with anybody else's computer system. Let's get the process down to where we're using 21st century technology.

Chairman BURR. My thanks to all of you for your candid responses, and I say that with the full knowledge of knowing that this issue is a multi-committee jurisdictional issue on the Hill. So we've got just as much to fix up here. I think some of the things that you have expressed are the results of no coordination legislatively, and I think we're going to take that at heart as we move forward.

Vice Chairman.

Vice Chairman WARNER. Thank you, Mr. Chairman.

Again, thank the panel for their I think accurate description. I think it's really important that we all think about this, and I appreciate the GAO putting this on the national security high risk, because not only are we wasting taxpayer dollars by hiring individuals that then cannot do the work they're hired to do or, as some of the industry panels indicated, will then not take a job because of the clearance process—and I think we particularly lose on the government side, where people would come in and serve at a much

perhaps lower salary than they would on the industry side, but because of the security clearance.

And I really appreciate, Mr. Berteau, your comments about the use of technology. If you can give—we'll start with you and at least start through our industry colleagues—other specific examples on how, on a technology basis, we can improve this process that, again, candidly, hasn't been significantly updated since the 1950s? Mr. Berteau, do you want to start, and then we'll go down, specific technology examples?

Mr. BERTEAU. I think that the entities that are involved in both the front-end, the scheduling process, the investigation process, and the adjudication process have all identified a number of places where they can bring that technology to bear. The greatest advantage I think we can take is to have integrated data across the government, so that in fact we've got access to everything everywhere.

The intelligence community has made more progress here than much of the rest of the government has had. But they also have the advantage of scale. The scale is smaller in they've got the funding and resources and the motivation to do that. I think we could give you a list of specifics that you could consider as you go forward as well.

Vice Chairman WARNER. Ms. Chappell.

Ms. CHAPPELL. I would say, going back to my previous answer, that continuous evaluation. A lot of this data that we go personally ask these people, that are the same questions we've asked for 40 years, that data, a lot of that data is available in open source, that's available to anybody. It's a matter of public record.

Vice Chairman WARNER. Rather than having somebody send a letter to an educational institution—

Ms. CHAPPELL. Correct.

Vice Chairman WARNER [continuing]. Or make personal visits. Could you drill down for a minute on continuous evaluation, at least for SECRET clearance level? It seems like it would make so much sense.

Ms. CHAPPELL. If you go down through and look for bankruptcy, if someone files for bankruptcy that's a matter of public record, for example. We can get that through just trolling the web.

Vice Chairman WARNER. Without an agent going to a courthouse—

Ms. CHAPPELL. Without an agent having to physically travel and then go take that information down with pencil and paper, for example.

Vice Chairman WARNER. Thank you.

Mr. PHILLIPS. Sir, I'll give you two examples and one desired solution. We have—one of my fellow CEOs has a contract where he has people in the Green Zone doing DOD work and they cannot support in that same limited space, work for another department because they have to file an entire process to get a clearance in order to do that and it's totally separated. So right across the street, they can't go in and support, with a confined environment, for two agencies to do the same thing in a very difficult environment.

Separately, we have a separate CEO who's got a contract that does work, that the information flows to both DOD and somewhere

in DHS. That individual has to fill two applications and go through two investigations to do the same job.

Industry quite often utilizes public systems that we share, that are cloud-based, multi-layer security, and we pay for it for ourselves. We control the data ourselves. But it is a uniform set of systems that are available. We can make that decision.

I think establishing a uniform system that every agency that has funding can fund into and do its own processing would be very beneficial, because then those accesses would be available at the same security level for people to know what's happening and that cross-over and that reciprocity could happen just like that.

Vice Chairman WARNER. I think, just before I get my last question in for Ms. Farrell, we need both reciprocity and portability. One of the things, and I think one of the reasons why ODNI Coats, this is so high on his priority, he lived this experience. Having sat on this committee for a number of years, being accessed to all types of information, the amount of—when he left the Senate and a few weeks later when he was then appointed head of ODNI, because there was that short-term gap, he had to go through a whole new security clearance process. That was pretty absurd.

Ms. Farrell, one of the things that I'd like you to comment on is: What I've heard constantly is, typically from the government side, everybody knows it's a problem, but this, like much of G&A in terms of operations, gets pushed to the back of the line. How do we make sure that we as Congress can, with appropriate oversight, make sure that agencies don't take their security clearance budget and push it to the back of the line? Everyone acknowledges this is an issue and a problem, but these are dollars that don't ever seem to be prioritized because they are not sole to mission.

Ms. FARRELL. I think this is something that goes back to the top leadership, from the deputy director for management at OMB, who is the chair of the council that's driving the reform efforts and overseeing the reform efforts, and to send a message that this is a top priority, whether it's reducing the backlog or fully implementing CE, and resources will be provided and the agencies will follow suit.

If I may comment on the technology, the continuous evaluation is an area that you've heard has great promise, that could help streamline the process, perhaps be more efficient. As I noted, the efforts to implement continuous evaluation go back to 2008, with full implementation expected in 2010, and that has not happened.

We are encouraged by the DNI's recent directive expanding on what CE is. However, we still don't really know what continuous evaluation is going to comprise and when it's going to be implemented. I think that's going to be a huge step, for the DNI to develop a detailed implementation plan of when the phases are going to occur and the agencies' expectations to implement that.

Vice Chairman WARNER. Mr. Chairman, I'd simply say I think Ms. Farrell's comments are pretty clear. We've got to start at the top. I'm disappointed, and I know you are as well, that OMB did not take our invitation to actually participate, since they chair the inter-agency council to try to move forward on this. I think we need to get them back in at some point.

Thank you, Mr. Chairman.

Chairman BURR. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

All three of our private sector witnesses today have been understandably very critical of the unacceptable flaws in the government's clearance process and the lack of a system of continuous evaluation. Inadequate funding has been mentioned. I want to turn the question around.

There have been three widely reported, serious breaches at the NSA and all three involved contract employees. It is evident that relying solely on a moment-in-time snapshot of an applicant's security profile to determine clearances and secure our information and facilities is simply not working. I've been a strong supporter of moving to continuous evaluation, particularly following the Navy Yard shooting.

But my question for each of the three of you is: What responsibility do contractors have to identify and report changes in employee behavior that may indicate a vulnerability and should trigger a review of the security clearance? In at least one of the widely reported incidents involving NSA, the employees who worked with the individual were very aware of the issues that should have triggered a review of his clearance.

So I understand the role that government has and that we need to do much better. But what is your role, particularly in light of those three serious breaches, all involving contract employees? Mr. Berteau, we'll start with you and then move across.

Mr. BERTEAU. Thank you, Senator. Those are critical questions, obviously.

I make three points there. Number one, I know you know this, but the process is the same, whether you're a government uniformed personnel or a government civilian or a contractor, in terms of the investigation and adjudication process.

Senator COLLINS. I do know that.

Mr. BERTEAU. And I think that the issues that we've been talking about today, some of the process fixes actually incorporate in them a number of the lessons learned from those very examples that you cite here, continuous evaluation being the key piece of it here. So I think that a number of the proposals, some of which are already being implemented, although, since we don't get visible insight into that, we don't know how far that implementation is—that's a question for your second panel—are designed to address those very same problems.

But I think there's a third piece. In the examples that you cite, you're right, there are individuals inside who do this, but from the company's point of view these are people working inside a government facility, and we frequently don't get the information about, or our member companies don't get the information, about the employee that the government itself has.

So there's got to be greater collaboration and cooperation between the government oversight mechanisms and the contractor oversight mechanisms. This is where personnel issues, privacy issues, security issues, and contract issues come together, and we've got to design it that way up front in the contract itself.

I think we're very capable of doing that. We know how to do it. We just don't do it every time.

Senator COLLINS. Ms. Chappell, what is Raytheon's responsibility?

Ms. CHAPPELL. We have a responsibility to train our employees. Yearly, we go through an employee training series that's mandated across all of our employees. In some cases where we have employees sit at government facilities, they take yet a second round of training that is required by the government customer as well. So that's two.

The second thing we do is what we call "user activity monitoring." When you log on to a Raytheon system, it's very clear to you. It says right there on the screen that your activity is being monitored while you're on those systems. So we have a process where we use analytic-type of capabilities to look at what people are doing on the systems, to monitor their behavior, to look for things that are outside their normal patterns or their normal work scope. That data is then provided to our security operations center, and then if it triggers an alert we go through an investigation process.

If someone comes through and says there's something going on with an employee, we trigger an investigation.

Senator COLLINS. Mr. Phillips, very quickly: If ManTech has a group of employees working for the government on highly sensitive information and many of the employees of that group think that one of the employees has gone off the rails—developed a drug problem, has financial problems—what specifically happens?

Mr. PHILLIPS. Specifically, ManTech has an insider threat program that identifies high-risk employees, and once those individuals, whether they hold a position of trust, we see a behavior that we need to track, it rolls into a process that's controlled through our senior security executive, coordinated with our human resources and legal department, and overseen by myself, with board updates every quarter to make sure that we are tracking those individuals that have been identified from an insider threat perspective.

We report that information to the government. We also start monitoring their overall behavior, where appropriate, to make sure that that individual's behavior doesn't provide additional risk of harm to our employees or Federal employees or potentially increase the position of trust or breach of data to the government.

Additionally, we spot-check people coming out of our own SCIFs for data. We want to make sure that as a partner we're doing everything we can. The only thing we suggest: We have to share information better about individuals who hold positions of public trust.

Senator COLLINS. Thank you.

Chairman BURR. Senator Feinstein.

Senator FEINSTEIN. Thanks very much, Mr. Chairman. I'd like to follow up on Senator Collins' questions to you, Mr. Phillips. Specifically, what changes have been made by your company in the wake of Snowden and Martin?

Mr. PHILLIPS. Ma'am, since then we've increased our insider threat process. We do more training—

Senator FEINSTEIN. From what to what? If you could be specific here, that would be helpful.

Mr. PHILLIPS. Sure. I think all of government is moving towards mandating industry be a partner in this process. We already had a process in place, but what we're doing is we're making sure that every behavior—we physically go to our program managers and we tell them: If you or your employees see a behavior, we need to see it, we need to know.

Senator FEINSTEIN. Well, where did you miss with Snowden?

Mr. PHILLIPS. We did not—we did not have that event within our framework. The Snowden component or something like that specifically is the employee is on a Federal facility, and a company cannot access the government's data to see the behaviors. They have to be visually seen by the people around that individual. We need to better share information.

Senator FEINSTEIN. Isn't that an important point right there?

Mr. PHILLIPS. Yes, ma'am, it's very important.

Senator FEINSTEIN. Because these were big events, and it's very hard for us to know the background and how it happened. So could you go into that in a little bit more detail?

Mr. PHILLIPS. Anything that is on a secured government network or secured government facility is controlled by the government, regardless of whether it's a military, Federal employee, or contractor. The information flow around that is fairly limited, for security reasons, but also personnel reasons.

The information-sharing program that we think is best long-term, aligning those who have positions of public trust and have agreed to that, with the appropriate protections of privacy, if they are on a network having classified information, how do we better collectively track the behaviors and actions of the individual so that we as a contract community can take the appropriate actions on that staff.

Senator FEINSTEIN. Well, as you know, both these employees were contract employees with NSA. How closely have you reviewed the procedures and have you made any recommendations to NSA?

Mr. PHILLIPS. Ma'am, the agency has gone through significant review and we as a contract community are adjusting to meet their required additional standards to be responsive to the risks that they may have seen within their review.

Mr. BERTEAU. Senator—

Senator FEINSTEIN. Well, maybe somebody can add to that, because that's a very general statement and it doesn't leave me really with any answer.

Mr. BERTEAU. Senator, if I could sort of add a little bit to that, not necessarily the Snowden case or the Martin case, but we see time and again a situation where the government will tell a contractor, this person is no longer suitable, take them off the contract, but they won't tell us why. They won't tell us what behavior has occurred, what has motivated them to do that.

So we're left trying to figure out what happened here, without the information from the government.

Senator FEINSTEIN. How often does that happen?

Mr. BERTEAU. I don't have a count of how often, because there's no database to do it. But I hear about it more than once a year, and I probably don't hear about it a lot of times that it does hap-

pen. So you have individuals, and it may be that the company releases that individual, but the individual can go somewhere else.

So that information-sharing that should occur here between the government and the contractors involved, cutting across the security domain and the personnel and human resources domain, has got to be improved.

Senator FEINSTEIN. Because of the 4,080,000 national security clearances, the contractors hold almost a million, 921,065 of those. That's a big constituency out there. Because it involves the defense companies, of which Raytheon is a California company that I'm very proud of, that's one of them, it seems to me that the private sector has an increased responsibility, too.

Ms. Chappell, how do you view that? How does Raytheon specifically view an increased responsibility?

Ms. CHAPPELL. I think we have stepped up our training requirements around this area; more sensitivity to what has happened and making people aware. When it's on our own networks, we have control on what we monitor and where we see risk and how we escalate that and where we investigate.

I think Mr. Berteau is very correct in that there needs to be better partnership. When our employees sit on government facilities and use government networks, there needs to be more information-sharing on what we can do jointly, because we don't have the ability to monitor those networks. So I think any insight we can get there is most helpful to us in making sure we adjudicate through our workforce.

Senator FEINSTEIN. Right. On pages 7 and 8—I'm looking for your written remarks and can't find them at the moment. But you make some good recommendations. Could you go into them for us, please?

Ms. CHAPPELL. On the written?

Senator FEINSTEIN. In the written, and let me find it.

[Pause.]

Ms. CHAPPELL. Just one second, please.

Senator FEINSTEIN. Yes. I'm sorry, Mr. Chairman. I'm sorry. My hand slipped and I lost the—

Ms. CHAPPELL. I think that was around the one application.

Senator FEINSTEIN. That's right, the fundamental reforms. And you began with the clearance backlog of 300,000 and the one application, and it runs through—now, this is more than a decade, as you point out, since they were first proposed. But to make immediate progress, you say "Raytheon encourages the government to prioritize and set incremental milestones for implementing government-wide reciprocity, continuous evaluation, and information technology reforms."

Can you be more specific about that?

Ms. CHAPPELL. On the one application, that is the one, standardized—one standardized, one digitized, so it's available, it can be shared across organizations. You don't have to fill that out more than once. One investigation, to make sure that, whether it's a DOD investigation, an Air Force, Army, or a CIA investigation, that that's the same investigation, that had the same standards, the same views on risk. Those can be shared across the different agencies.

One adjudication of that, so instead of having different adjudications you have one set of adjudication processes, one set of risks that that adjudication is based on, so that then that clearance can be agreed to and can be recognized across the different agencies. Then clearly, just the one clearance, to make sure that that reciprocity moves across organizations.

So I think they're pretty fundamental, pretty standard, pretty simple processes: one application; one clearance process; one adjudication, recognized by all.

Senator FEINSTEIN. Do you think that would make a difference with the 4 million and the 600,000 each year?

Ms. CHAPPELL. I think it would make a huge difference, because not only would it streamline the original investigation; you're not re-investigating the same people over and over, and the resources required to do the re-investigations would be focused on the backlog.

Senator FEINSTEIN. Thank you.

Thank you, Mr. Chairman.

Chairman BURR. Mr. Berteau.

Mr. BERTEAU. Mr. Chairman, if you would indulge me for just one added point. Senator Feinstein's line of questioning is really critical here. One thing I think is important to put on the record: The member companies for PSC and companies like Raytheon and ManTech are very limited in their ability to get information out of the government of the status of the investigation and adjudication that's going on with the people that they've submitted into the process.

If Kevin Phillips or Jane Chappell calls the government agency that's doing that, what they will likely be told is: We can't tell you anything; go talk to your contracting officer representative, who then has a process they have to go through internally, not the speediest of processes, and they may or may not get you an answer back.

We see cases where a decision has been made and not communicated to the company, in some cases for more than six months. So there is a lot that has to be done here in terms of improvement of the communication back and forth. I think the oversight role of this committee in encouraging that and getting visible results of that from the agencies involved would be very helpful.

Senator FEINSTEIN. Thank you very much. Would you be willing to write something up as to what both of you or three of you think would be the specifics and send it to the Chairman?

Mr. BERTEAU. Absolutely.

Ms. CHAPPELL. Yes, ma'am.

Senator FEINSTEIN. Thank you. Thank you very much.

Chairman BURR. Thank you, Senator.

Senator Blunt.

Senator BLUNT. Thank you, Chairman.

Ms. Farrell, in your testimony you talked about the 12 recommendations I think you made to the Director of National Intelligence. How many of those did they accept?

Ms. FARRELL. For the majority of those we directed to the DNI, they did not comment whether they agreed or disagreed. So we

don't know if they're going to take action on those recommendations or not.

Senator BLUNT. I think I must have read your testimony wrong. I got the impression that they had concurred with some, but not all.

Ms. FARRELL. They did concur with some.

Senator BLUNT. What does that mean, they concurred with some, but didn't accept them? I'm getting a thesaurus out here to figure out what that means.

Ms. FARRELL. They concurred, for example, with taking steps to develop a continuation—continuous evaluation policy and implementation. But on other actions they disagreed; they thought that they had already had things in play and that no more action was necessary.

Senator BLUNT. Which of the 12 things you recommended do you think would have the most impact on achieving the goal we want to achieve here?

Ms. FARRELL. For today, I think it would be the implementation plan for continuous evaluation. But I also have to note that there's been a lot of discussion about reciprocity, and reciprocity is statutorily required by the Intelligence Reform and Terrorism Prevention Act of 2004. So by that Act, agencies are supposed to honor investigations that are conducted by an authorized provider, as well as adjudications from an authorized adjudicator.

There's always certain exceptions, but reciprocity is in statute. It just hasn't had guidance so it could be implemented.

Senator BLUNT. And continuous evaluation, Ms. Chappell, how does that relate to—you're saying a lot of the same things: continuous evaluation; using open source data or data that's already been collected, rather than going through that process again. Do you want to talk about that just a little bit more?

Ms. CHAPPELL. What we're saying is, instead of waiting from day one when you're given your clearance to year five and having no investigation between that period, and then doing your periodic investigation with sending people out, traveling around the country, doing your investigation, all through that time period to continuously monitor data to see if there is any adverse data concerning that person and do you need to start—is that person of higher risk and do you need to pay more attention to that person sooner, rather than wait the normal five to six years for that background investigation.

Senator BLUNT. If that person, like Senator Warner mentioned about Senator Coats and that brief space, when someone has moved on to another job and is coming back, do they have to go through the whole clearance process again? They have to re-submit again everywhere they ever lived?

Ms. CHAPPELL. Yes, sir.

Senator BLUNT. Don't we have all that somewhere if they've been cleared once?

Ms. CHAPPELL. Yes, sir.

Mr. BERTEAU. Senator Blunt, I've lived in the same house for the last 29 years. I've had the same neighbors on each side of me for the last 29 years. Both are former government employees with suitability determinations and clearances as well. Every time I fill that

form out, it's the exact same information as it was the time before, the time before that, and the time before that. It's already in their databases. They just make me do it again.

Senator BLUNT. Does anybody have a reason that would justify why you'd have to do this again, if the government's already collected all this?

Mr. BERTEAU. There's an old saying—Eric Sevareid brought it out of World War II with him—called “The chief cause of problems is solutions.” And in almost every case, these elements of the process that are built in here was a fix to a previous problem. What we've never done is the kind of end-to-end analysis of what actual result are we trying to get out of this and how do we design a process that gets that result.

I think what you'll hear from the second panel is some of the efforts both at the National Background Investigations Bureau has under way and that DOD is developing a plan for, would take advantage of some of that opportunity. It's just going to take a long time, and we'd like to see it speeded up.

Senator BLUNT. Mr. Berteau, one other question. Are small companies treated differently when it comes to getting their employees cleared?

Mr. BERTEAU. Unfortunately, they go through the same process, and I think they have an added disadvantage. If a company has a substantial amount of work in the government, they may actually be able to make a job offer to a new employee and say: We've got something we can have you do while we're waiting the year or two years it takes to get this clearance through the process. It's very much harder for a smaller business, who doesn't have the business base or the overhead capacity to be able to do that. So you make a contingency offer.

Well, if this is a critical skill—let's say it's a cyber security expert who's just come out of college—you're asking them: Put your career on hold for an indefinite period of time, don't get paid, go do something else while you're figuring out what to do here, and then maybe we'll get a clearance at some point in time and be able to hire you.

This has two negative advantages. One, it's going to reduce the number of people who are going to want to do that. Secondly, they're going to have lost their technical edge, because the system is moving on, the cyber security world is moving along, while they're not working in it. So it has a double impact.

When I mentioned the importance of balancing risk here, there's a risk that we often don't take into account. It's not just the risk of awarding a clearance to somebody who ends up doing something wrong. There's a risk to government missions and functions in every step of the way by not doing it in a timely way and not by having the best and brightest people on board to do that. That's got to be part of the calculus. Nobody documents that.

Senator BLUNT. Thank you.

Thank you, Chairman.

Chairman BURR. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman. It's been a good panel.

I'm just going to ask one question of this panel, and it's for you, Ms. Farrell. It seems to me one of the central issues here is there is a culture where over-secrecy is actually valued and there is no accountability for excessive secrecy. So we end up with four million people with security clearances. I've heard my colleagues talk about the backlog question and I know that that is very important to our companies. But I think to really get at the guts of this issue we've got to deal with this over-secrecy kind of question.

I'd like to ask you: What in your view is the government doing that is most helpful in terms of reducing that four million number, which I think reflects that there are too many secrets out there and too many people are sitting on them. What's the government doing about that?

Mr. PHILLIPS. Senator, I'll start—

Senator WYDEN. I'd like to start with the GAO on it.

Ms. FARRELL. Thank you. That's okay. We have in the past recommended that DOD and its components, the services, as well as the agencies, evaluate their positions that require clearances to make sure that the clearance is required in the first place, and then have procedures in place where they periodically reevaluate those positions to see if those clearances are still necessary. That would be a way to make sure that the requirement is correct.

Most people think that clearances follow people. Clearances don't follow them. They follow the positions.

Senator WYDEN. I want to be respectful. I know of your recommendations. I'm curious as to whether you think the government is moving effectively and expeditiously on actually doing something about it, because this strikes me, this excessive number of security clearances—and your recommendations are always to have these efforts to reduce them—it's been the longest-running battle since the Trojan War. I've been on this committee—I think, with Senator Feinstein, we're the longest-serving members. And I've heard this again and again.

So what is the government doing that is actually effective in your view about this? Not your recommendations, which I think are very good, but what's the government doing that is actually effective now in terms of reducing this number?

Ms. FARRELL. I think the answer is obviously: Not enough, because if they were doing enough in terms of leadership and prompt action, they wouldn't have the backlog that they have or the number of people that you're calling into question.

Senator WYDEN. Okay. I'm going to submit some questions to you in writing as well.

Thank you, Mr. Chairman. I look forward to the second round.

Chairman BURR. Senator Cornyn.

Senator CORNYN. Thank you, Mr. Chairman.

With the hack of OPM a couple of years ago, reportedly by a hostile foreign power, countless Americans have had their privacy violated and their personally identifiable information obtained by that foreign power. Do any of you have any observations or comments about what impact that sort of lack of security for that sensitive information, what impact that's had on the best and the brightest people who we would like to serve in these important positions?

Ms. CHAPPELL. I'll start with that, because my personal information was some of that information that was leaked. Not only my information, but the people who I had down as references, my family members also, their information was also compromised. So I think it's incredibly important that this data is secured and that it goes through the same cyber process that the programs that we support do.

Senator CORNYN. Mr. Berteau, you were saying how you have to fill out the same information on repetitive applications for security clearances. I guess we know that foreign nations have that information, but the U.S. Government apparently doesn't keep it in a place where they can use it without having to ask you each time.

Mr. BERTEAU. Senator, it is my understanding that actually a number of steps have been taken inside the Office of Personnel Management to provide greater security. It's a question I think for the second panel on the status of those steps.

But we also have to recognize that we'll never be 100 percent secure on being able to do that. I think we have to be able to mitigate against that as well.

I would also note that it's not just the central databases that come into play here. It's all the individual things inside each of the agencies as well. We probably are in a situation where we're going to have to be able to recognize and mitigate that as rapidly as possible.

I'm probably a little less concerned about that particular, although I got a letter and my wife got a letter and my kids all got a letter as well. I had the responsibility inside DOD to actually oversee the mailing of those 22 million letters. We mailed out a million a week and it took the better part of half a year to notify everybody.

I note that that mailing occurred about a year and a half after the breach. So we also need to be able to let people know in a more timely way that their data has been compromised.

Senator CORNYN. I don't know anything about that episode that we can be proud of. It just seems to be it would be embarrassing, and obviously people are at risk as a result.

Let me move on to ask about interim clearances, the role of interim clearances. What I don't understand is how can somebody get an—have a sufficient background investigation to get an interim clearance, and what limitations are put on that clearance that would not be available—or that would not apply to a complete clearance, so to speak? And how does that actually work in practice, the role of interim clearances and the background investigations that are conducted to approve those?

Mr. PHILLIPS. Senator, thanks for the question. ManTech is entering its fiftieth year of supporting national security this year, and we have forever had interim clearances being an integral part of moving people into supporting the Federal Government.

As you know, the interim clearance process is a decision that's a government decision. It is not something we as contractors can decide. We have to inform the government and let them make those adjudications.

We have not seen, as a company, issues with the process and how we do it. That said, one of the issues is, because of the time

it takes to get a security clearance, that the interim security clearance timeline is now longer than it was three years ago. So part of our suggestion is we need to move that timeline back so the time people have interim security clearances is narrowed.

The process itself is: The background investigation that is commercial is done on the individual from a company standpoint. The forms are reviewed in total about the employee to make sure that the potential applicant, to make sure that all information is available, so that that government employee or official can make a decision whether sufficient grounds to grant an interim clearance based on those facts, before the more manual investigation takes place.

In our history as a company, less than one person per year has been identified in that sequence as not being supportable to doing security work in the future.

Senator CORNYN. Thank you.

Chairman BURR. Senator Heinrich.

Senator HEINRICH. Thank you, Mr. Chair.

I want to follow up a little bit on those good questions from my colleague from Texas. For those of you in industry—and we'll start with you, Mr. Phillips—how often have you seen a TS–SCI interim clearance? Is that a common thing?

Mr. PHILLIPS. For our industry, it is not uncommon. But as an example, out of our, let's say, 150 people doing an interim status, a vast majority of them are SECRET for the type of work we perform. So I can't compare it to any other application or requirement.

Senator HEINRICH. Got you.

Mr. PHILLIPS. Those who are in an interim SECRET status have already received a SECRET clearance. So it's fairly narrow bandwidth.

Senator HEINRICH. Ms. Chappell.

Ms. CHAPPELL. From my personal knowledge, I don't know of interim clearances on a TS–SCI kind of clearance. Those are usually finalized. From an interim clearance, they're more on the SECRET side. Quite frankly, with the backlog of clearances that we have right now, I think the risk of not doing that and not being able to perform the mission is very high.

Senator HEINRICH. That's very helpful.

Mr. BERTEAU. Senator, in my experience—I don't know if there's data collected on this, but in my experience it was more common in the past. It's a lot less common today, and it has been a lot less common over the last few years. I think it's one of those examples of as we've learned—

Senator HEINRICH. For good reason.

Mr. BERTEAU. For good reason, I agree.

Senator HEINRICH. For the risk that's inherent in that.

Does the government track how many interim security clearances are issued by type, by agency, by personnel type? And is there a process in place to make sure that when that temporary access period has expired that there's a review to say, red flag, this has come to an end, we should look at this person again?

Ms. FARRELL. I take it you want me to answer that?

Senator HEINRICH. Yes, if you could.

Ms. FARRELL. That information might be at the agency level in their case management systems. But it was not at the levels that we looked at in our reviews when we worked with ODNI to collect data on the investigation time as well as adjudication and intake for specific agencies.

Senator HEINRICH. So obviously the whole of government, all the agencies aren't here right now. But that's something we should probably pay a lot of attention to.

Ms. FARRELL. Yes.

Senator HEINRICH. For any of you who want to offer your advice on this: It seems to me from some of the previous testimony that it sounds like continuous evaluation is really important, but it shouldn't necessarily supplant a periodic review; it should supplement a periodic review. Is that your view across the board, and any of you who want to offer your advice on that, I'd be curious.

Mr. PHILLIPS. Yes, sir, I'll start. Technology allows for continuous evaluation where ten years ago you really couldn't do it. So start with that. It's a very good thing to utilize and over time it will become a more and more important thing because it can be depended on, and in fact it will identify things, not five years from now, but along the way between now and five years. So we consider it a use of technology to the benefit of national security.

Within that framework, depending on the level of trust on the CE process itself, the periodic re-investigation percentages can come down. I don't see it going away, but it can be like the IRS: We're going to audit you every once in a while, versus everybody 100 percent.

Senator HEINRICH. So the interim period between those periodic reviews might get longer based on a lower rate?

Mr. PHILLIPS. And there can be sample periodic re-investigations to help inform and make sure the process is working.

Ms. CHAPPELL. I would just say it slightly different. I would say it focuses where the higher risk is and where you should focus periodic investigations on.

Senator HEINRICH. Ms. Farrell, I want to ask you one more question before I run out of time here. You testified that the National Background Investigation Bureau is trying to decrease the backlog, but it has huge challenges in actually achieving this. One of the stories I've seen that I'm intrigued by that seems to be working is NBIB is taking and deploying teams of investigative personnel to specific sites for a two-month period where they'll set up shop in a dedicated work space, and they try to crank through some of the most time-sensitive clearance investigations without the back-and-forth that we heard about in some of the testimony, the travel, the inefficiencies.

This is happening right now at a couple of labs in the DOE labs in New Mexico. It seems like a rare good-news story of increasing efficiency. Do you agree with that, and is this a model that we should be potentially applying more broadly?

Ms. FARRELL. What we found during the review was that the Bureau did not have the capacity to carry out their investigative responsibilities and reduce the backlog. The Bureau looked at four scenarios of different workforces to try to tackle this backlog. They looked at just if things stay the same; they looked at very aggres-

sive hiring of contractors. They decided that it was not feasible for the plan where they would put so much emphasis on the contractors; and the two plans that they did look at, the backlog still would not be reduced for several years.

There hasn't been a selection, though, of which plan they're going to go with in order to reduce the backlog. So that is going to be key. You can't reduce the backlog if you don't have the workforce.

Senator HEINRICH. I don't disagree with you. I don't think you answered my question. But my time is over, so we're going to have to move along here.

Chairman BURR. Senator King.

Senator KING. Mr. Berteau, first I want to congratulate you because you made the key point of this whole hearing for me. It's the opportunity cost that we should be talking about. It's the good people lost. That's what brings me here today, because I know too many stories of people who just gave up, who spoke Arabic, who had visited, lived in the Middle East, and because of that couldn't get their clearance. It was a kind of Catch-22, and those are the very people that we want.

So I think that's what we have to keep focusing on, is those immeasurable people lost, the opportunity cost that has made this such an important inquiry.

Ms. Farrell, who's in charge? If John McCain were here, he'd be saying; Who can we fire? Why is this—this is a pure management problem, it seems to me.

Ms. FARRELL. This is a management problem, and I referred to the Performance Accountability Council because those are the principals that are in charge of implementing the reform efforts and overseeing—

Senator KING. Who is on that council? Who are the people?

Ms. FARRELL. That's the deputy director for management at OMB. It's the director for national intelligence, who is also the security executive agent, which means that person sets the policy across—

Senator KING. My problem with that is any time you have a council the term "all of government" has been used. I'm sick of that term. That means none of government. That's what people say when nobody's in charge.

Is there one person who has the responsibility for fixing this problem, and who are they?

Ms. FARRELL. I would point to the chair of the Performance Accountability Council, because that person does have the authority to provide direction regarding the process and carry out those functions.

Senator KING. Is that person going to be here today, do you know?

Ms. FARRELL. I believe that person declined.

Senator KING. Well, that's kind of ridiculous, isn't it? So the one person in the government that's in charge of this issue, that's a very important issue, isn't here because—did they have to wash their hair? What's the deal?

Ms. FARRELL. I can't speak for OMB, sir.

Senator KING. Well, that's really—that's really disappointing. Okay.

Again for you, Ms. Farrell: The private sector has moved on from the 1940s style of doing these things. The financial sector does it much more quickly. Have we tried to learn from them? Has there been any effort to study how the financial sector does this, for example?

Ms. FARRELL. I do believe that the Executive Branch agencies have reached out to the private sector. After the Navy Yard shootings, they did a 120-day review. They identified challenges within the process. There was a lot of coordination with government and non-government. Many of the recommendations that they had were recommendations that they had been working on, though, since the reform began back with the passage of the OFAC.

Senator KING. Well, I would hope that we could try to learn something from the private sector, because they appear to be doing this much more efficiently.

Mr. Berteau, a technical question. The people who come to interview you to redo these security clearances, do they carry a clipboard?

Mr. BERTEAU. I think they do, sir, and I think it's legal-sized, so that it has more room.

Senator KING. To me, the clipboard is the sign of not being in the 21st century.

Mr. BERTEAU. I'm sorry to hear that. I actually own a couple of clipboards and I occasionally use them.

[Laughter.]

Senator KING. I used to say it was the universal symbol of authority. But if you go into a hospital and they hand you a clipboard, they're seeking data from you that they already have somewhere else in their system.

Mr. BERTEAU. That's certainly been my experience, yes, sir.

Senator KING. That's the point I'm trying to make.

Mr. BERTEAU. And I think that's certainly within my experience.

If I could add something on the "who's in charge" thing. I think you've hit a very key point here. There are divided responsibilities and some of those divided responsibilities actually spill over into the question that Senator Wyden raised about really focusing on—we've been focusing entirely on the supply side of this equation: How do we actually move people, put them in the process, and put them in a clearance?

There's a demand side of this equation as well. Actually, operating under the authorities granted by this committee, a previous DNI did a substantial reduction in the number of billets that required a clearance. I don't remember the exact number. I think it was something around 700,000 that they eliminated the requirement for a clearance.

If you could do one thing to reduce the backlog, getting rid of the demand would be the one thing. But what we've seen over time—and this is back to your question of who's in charge—is other responsibilities, responses to other incidents, the Navy Yard shooting, for example. When I was back in the Defense Department, what I saw was in fact you had to practically get a clearance to get a pass to get on the base, even though there would be nothing you would ever touch in the way of classified material once you got on. That's

out of an abundance of caution of we don't want somebody to be able to come on the base with a gun and be able to kill our people.

There are other ways to do that, I would submit, than expanding and lengthening the background investigation process, and continuous evaluation using 21st century technology is the key to that. The government has to do that.

Senator KING. I'm running out of time, but I want to ask one more question. Am I correct in taking from this panel that these security clearances are not transferable, they're not portable? You get one in one agency and if you go to another agency you have to start all over?

Mr. BERTEAU. It varies. There are parts of the government where—

Senator KING. That's a disappointing answer.

Mr. BERTEAU. There are places where the portability is pretty robust, and it doesn't take very long, sometimes maybe only a day or two. There are others, Department of Homeland Security, for example, where I believe the average to move from one to another is almost 100 days, within the same Department, under the same Cabinet officer.

Senator KING. I'm sorry. They already—I can't believe what you just said. You mean a person within the Homeland Security Department who has a clearance, to move from one job in Homeland Security to another job in Homeland Security takes 100 days?

Mr. BERTEAU. Yes, sir. And it could even mean that a contractor sitting at the same desk, moving to a different contract, has to go through a new process.

Senator KING. That's preposterous.

Mr. BERTEAU. Yes. I think that's a very nuanced and subtle word to use for it, yes, sir.

[Laughter.]

Senator KING. Thank you, Mr. Chairman.

Chairman BURR. Senator Lankford.

Senator LANKFORD. I want to be able to pick up where you just left off, because that was actually one of my key questions, was about the reciprocal agreements for clearances. What's holding that back that you have seen at this point of why the agencies don't trust each other enough to be able to handle clearances? Is this an issue of "No, our people have to be able to do it; I don't trust your people" or not a common set of standards?

Mr. BERTEAU. It's probably a combination of a host of things. I think the three things that you could do about it: number one is force a set of common standards that are a starting point. Even within DHS, for example, there's only statutory standards for one part of DHS. It happens to be the Transportation Security Administration and that's a result of a different line of Congressional inquiry.

Setting common standards and then reviewing and making sure that the deviations or the additions to those standards are minimized and they have to be approved by the top leadership. So there's a leadership question. That's the second piece that comes in.

Senator LANKFORD. So what is currently not aligned right now on our standards?

Mr. BERTEAU. I think it tends to be more in the civilian agency side than it does in the intel community and the Defense Department side. I think there the standards are a little clearer. But they're not clear to us. We as contractors often don't know what standards are going to be applied to the individuals.

Senator LANKFORD. Can I push "Pause" in there real quick?

Ms. Farrell, what would be the—could we get a list from anyone to be able to say, where are we deviating in standards, civilian, defense, contractors, whatever it may be?

Ms. FARRELL. The standards should be the same. There's Federal investigative standards. They do not differ by category of the workforce. Federal adjudicative standards are also supposed to be uniformly applied.

There are no—there's no data, there's no measures about the extent to which reciprocity works or does not work. This is something that we have recommended before, that there should be a baseline to determine whether or not reciprocity is working, and if it's not working then to be able to pinpoint the issues that are being discussed as to why it's not working.

Many years ago, it was believed that reciprocity was not working because agencies did not trust the quality of the investigations that someone else had done. But we don't know what the issue is today.

Senator LANKFORD. So when I meet with the chief human capital officers of the agencies, affectionately called "CHICOs," those folks tell me that one of the key areas that slows down Federal hiring, which now is over 106 days on average across the Federal Government, is this reciprocity issue; that this issue is not only slowing down and creating a bigger backlog and, as you mentioned, Mr. Berteau, a demand issue, that we've got to be able to go through this again and again and again for the same person, and an incredible nuisance for the person that's actually going through it for the third time, but it's also decreasing our Federal hiring and the speed of actually getting good people on the job.

So what I'm trying to drill down on: Is this an issue of agencies having a standard across all the Federal Government, but they add one more and because they've added one or two more than we've got to redo the whole thing, rather than trusting somebody else has already done it and we're going to just do this one additional check? What is it?

Ms. FARRELL. This is an issue of the DNI not issuing the policy on how reciprocity should be applied.

Senator LANKFORD. So reciprocity is already required?

Ms. FARRELL. It's required by statute.

Senator LANKFORD. So it's required, but you're saying it's just a matter of releasing a document from ODNI or from anyone else on how to actually apply what is current law?

Ms. FARRELL. Because current law does state "with certain exceptions." So it's up to the DNI to know what those certain exceptions are, so that the agencies will be able to determine if an investigative can be accepted as well as an adjudication.

Senator LANKFORD. Because at this point who is determining what the "certain exceptions" are?

Ms. FARRELL. The agencies.

Senator LANKFORD. So they can determine “I don’t trust them” or “I don’t know them” or whatever it may be?

Ms. FARRELL. Correct. There’s some guidance out there, but it’s not clear. So the DNI is working on a reciprocity policy and we are waiting for that policy to be issued.

Senator LANKFORD. What is the key information-gathering that is needed? You also mentioned this as well, about individuals getting onto a facility that may not need security clearances, because they’re not going to touch documents, they’re not going to see elements they shouldn’t be able to see. What is the lower level that could be done faster, to make sure those individuals can get access and start to do their job, but not have to go through the full check?

Mr. BERTEAU. The DNI does have the statutory authority and responsibility for the standards for security clearances. There’s a second set of standards just for suitability or fitness to be in the job and for the credentials to be able to access the facilities. Those standards are governed by the Office of Personnel Management, not the DNI, and there frequently needs to be a little better mapping between these two.

I think the greatest thing this committee could do is to require regular reporting of a lot more information about this. My experience as a government official is when I’m required to send you a report on how I’m doing, I’m going to pay a lot more attention to what I’m doing than if I’m not.

Senator LANKFORD. Thank you.

Chairman BURR. Do any members seek additional time?

Senator Cornyn.

Senator CORNYN. Can I just ask one more question, Mr. Chairman?

Chairman BURR. Absolutely.

Senator CORNYN. Who in the United States Government decides who is eligible for a security clearance?

Ms. FARRELL. That would be the—usually it’s the agency of the employee that’s applying for the clearance. The agency takes the investigative report and determines if someone is eligible or not.

Senator CORNYN. Thank you.

Mr. BERTEAU. Mr. Cornyn, sometimes there are easy decisions that are made at a lower level within the adjudication process, and sometimes there are harder calls that have to go higher up before a decision is made. This has to do both with the quality and characteristics of the individual case, but also the dynamic of the job and how fast it’s needed and what needs to come into play here. It can actually be calibrated a little bit in terms of who comes into play here.

That’s also a very good question, I think, to ask the government representatives on the second panel.

Chairman BURR. Vice Chair.

Vice Chairman WARNER. Again, thank you, Mr. Chairman, for holding this hearing. This has been something that I’ve been working on for some time. But I think getting more members engaged, because we are losing good people. But I go back to Ms. Chappell’s comments: one, if we can use technology; and two, the closer we can get, at least at the SECRET level, on one standard, one form, one adjudication, and one clearance. Seems like it’s kind of common

sense, and you marry the technology with continuous evaluation and we could make real, real progress.

The good news is there is no—ODNI Director Coats and I think a host of others realize this is a problem. I again thank the chair for holding this hearing.

Chairman BURR. I thank the Vice Chair. I thank all the members and, more importantly, I thank those of you at the dais as witnesses today. Your testimony is invaluable to us.

I walk away to some degree more optimistic than I came, because I think that the biggest issues that you've raised can be solved. And I think this is a question of can we put the right people in a room that understand when you talk about reciprocity, what is that? As I said to Senator King, we shouldn't be shocked. DHS is the comingling of about 37 different pieces that we moved from different areas of government and we put it under a new agency. Given that there was baptism by fire of the Secretary, it's not unrealistic to believe that they still operate like the core agencies they came out of. They just happen to be under a new banner.

So I think these are all things that are doable, but we've got to have the right leadership in the room talking about real solutions. I think that it's the commitment of this committee that we will start and complete that process, and at the end of the day hopefully a year from now you will come back and tell us what great things have happened within government, and it will be because of your testimony today.

With that, the first panel is dismissed and I would call up the second panel.

[Pause.]

I call into session the second panel. I'd like to welcome our witnesses for the second panel. We just heard from the industry on the challenges they face and some potential solutions moving forward. We now have an opportunity to hear from the Executive Branch, their perspectives and their ideas. I understand the daunting task and job before each of you, vetting more than four million cleared personnel and identifying threats before they materialize. It's not easy.

But we can do better than we're doing today. As we continue our dialogue, I hope you'll speak freely, frankly, and think creatively, because this hearing is not only about identifying the problem, but it's about uncovering the solutions.

I want to thank each of you for being here, and I just want to reiterate what I said at the end of the last panel. I actually am more optimistic right now than I was before we started, because I think we've been able to clearly understand the big muscle moves, and I think that putting the right people in the room might enable us to try to overcome some of the challenges and replace it with solutions that we would have full agreement are worth trying or that we feel will achieve a different outcome.

I'm not going to turn to the Vice Chairman. I'm going to turn directly to Mr. Dunbar, who I understand will begin. Then the floor will go to Mr. Phalen and then Mr. Reid and Mr. Payne. Mr. Dunbar, the floor is yours.

STATEMENT OF BRIAN DUNBAR, ASSISTANT DIRECTOR, SPECIAL SECURITY DIRECTORATE, NATIONAL COUNTER-INTELLIGENCE AND SECURITY CENTER, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Mr. DUNBAR. Thank you, Chairman Burr, Vice Chairman Warner, and members of the committee. Thank you for the opportunity to appear before you today to discuss security clearances challenges and reforms. The Director of National Intelligence is designated as the 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, if applicable, polygraph, for eligibility for access to classified information.

The National Counterintelligence and Security Center has been designated as the lead support element to fulfill the DNI's SecEA responsibilities. We're responsible for the oversight of policies governing the conduct of investigations and adjudications for approximately four 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 investigative 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. We have collectively enjoyed some noteworthy progress in security reform, including the development and implementation of multiple security executive agent directives, examples of which I've outlined in my written statement for the record.

However, as recently noted by DNI Coats in his annual threat assessment, today's security clearance process is in urgent need of substantive reform across the entire enterprise. We must quickly and with laser focus identify and undertake concrete and transformative action to reform the enterprise, while at the same time continuing to ensure a trusted workforce.

Underpinning this reform effort must be a robust background investigation process, which enables Federal employees and contractor workforce partners to deliver on agency mission while also protecting our Nation's secrets. When the background investigation process fails or is delayed, mission delivery suffers, the national security is put at risk, and our ability to attract and retain the workforce of the 21st century is inhibited.

Despite the hard work of dedicated, patriotic professionals who are working these issues daily, we have reached a time of critical mass which demands transformative change. Significant challenges for the background investigation program continue to adversely affect government operations. The current investigative backlog is approximately 500,000 cases and the average time for investigating and adjudicating clearance is three times longer than the Intelligence Reform and Terrorism Prevention Act standards.

For the first quarter of 2018, our metrics indicate the fastest 90 percent of TOP SECRET background investigations government-wide took an average in excess of 300 days. This is four times longer than the IRTPA standards and goals. In addition, background investigation-related costs have risen by over 40 percent since FY 2014. The SecEA, the suitability executive agent, or SuitEA, all security organizations, and all impacted industry partners agree that this is unacceptable.

I would like to take the opportunity to provide the committee with more detail regarding our upcoming Trusted Workforce 2.0 initiative. This initiative is designed to address the transformational overhaul I referenced earlier. It is an enterprise effort sponsored by the security executive agent and the suitability executive agent, in concert with our partner organizations, which will bring together key senior leadership, change agents, industry experts, and innovative thinkers to chart a bold path forward for the security, suitability, and credentialing enterprise.

The participants, including all Performance Accountability Council principal organizations, are committed to critically reviewing and analyzing with a clean slate and forward-leaning approach how to accomplish the transformational overhaul which is required. As mentioned in my statement for the record, our Trusted Workforce 2.0 initiative kicks off next Monday and Tuesday, 12 and 13 March, at the Intelligence Community Campus, Bethesda. We look forward to conceptualizing, implementing, and ultimately accomplishing the revolutionary change required across the clearance enterprise. In addition, we look forward to updating the committee on our progress.

The SecEA and SuitEA have committed to transformational overhaul in at least three areas: first, revamping the fundamental approach and policy framework. The current standards are built on decades of layered incremental changes and have not fundamentally changed since the 1950s. We accept the ambitious goal that by the end of 2018 we will identify and establish a new set of policy standards that transforms the U.S. Government's approach to vetting its workforce. Our objective must be to ensure a trusted workforce across government and industry who will appropriately protect vital national security information with which they are entrusted.

Second, overhauling the enterprise business process. The current process is slow, arduous, overly reliant on manual field work, and does not leverage advancements in modern technology and the availability of data.

Finally, we must modernize information technology. Existing information technology constrains our ability to transform fast enough. We must leverage today's technology to connect vital national security processing required and ensure we are well positioned to adopt tomorrow's advancing technology. After more than a decade of incremental policy change, there is still an unacceptable operational burden on government agencies making security and suitability determinations. We owe those dedicated professionals a high-performing process that meets the needs of our workforce and ultimately the American citizen. We are committed to full transparency in these efforts.

Thank you for the opportunity to appear before the committee
and I will be happy to respond to any questions.
[The prepared statement of Mr. Dunbar follows:]

**STATEMENT FOR THE RECORD FOR BRIAN DUNBAR, ASSISTANT
DIRECTOR, SPECIAL SECURITY DIRECTORATE, NATIONAL
COUNTERINTELLIGENCE AND SECURITY CENTER:**

**SENATE SELECT COMMITTEE ON INTELLIGENCE
HEARING ON SECURITY CLEARANCE REFORM**

*Wednesday, 7 March 2018; 9:30 a.m.
Room 106, Dirksen Senate Office Building*

Chairman Burr, Vice Chairman Warner, and Members of the Committee, thank you for the opportunity to appear before you today to discuss security clearance challenges and reforms.

As the Assistant Director (AD), Special Security Directorate (SSD), National Counterintelligence and Security Center (NCSC), Office of the Director of National Intelligence (ODNI), I am responsible for supporting the DNI in his role as Security Executive Agent (SecEA) who, along with the other members of the Security, Suitability, and Credentialing Performance Accountability Council is responsible for leading and supporting security clearance standardization and reform across the U.S. Government. The National Background Investigations Bureau within the Office of Personnel Management (OPM) and the Under Secretary of Defense for Intelligence are partners in the security clearance reform effort, and their representatives are here with me today.

The security clearance process generally involves determining an individual's need for access to classified information or to hold a sensitive position, facilitating reciprocity for existing clearances, or completing a background investigation, reviewing investigation results, making an eligibility determination, and periodically reviewing the individual's continued eligibility.

The DNI, as the SecEA, is responsible for developing, issuing, and overseeing effective, efficient, and uniform policies and procedures governing the conduct of investigations, adjudications, and, as applicable, polygraphs for eligibility for access to classified information, or to hold a sensitive position. The NCSC has been designated as the lead staff support element to fulfill the DNI's SecEA responsibilities, and SSD serves as the primary NCSC element to address these duties. Departments and agencies are responsible for building and executing personnel security programs that are in compliance with these policies and procedures. These responsibilities extend to approximately four million national security cleared personnel.

In exercising the SecEA's responsibilities, we work closely with the agencies responsible for administering national security programs and for conducting investigations, adjudications and polygraphs. This ensures that our policies and practices are informed by those working to protect national security equities and ensure a trusted workforce.

I am going to focus my remarks on the efforts taken to improve the security clearance processes and procedures, reciprocity, and the general challenges we face. In partnership with the Performance Accountability Council, the DNI is committed to transforming the security clearance process, and remains committed to providing departments and agencies with policy direction while continuously assessing ways to improve. We have issued guidance to the community on a wide variety of issues and have achieved a number of successes to this point.

- As the SecEA, the DNI has issued six Security Executive Agent Directives (SEADs) on issues ranging from Security Executive Agent Authorities and Responsibilities to Continuous Evaluation Policy and Requirements, with two planned future SEADs on reciprocity and temporary access, respectively. These policies were extensively coordinated within the interagency and executive branch and represent consensus government-wide approaches to very complicated issues.
- The DNI has successfully launched the Quality Assessment Reporting Tool (QART), which enables the assessment of the quality of background investigations. QART will be used to inform investigative policy and training. To date, multiple agencies have registered in QART, and the tool presently contains over 10,000 investigative entries.
- We have implemented efforts to track and report on the application of security clearance reciprocity, and continue to see improvement in this area. Reciprocal acceptance of background investigations and national security determinations support employee mobility and mission accomplishment — both objectives are critical to ensuring that we use our human resources with maximum effectiveness.

To provide the Committee some metrics on reciprocity, in FY 2017, the core IC agencies — the Central Intelligence Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, and the

National Security Agency — as well as the Drug Enforcement Agency, the Department of Homeland Security, the Department of Energy, the Department of State, the Federal Bureau of Investigation, the Treasury Department, and the United States Coast Guard, reciprocally accepted 95.3% of cases reviewed. While we oversee the security clearance portion of this, there are other elements of the process involved which are beyond the control of security elements (e.g., time from human resources/industry processing to submission to security for determination).

We are actively engaged in modernizing security clearance processes, including implementing Continuous Evaluation (CE), which will conduct automated records checks on a segment of covered individuals between the 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 potential increased investigative and adjudicative workload, complexity of developing the associated technology, and the unknown impact to agency workforce requirements. The initial operating capability of the ODNI CE system is available on the classified network and is performing eligibility checks. Our goal is to deploy a fully operational CE System in 2018 that will be available to all executive branch agencies.

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 with 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 aligns 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.
- 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).

While there have been improvements in some areas, we must continue to focus on the way forward. In a nutshell, the enterprise must become more nimble, agile,

modern, and reflective of advancements in information technology. While we have been engaged in implementing and refining ongoing security reform initiatives, we must continue to pursue opportunities to revolutionize the way we do business. A developing initiative is the “Trusted Workforce 2.0.” Trusted Workforce 2.0 is an enterprise effort, in concert with partner organizations, which will bring together key senior leadership, change agents, and innovative thinkers to chart a bold path forward for the security, suitability, and credentialing vetting enterprise.

While significant reform progress has taken place for our vetting processes, we still have substantial challenges that necessitate concrete and transformative action to directly reshape both the pace and scope of improvement in this arena to implement revolutionary change. We will review with a “clean slate,” and a forward-leaning approach, how we might best effectively and efficiently deliver a trusted workforce in the future. Trusted Workforce 2.0 begins in earnest this month.

Thank you for the opportunity to appear before the Committee. I will be happy to address any questions.

Chairman BURR. Thank you, Mr. Dunbar.

STATEMENT OF CHARLES S. PHALEN, JR., DIRECTOR, NATIONAL BACKGROUND INVESTIGATIONS BUREAU, U.S. OFFICE OF PERSONNEL MANAGEMENT

Mr. PHALEN. Chairman Burr, Vice Chairman Warner, members—

Chairman BURR. Let me thank you, thank you in his absence.

[Laughter.]

Mr. PHALEN. I'll bring my clipboard later.

Members of the committee: My name is Charles S. Phalen, Jr. I am the Director of the National Background Investigations Bureau in the Office of Personnel Management, and I do appreciate the opportunity to appear before you today. NBIB currently conducts 95 percent of the investigations across the Federal Government. The results of this mostly singular supply chain are used by over 100 agencies to make their independent adjudicative decisions. Even those few agencies that have their own delegated or statutory authority to conduct investigations, such as agencies in the intelligence community, rely on our services in some capacity.

I'd like to start by addressing our existing investigative inventory and put some context around the numbers, which have been the subject of much media attention. In 2017 we completed 2.5 million investigations across all our investigative types. As of today, our inventory is approximately 710,000 investigative products. These include simple record checks, suitability, credentialing investigations, and national security investigations.

It's important to note that the top-end number I just mentioned is much greater than the number of individuals waiting for their first, their initial, security clearance to begin working with or on behalf of the Federal Government. Of that total inventory, about 164,000 are either simple record checks that move in or out of inventory daily or are investigations supporting credentialing or suitability determinations. The remaining inventory is for national security determinations or clearances. Approximately 337,000 of those are for initial investigations and about 209,000 are for periodic reinvestigations.

Since we've stood up 17 months ago as NBIB, we have worked to increase our capacity and realize efficiencies. The stabilization of the top-end inventory over the past six months has been attained primarily because we have invested in the necessary infrastructure. We are approaching this challenge on three fronts: First, to recover from the 2014 loss of the USIS contract for investigative capacity, we have rebuilt both contractor and Federal workforce capacity. As of today, there are over 7,200 Federal and contract investigators working on behalf of NBIB. That's good. That's not enough.

Second, our investigative capacity can be significantly enhanced through smarter use of our workforce's time. Through the implementation of our business process reengineering strategy, we have clearly defined the critical process improvements and technology shortfalls corrections needed to support those requirements, and our decisions have been enhanced through better data analytics.

We have improved our field work logistics by centralizing and prioritizing cases, first with agencies, beginning about 18 months ago, and more currently we are beginning to start hubs with industry. We have increased efficiencies of conducting and reporting on our enhanced subject interviews and implemented more efficient collection methodologies by leveraging the powers of technology to discover and gather information, and to free the investigators' focus on those aspects of investigations where human interaction is still critical.

Third, we are fully supportive of the upcoming executive agents trusted workforce initiatives. Our processes today are driven by the existing policies, some dating back seven decades, and we know from our experience that there is much to be gained through this strategic policy review effort, and we are fully behind it.

Underpinning all of this is the planned transition to a new information technology system being developed by the Department of Defense. The National Background Investigation Services, NBIS, will ultimately serve as NBIB's IT system to support background investigations and will offer shared services to the end-to-end process for all government agencies and departments.

NBIB, with the support of its inter-agency partners, has made and will continue to make improvements to the background investigations and vetting processes. As an example, for the past year we have offered our customer agencies a continuous evaluation product that meets today's guidance issued by the Director of National Intelligence for continuous evaluation.

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

Finally, as the Federal Government works to implement the transition of the Department of Defense-sponsored background investigations from NBIB to DOD, we will examine our workforce needs, our capacity, our budget, and work with our partners to minimize disruptions. We have a shared interest in reducing the inventory, taking steps to effectuate the smooth transition of operations, and we have a shared understanding of the importance of this entire process and its ultimate impact on national security.

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

[The 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

**SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE**

on

"Security Clearance Reform"

--

March 7, 2018

Chairman Burr, Vice Chairman Warner, and Members of the Committee, my name is Charles S. Phalen, Jr., and I am the Director of the National Background Investigations Bureau (NBIB) at the U.S. Office of Personnel Management (OPM). I appreciate the opportunity to appear before you today.

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., NBIB's electronic questionnaire, national agency record checks, central clearance repository, etc.). NBIB's systems and processes are aimed at leveraging automation to the greatest extent possible, transforming business processes, and enhancing customer engagement and making our work more transparent to those customers. 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.

**Testimony of Charles S. Phalen, Jr.
Director
National Background Investigations Bureau
U.S. Office of Personnel Management**

--
March 7, 2018

I would like to address NBIB's existing investigative "backlog," which has been the subject of media attention. The decision to terminate our USIS contract at the end of 2014 meant the loss of approximately 4,500 investigators, or 64 percent of our investigative workforce at that time. As we have worked to rebuild that capacity, the investigative workload-in-progress grew substantially. This was a consequence of the limited number of investigators in the field and was further exacerbated by increased demand by customer agencies, resulting in the current inventory. I am pleased the workload-in-progress has stabilized over the past two quarters as a result of building capacity to meet the increased demand, as well as process improvements. In 2017, NBIB completed 2.5 million investigations across all investigation types. As of today, NBIB's inventory is approximately 710,000 investigative products, including simple record checks, suitability and credentialing investigations, and more labor-intensive national security investigations. It should be known that not all these investigations should be considered backlog, as NBIB's inventory includes 160,000-180,000 investigative products that are considered to be a steady state inventory for which NBIB can meet timeliness goals with its current workforce capacity. That number of investigate products, however, 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 164,000 are either simple record checks that move in and out of the inventory daily or investigations that support credentialing and suitability determinations. The remaining inventory is for national security determinations or clearances, of which approximately 340,000 are for initial investigations and 206,000 are for periodic reinvestigations.

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 Security Executive Agent the Office of the Director of National Intelligence (ODNI), the Suitability and Credentialing Executive Agent of OPM, as well as the Department of Defense (DoD), and other customers, to focus our efforts in primary areas, such as increasing our investigative capacity; re-engineering current processes for increased transparency and effectiveness for our customers; and reassessing policies to revolutionize the way we gather and evaluate information.

NBIB has worked to increase capacity and realize efficiencies in as many areas as possible. The stabilization of the inventory has been attained because NBIB has invested in the necessary infrastructure. This infrastructure has been built through contractor and Federal workforce capacities. As of today, there are over 7,200 Federal investigators and investigators who are employees of OPM contractors working on behalf of NBIB, a number we are continuing to grow. In the past year, the Federal and contractor workforce capacity increased by over 25

**Testimony of Charles S. Phalen, Jr.
Director
National Background Investigations Bureau
U.S. Office of Personnel Management**

--
March 7, 2018

percent to address the current investigative inventory. Whenever new investigators come on board, there is a “ramp up” period during which they acquire the experience to accelerate their production. As investigators reach maximum productivity, NBIB’s monthly production rate is projected to continue to increase throughout 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 truism 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 focus has allowed NBIB to reform practices that, traditionally, were manually-intensive and reduce the number of hours each investigator needs to spend on each case. NBIB has improved fieldwork logistics by centralizing and prioritizing cases; increasing efficiencies of Enhanced Subject Interviews and reporting; and using more efficient methodologies by leveraging the power of technology to collect information. NBIB has also increased digitization and automation of 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. This change reduces the number of paper queries that need to be sent and the time it takes to receive replies, as well as reducing the number of files that must be maintained on paper, all of which facilitates faster case closings and adjudications. We also created a Strategy and Business Transformation office to make sure we execute our plan and continue to work toward long-term solutions to transform our processes. Some initiatives underway include exploring how we can integrate information collected by Trusted Information Providers – including agencies and industry – into the process sooner to reduce duplication of efforts and leverage this data properly. The cumulative impact of these efforts could free agents to move to other requirements based on the time saved as cases are more quickly closed.

We are hopeful that the transition to the new information technology system being developed by DoD, the National Background Investigations Service, or NBIS, will help us increase efficiencies even further. As a partner to DoD in the build of NBIS, NBIS will serve as NBIB’s IT system to perform background investigations, as well as offer shared services for the end-to-end processes for all government agencies and departments. As NBIS comes online, NBIB will be able to phase out its legacy system in favor of NBIS. In FY2017, in order to clearly identify key NBIS requirements and to maximize our existing resources, we began and are continuing to implement a Business Process Reengineering strategy to clearly define critical process

**Testimony of Charles S. Phalen, Jr.
Director
National Background Investigations Bureau
U.S. Office of Personnel Management**

--
March 7, 2018

improvements and technology support requirements, and enhance our decisions through better data analytics.

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 (PAC), the interagency group established pursuant to Executive Order 13467 to oversee reform of the Federal Government's background vetting program, 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.

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 PAC Principals and DoD on a daily to weekly basis as the Government's primary investigative service provider, and coordinates with 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), the Office of Management and Budget, 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.

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

March 7, 2018

Our operations follow the investigative and adjudicative processes and standards set out by the Security Executive Agent and the Suitability and Credentialing 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 is sustained, and 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 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.

Finally, as the Federal Government works to implement the transition of background investigations for DoD personnel from NBIB to DoD in accordance with Section 925 of the FY2018 National Defense Authorization Act (Pub. L. 115-91), NBIB continues to examine our workforce needs, capacity, and budget as we work to minimize disruptions to our operations, our contractors, and our customers. Certainly, challenges will present themselves going forward; however, through an internal working group at NBIB and continued communication with the members of the PAC Principals and DoD, we have come together to carry out this transition. NBIB will continue to partner with Executive agents and DoD and other agency partners. We have a shared interest in not only reducing the inventory, but also in taking steps to effectuate a smooth transition in operations.

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

Chairman BURR. Thank you, Mr. Phalen.
Mr. Reid.

STATEMENT OF GARRY P. REID, DIRECTOR FOR DEFENSE INTELLIGENCE (INTELLIGENCE AND SECURITY), DEPARTMENT OF DEFENSE

Mr. REID. Thank you, Mr. Chairman, Mr. Vice Chairman, distinguished members of the committee: On behalf of Secretary of Defense Mattis, thank you very much for the opportunity to meet today to discuss a very important topic at hand. I have submitted my statement for the record and, sir, with your permission, I would just like to take a few minutes to amplify a couple points.

First of all, the Department of Defense fully recognizes and appreciates the necessity for security clearance reform, and we're fully committed to doing our part to develop and implement new and innovative methods for establishing and sustaining a trusted workforce, in a manner which upholds the highest standards of protection for national security information, safeguarding our people, and always ensuring the highest degree of readiness to defend our Nation.

With the support of Congress, multiple committees, and our close inter-agency partners represented here today from the Office of the DNI, the Office of Personnel Management, and the Office of Management and Budget, we have for the past some 18 months been developing plans to transition responsibility for background investigations for our portion of the workforce from Mr. Phalen's organization to the Defense Security Service led by Mr. Payne.

The Chair and Vice Chair may recall, we met and briefed on this about 11 months ago internally, and we've been moving out steadily. Last August, Secretary Mattis approved our plan, which was referred to as the Section 951 plan and was tasked to us in the 2017 Authorization Act, to submit a plan for this transition. This past December, upon approval of the National Defense Authorization Act for 2018, this included direction to the Defense Department to implement the transition plan we submitted under previous tasking and to do so by October of 2020.

We are well under way to meet this objective, in fact can project today that the initial phase of the plan—and there's some dependencies I'll talk about, but we are preparing ourselves to begin implementing this plan later this year, in the October time frame, concurrent with the next fiscal year, and there are some conditions I'll talk about.

Our team, this inter-agency team represented here today, we are all working very hard every day to put the resources and the procedures in place to make this happen, and Mr. Payne will talk about some of that in detail. But more than just a straight transfer of the current mission and the current method to our department, and in line with the intent of the security executive agent, as just talked about with the 2.0 initiative, DOD is actively developing these alternative procedures for conducting background investigations, advantaging ourselves with all available technology and other things.

Our fundamental concept is to build on the existing continuous evaluation program, which the security executive agent has already

established, to build around that and supplement that with additional tools, such as risk rating tools, which analyze individual risks, analyze risk by position, and inform us of where to look and where to focus these processes. We have a process for automated records checks—some of this is in use today at NBIB—to build around that, to take the shell of continuous evaluation, enhance that with other tools that give us a full comprehensive picture on a contemporaneous basis of the risks that we are dealing with in individual risk, in human risk, associated with responsibilities, levels of responsibility, risk profiles, and a host of other data that are connected to other programs we have, such as insider threat, such as user monitoring, such as base access, facility access.

We are in a position to aggregate that data to give us a much more comprehensive understanding of the risk than we currently have. That is the backbone of the automated process we're referring to. We have worked this with our colleagues here. We have shared it and briefed this to many of the industry leaders that you had in the previous panel and the organizations they represent. And there is full agreement of everyone I've briefed that this methodology is viable and sufficient and goes far beyond where we are today in updating our understanding of risk in the workforce to a more future-looking state.

We will soon—I said there's a condition about when we'll start. We will soon be submitting to the DNI our proposal requesting approval to begin phasing in the use of this process for selected segments of our workforce, and we will do this in a very graduated manner so we can assess and evaluate the results, everyone involved can understand what's taking place and appreciate where we are and accept the results. At the same time, we have to build up a capacity to do this on scale.

So this is a ramp. The plan we submitted is a ramped plan. It's a three-part plan, over three years. As I said, we are prepared, subject to the concurrence of the security executive agent, to formally commence this in October of this year.

This will be a long-term process and it will be done in a graduated manner. We will build up our capacity and we will bring everyone along with this, industry, government, Congressional oversight, all of our reporting requirements, all of our accountability requirements. We have every ability and full intent and no latitude not to uphold and not to represent what we're doing. There's nothing below the waterline that folks won't understand. We're very cognizant of this reciprocity issue and how people need to appreciate what's happening so they have trust and confidence in the system, and we're prepared to do that.

We're equally mindful, as we do this, that we must continue to rely on the National Background Investigations Bureau to process the some 500,000 DOD cases that are in their inventory. Those cases have gone into that system. We are enabling NBIB to do that now. We are the sponsor for the IT system. We will continue to do that and build those tools out, all of which will transfer, but they will continue to be available to all of government, and all investigative services providers in the Federal Government will have access to these tools and procedures that we are developing.

In the later stages of our plan, later into next year, we will begin working with NBIB to understand and implement the resource transfers. The financial resources we put into NBIB are on a pay-as-you-go, on a revolving fund. But the human capital, the Federal and contractor workforce that supports NBIB now, as they ramp down to a smaller population—we are 75 percent of their business load roughly. So as we shift that, we're working with them right now and we have a commitment to provide a plan through the PAC principles of what our ramp-up plan is and what their ramp-down plan is, and obviously those need to be in harmony. We will continue to rely on them to work down the inventory and we will support and enable them to do so.

I would just add here, they've done a tremendous job of dealing with a very difficult set of challenges with the inventory that Mr. Phalen inherited when he took that job, and we're very much appreciative of what they're doing.

I can't underestimate the complexity of this endeavor. This is—as I said, it's about a \$1.1 billion enterprise. We have a volume of 700,000 cases a year that they process for us. There are some 8 to 10,000 people that do this. And all of this will be in motion as we phase and implement this plan, keeping them whole and viable with a re-scoped mission and establishing our ability to do our mission, which would then be benefited by the fact that we have control of our own initiation process, the submissions piece, the investigations piece, and the adjudications, and then, very important going forward, the follow-up, the continuous vetting, continuous evaluation, foundations that I already discussed.

We're working on this every day. We have great teamwork. We appreciate the support of Congress in this endeavor. Sir, thank you again and I look forward to your questions.

[The 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
SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE
on
Personnel Security Clearance Reform
March 7, 2018

Chairman Burr, Ranking Member Warner, and Committee Members, thank you for the invitation to offer testimony on behalf of the Department of Defense on the status of security clearance reform.

The Department is focused on collaborating with our interagency partners to transition the investigative mission for DoD personnel to the Defense Security Service (DSS) and to modernize the government-wide vetting enterprise. This is a top reform agenda item for the Secretary, and three Under Secretaries of Defense – for Intelligence, Personnel and Readiness, and Comptroller – along with the Chief Management Officer and the Chief Information Officer, who are personally engaged in efforts to develop and implement new and innovative approaches to modernize the vetting process while also addressing cost, performance, and timeliness within the Department. Ensuring the effectiveness and efficiency of the personnel vetting enterprise is also critically important for the Military Department Secretaries, as it will lessen the negative impact on their mission readiness.

As the committee is aware, the Department's implementation plan, under Section 951 of the National Defense Authorization Act for Fiscal Year 2017, highlights our intent to look beyond the realm of incremental improvements and take full advantage of today's technology and innovations to alleviate the burdens of costly, time-intensive investigations. We acknowledge the key challenges ahead and are prepared to address any obstacle that arises including logistics, budget, human resources, and cultural issues. By working closely with the Performance Accountability Council and the Executive Agents, we intend to modernize our current investigative processes to meet the challenges of the evolving threat landscape and the dynamic changes in our workforce.

Executing the phased implementation plan over a three-year period will provide DoD with a unique opportunity to build on our existing continuous evaluation and automated records checks architecture and leverage insider threat mitigation measures, user activity monitoring and related initiatives to more effectively manage risk. Currently, the Department has 1.1 million DoD personnel enrolled in a continuous evaluation program, exceeding our annual goal for last year. This program has demonstrated clear and compelling benefits of ongoing and more frequent vetting of cleared personnel and, when expanded, will integrate with DoD's insider threat and physical access programs to create a more comprehensive security architecture. These continuous vetting methods, which significantly decrease the risk associated with periodic reinvestigations that are currently conducted every five or ten years, have shown convincing results for early detection of security risks and provide the basis for new approaches to modernize the vetting enterprise.

We will also continue to work very closely with the Executive Agents to streamline traditional labor-intensive processes that exist today, to continue to identify ways to economize field investigative work and automate the process wherever possible. Long delays for background investigations can be eliminated by enhancing and largely replacing time intensive field work with the power of big data analytics, artificial intelligence, and machine learning. We will use field investigations to fill gaps, not as the means to collect information that is more readily available through automated processes.

As we implement the Section 951 plan, we remain committed to our task to design, build, operate, secure, and maintain the National Background Investigative Service, or NBIS. This is a single end-to-end IT shared service solution for personnel vetting throughout the government; not only for NBIB, but for all federal agencies that conduct background investigations or adjudications. DoD will remain committed to resourcing NBIS throughout this transition process. By optimizing our investments and simplifying service delivery, we can achieve significant cost savings and cost avoidance, while more effectively driving system efficiency.

This work will be done hand-in-hand with the Performance Accountability Council as well as the Security and Suitability Executive Agents, collaboratively developing alternative vetting procedures that will establish and sustain a continuous vetting process that can identify at-risk situations as they occur, and focus investigative and management intervention efforts ahead of a problem. These alternative investigative methodologies will be supplemented with automated prioritization tools and integration with partner missions such as insider threat and physical security programs. As a result of this work, we will implement modern alternative processes that are approved and vetted with no impact to reciprocity.

We will continue to collaborate with our partners to identify these additional measures in parallel with our work to implement the Section 951 plan. Once established, we will route new work into that pipeline, allowing NBIB to focus on their existing work and modernization efforts, as we continue to develop automated processes and integrate them into the overall vetting architecture for use across the government.

DoD continues to engage actively with our congressional partners, industry and the think-tank community through security-focused forums and roundtable discussions that have resulted in excellent feedback essential to developing innovative and effective enterprise-wide solutions. We have developed new relationships and reinvigorated long-standing ties to ensure our partnership with industry avails of us the best practices. What we learn from the experience of the private sector helps us examine innovative methods for assessing risk in the workforce and

crafting mitigation strategies to protect people, information, and programs from insider and outsider threats.

As we prepare for the phased implementation of our plan, the Department is well postured to take bold steps, while maintaining cognizance over the risks associated with an endeavor of this magnitude. We are getting the right people on board – recruiting talent, adjusting organizational design, establishing the management structure, completing the IT infrastructure, and most importantly, embracing a new way of doing business. Simultaneously, we will need to keep the critically important DSS National Industrial Security Program mission operating effectively while we adapt DSS to its future state.

This is a very ambitious endeavor, but highly necessary in light of all the challenges we have faced in recent years. We must restore confidence in the background investigation process, eliminate long and costly delays, and fine tune our vetting protocols to guard against future compromises of national security information. Our plan is sound, we are steadily laying the groundwork for execution, and we have solid support across the government and with our industry partners. Thank you again for your interest in this most important topic. I would be happy to discuss these DoD initiatives in more detail. I look forward to your questions.

Chairman BURR. Thank you, Mr. Reid.
Mr. Payne.

**STATEMENT OF DANIEL E. PAYNE, DIRECTOR, DEFENSE
SECURITY SERVICE, DEPARTMENT OF DEFENSE**

Mr. PAYNE. Mr. Chairman, Mr. Vice Chairman, members of the committee: Thank you very much for this opportunity to speak with you on this topic. You have my written statement. I'm not going to go into that. I'll try to keep my comments as brief as possible because I know you have a lot of questions.

I will say that I am the individual who's going to be responsible for executing the mission in DOD for background investigations and begin to build that mission. As a result of that, Charlie and I have to work, Mr. Phalen and I, have to work very closely with each other and our teams have to work very closely with each other so that we do this in a manner that doesn't hinder NBIB's ability to work down the backlog while at the same time increasing our capacity to pick up these investigations.

That being said, and in view of the previous panel that was here and the comments that came from the previous panel, I am responsible for industry security currently. While we do not do the background investigations ourselves—that's Mr. Phalen's organization that does that—we initiate the background investigations. I am the individual who grants interim security clearances and takes them away. I am also responsible for the execution of DOD's continuous evaluation program, which from my perspective has been greatly successful and is the way of the future. We have to go down this route if we are going to make the necessary changes to make this process better.

In addition to that, the insider threat programs for DOD. I own the Defense Insider Threat Management and Analysis Center, which is where all of the insider threat concerns in DOD come to. We work with the individual agencies within DOD to resolve those particular issues.

All of those things combined, as Mr. Reid outlined a few minutes ago, all of those things combined are things that we did not have back in 2004, 2005 when DOD had the initial mission for background investigations. We have them now. That's the way of the future. That is the way that we have to go.

If we are going to make any progress in making this program faster and making this program more secure, we've got to look at a different methodology of doing this. It has to—we have to utilize continuous evaluation and automated processes, many of which Mr. Reid outlined in his statement. But in addition to that, we have to look at the standards. We have to change standards. If we are going to do this successfully, we have to change standards. That's going to result in some big decisions on our part, and those big decisions pertain to how much risk we are willing to accept.

As Mr. Berteau in the previous panel stated, we're never going to be able to reduce the risk to zero unless we stop hiring. Obviously, we can't do that. There's always going to be risk involved in the investigative process. There's always going to be risk involved in the security clearance process. What we have to determine is how much risk we find acceptable.

Thank you very much.

[The prepared statement of Mr. Payne follows:]

**Statement
By
Daniel E. Payne
Director, Defense Security Service
Senate Select Committee on Intelligence
7 March 18**

Mr. Chairman, Vice-Chairman, and members of the Committee, I appreciate the opportunity to speak with you today on our efforts to transfer the DoD background investigations mission from the National Background Investigations Bureau (NBIB) to the Defense Security Service (DSS). We know that we must conduct this transfer in a manner that has the least impact on NBIB's ability to reduce their current investigative inventory, the bulk of which belongs to the Department of Defense (DoD). The DoD has a vested interest and is the primary beneficiary of NBIB's ability to reduce their current investigative inventory.

DSS plans to conduct the transition in a phased manner over a three year period. DSS will assume responsibility for the least labor intensive investigations first, while we build our investigative capacity and infrastructure. During the second phase, DSS would seek to transition resources from NBIB to DSS. By the end of the third year, DSS will be able to assume the most labor intensive investigations. Our goal is to gradually reduce the number of investigations we send to NBIB, allowing them to apply the excess capacity that is created toward the reduction of the existing inventory. This phased approach, combined with other efforts currently underway by NBIB to increase their investigative capacity, should have a positive impact on the reduction of inventory.

I think, however, it is important for us to discuss something that is fundamental to the challenges we all face with the security clearance process. The way we currently do business has

to change; we simply cannot continue to maintain the status quo. The current security clearance process was developed decades ago and, while there have been a number of significant changes over the years, the foundation remains intact. We have to modernize and transform the process.. We now have insider threat programs, continuous evaluation, continuous vetting, electronic adjudication, risk rating tools and a number of other things we never had used before. We need to better utilize these tools to help identify the high risk populations.

We must use our investigative resources in a targeted manner rather than a one size fits all manner. But we have to go even further than that. We must look for a 21st century way to get the information we need to meet our adjudicative standards and we need to determine, as a government, how much risk we are willing to accept. Director of National Intelligence Coates recently stated in testimony before this Committee that the security clearance process was “broken.” He also quoted Vice-Chairman Warner as having said that the security clearance process did not need evolution, it needed revolution. I think we all agree.

To that end I wish to highlight and applaud an effort that has been initiated by Director William Evanina of the National Counterintelligence and Security Center which will commence over the next few weeks. Director Evanina’s office has collaborated with both internal and external experts of the personnel security field to take a “blank slate approach” to the security clearance process. The goal is to start from scratch, with no ideas off the table, to develop a completely new security clearance process. I think this type of review is long overdue and I commend him for initiating it.

Thank you again for inviting me to participate in today’s hearing and look forward to answering any of your questions.

Chairman BURR. Thank you, Mr. Payne. Thank you to all of our witnesses.

Again, we'll recognize members based upon seniority for up to five minutes. I recognize myself first.

I'm going to tell you a story. The story starts about ten years ago. A 22-year-old graduates college, never even plans to work for government, gets offered a job, a civilian at DOD. Couldn't be more excited. Parents more excited than he was. Job, paycheck, things that you hope they're going to find. Then a process of 11 months of security clearance.

It gets back to some things that were said in the first panel. I don't think that I'm an exception. That happened to be my son. Here's a kid that is incredibly excited to work for government, work where he did, ready to go. And after 11 months, he wonders whether he made the right decision. He didn't lose his skills, like some will do today if it's technological. But the question is, how much of that initial passion for working for government do you lose from the standpoint of retention down the road?

Understand, I get it first-hand why we've got to accomplish what you've set out to do. It is unacceptable to this next generation, just the fact that things go so slowly. I say that with full knowledge, and I'm still talking about the Federal Government, and there are some things even Congress can't change. But the reality is that we can do much better.

Mr. Reid, I thank you for your brief almost a year ago. The fact is the time line's about exactly where you told us it was going to be. We're excited to see the roll-out. Mr. Payne, a lot of pressure on your shoulders. I get that. But we can't go forward unless we do this. I know the commitment of Dan Coats and I don't think that that's going to change as long as he's there. I think now we're matching it with a desire by members of Congress to make sure we not only identify those things that need to be changed, but we accomplish the solution. So I think that we've got good partners.

Mr. Reid, Mr. Payne, this is to you. Are there additional authorities that you need to accomplish this roll-out and eventually fully move the system to what you have designed?

Mr. REID. Senator, from an authorities standpoint, Section 925 of the current NDAA gives us—reinforces the Secretary's authority in the first instance to conduct background investigations, which was a plus. It also provides direction, not so much authority, for us to consolidate other elements within the Department, which also is very helpful.

Chairman BURR. Let me ask it a different way.

Mr. REID. Yes, sir.

Chairman BURR. Is there anything in Federal statute today—

Mr. REID. No, sir.

Chairman BURR [continuing]. That hinders your ability to change your review process the way you think it needs to be done?

Mr. REID. Not that I'm aware, not in statute. Now, we are wholly dependent on Director Coats and his leadership to approve, as I outlined, our alternative process. The Secretary cannot, Secretary Mattis cannot do that unilaterally. We are beholden to the security executive agent and the suitability executive agent for the standards they set and the process they control. We don't have a prob-

lem with that process. We're eagerly looking forward to participating in the Trusted Workforce 2.0, because it comports to the plan that we've already set out to conduct. So I do not believe there's anything in Federal law that is an impediment to what we want to do, sir.

Chairman BURR. Mr. Dunbar, I'd also ask you to go back and make sure from an ODNI standpoint that there's not some statute out there that is going to pop its ugly head up and say: Well, you know, this does make a lot of sense, what we're doing over here, but you can't do that until we change this statute. If we've got things to change, let us know now so that we can implement this on the timeline that's designed.

Mr. DUNBAR. Yes, Senator, absolutely.

Chairman BURR. I should have said this at the first panel and I'll say it now. I'm not adverse to additional investigators. I'm not adverse to increasing funding. I am adverse in doing either of those things before we change the system. So until you change, it's hard to truly evaluate what the need is going to be, what the cost is going to be.

I am hopeful—and I think, Mr. Reid, this is your intent—that this takes the timeline for security approval and drives it down. Can you give us what your goal is from a standpoint of a timeline? If today—if 9 years ago it took 11 months, I can't imagine what it is today for that similar TS-SCI individual. What's your goal now?

Mr. REID. Yes, sir. The established goals for each level of clearance are attainable under our plan, but, better than that, under our plan—currently, for a SECRET reinvestigation, the guideline goal is 145 days. It's taking about twice that long. Under our plan, our vision is that that periodic reinvestigation as it's currently conducted does not exist, that a contemporaneous continuous vetting process would be implemented in place of that.

Now, there will still be deliberate face-to-face sort of re-upping of employees. It's not autopilot. But the monitoring and the reporting, which we are already doing in our program now, will be the backbone. So the answer to that question is the goal is to eliminate the requirement currently existing for periodic reinvestigations at all levels. We have some work to do to get beyond the first level.

Chairman BURR. What can I tell that next 22-year-old who wants to be a civilian DOD employee and is getting ready to go through the background check, 22 years old, out of school, never lived anywhere but school and home? How long is it going to take to process him for a clearance?

Mr. REID. Again, under the current process that ranges from 200 to 400 days. Under the future process, it's perfectly attainable to get down to, in the current guidelines, which are for TOP SECRET 150 days, but we feel it can go much lower with the automation and the tools that I described, sir.

Chairman BURR. Vice Chair.

Vice Chairman WARNER. Thank you, Mr. Chairman.

I think we've heard a lot of commonality from the first panel to the second panel in terms of goals. It's not a new problem. But I look at just the last, performance over the last couple years. We've had doubling of the backlog. From Mr. Phalen, while you say it's

stabilized, I don't hear—and I'm going to come to you in a couple minutes—when are we going to actually get it down?

We've had a doubling of the costs. We have everybody using the term "continuous evaluation," yet we seem to not have commonality on that or how we're going to get there. We have the notion of increased technology. But again, I don't see a timeline presented. We see in certain areas, for example, the financial sector, where there are enormous security concerns, they have been able to implement tools like continuous evaluation using increased technology.

I get the frustration on the DOD side that say, we've got to split this up. But we're talking about an effort to go with, if we accept some of the industry's interest in terms of one application, one investigation, one adjudication, and one clearance, it seems like we're going the opposite direction.

So I'd like to hear either from Mr. Reid or Mr. Payne how we make sure, if we go through this process, we're not going to simply create more duplication, less portability, less reciprocity, than what we have right now, which again I'm the first to acknowledge is not working.

Mr. REID. Yes, sir. The application, the standards, are federally directed. There is one, there is one standard. What we are embarking on and preparing to implement is an alternative methodology to reach those standards. Now, in parallel, these guys talked about everyone getting together and looking at the standards. If they change, they'll change for everybody. We're not creating a new standard. We're not creating a new application. We are automating behind the application the process that we go through to collect the data that's relevant to form the basis of a background investigation, that becomes the basis of an adjudicative decision or determination.

We are not changing the standard, sir.

Vice Chairman WARNER. Recognizing that you are the vast majority, how are you going to make sure the goal of reciprocity and portability takes place as you build this new system?

Mr. REID. In the very first instance, sir, that will be by adhering to the guidelines set by the executive agents in everything we implement. We do not have unilateral authority to change that process without the executive agents' concurrence. So we will align our process to their standard.

Vice Chairman WARNER. Respectfully, I know you're trying to head us in the right direction, but it sounds like a lot of process words rather than specific guidelines, timetables, and how we're going to get there.

Let me just—and while I share the Chairman's concern about simply throwing money at it, but my understanding is there's an awful lot of agencies, they kind of build this into their G&A and they don't continue to prioritize funding, so that the funding that is even supposed to be there isn't getting there. So I don't think we ought to throw more dollars, but I do think we need to make sure that agencies make this a priority within their funding scheme. I hope DOD, which has gotten a very generous bump-up in the last budget—if you're going to take this on, it would be very

disappointing, at least to this Senator, if we came back and said, “Well, we didn’t have the dough to do it.”

I’m going to go to Mr. Phalen. Mr. Phalen, stabilizing at 700,000 is not acceptable. It’s just not acceptable. I’d like to know when we’re going to start seeing those numbers driven down on the backlog.

Also, Senator Heinrich raised issues on the earlier hearing about new techniques that some of the government labs were using in terms of, for example, hubbing interviews. Why is it taking so long to try to implement what seems to make common sense in terms of hubbing interviews. I’ve got an area like Norfolk, Virginia, where we’ve got huge numbers of people trying to—waiting for clearances. What can you talk—what can you say specifically about using these tools that seem to be working in DOE kind of across the breadth in other areas where there’s concentration of Federal employees, like Norfolk in my area or Northern Virginia in my area?

Start with how we’re going to drive that 700,000 backlog down, not stabilize it, drive it down.

Mr. PHALEN. Starting one step even further behind that, when I first joined this organization 17 months ago, the capacity to conduct the work that we were required to do was insufficient to conduct that work, period. That’s why, as you saw in the first few months after we stood up, that that inventory continued to rise as opposed to begin to stabilize.

When we reach the point where we have the same capacity that we had in 2014 when this all fell apart, that’s a way station along the way to reach that point of stabilization. It’s not the endgame. In one sense, I’m proud we hit that stabilization, but I’m not proud that we have not brought that inventory down. Our goal is to bring it down. Last week I noted to a committee on the other side, the House side, that we are looking at potentially as much as 15 to 20 percent reduction by this time—not by this time—by the end of the calendar year. That’s still not sufficient, but it will be—by itself, it will begin to drive that number down. It will probably take us a couple of years to get down to a level that is much more effective.

Along the way, we are trying a number of things. We’ve talked about technology. We need to be able to get at information, collect information more reliably, more quickly, through technology, as opposed to shoe leather, as was mentioned in the previous session. The problem is getting to some of those sources right now, particularly law enforcement sources, is not as easy as one would hope, and we still have to put a lot of people on the street to find police records in relevant areas. But we’re continuing to work on that closely with the police agencies at the State and local, Federal, tribal level, to continue to do that.

You talked about hubbing. We started that with the Department of Energy as a surge rather than hubbing, about 17, 18 months ago in Los Alamos. It looked very promising. We have since that point, we have done a number of things that are both hubbing and surging. One is more concentrated than the other. Most recently, we finished one in Wright-Patterson Air Force Base in the Dayton area. We recognized an increased efficiency of somewhere in the low 40 percent positive note. In other words, what would normally be an hour’s worth of work they were finishing in 36 minutes. That’s a

rough estimate. They were far more productive in that hubbing area.

You mentioned the area around Tidewater. We are actually beginning a session in Tidewater on April 1st. We have pulled together all of our—all the Federal agencies that are down there, all the DOD agencies that are down there and pull together all of our assets, both staff and contract investigators, and we're going to focus on that area.

But that is one of probably about eight or nine that I could mention just in the last year where we have actually done this and found very positive results. Certainly Dayton, San Antonio, out in Nevada, Tinker Air Force Base, Oklahoma City. I mentioned Tidewater. And one that I think is going to be very promising to us on two fronts. One is, we've been working with industry directly to find areas, not by company, but by geography and by program, to find those areas in the country where we can again focus our resources—places like Southern California, places again like Tidewater, like the Space Coast in Florida, where we can bring that together and work with industry to bring—to focus our energies down there.

A second part of that is, to follow on to a comment that was made I believe by one of the early panelists, it's clear to me from both our current work and my last experiences in life that industry collects an awful lot of data before they put somebody in for a clearance, before they even decide to hire somebody. We need to find a way to leverage the work that they have already done, accept it, and build it into part of the process, and not having to go back and ask those same questions. That will by itself reduce a lot of time in collection and effort.

That's sort of a high-level view. I hope that it gets to some of those points you mentioned, sir.

Vice Chairman WARNER. I'm curious you didn't mention National Capital Region as one of these areas that would be a recipient of a hubbing area, since it's the greatest concentration of the need for clearances.

Mr. PHALEN. Interestingly enough, I asked that question yesterday and spoke to the folks in charge of the activities in this area. We are in the Washington, D.C., area, for work that has to be done in the Washington area, we are actually pretty close to being up to speed in the Washington, D.C., area. It is other parts of the country where somebody's background may take them to other parts of the country where it is not as up to speed as it could be.

Vice Chairman WARNER. I'll be happy to send a lot of my friends in the contractor community to you on that fact. They don't believe that fact.

Mr. PHALEN. Understood.

Chairman BURR. Senator Lankford.

Senator LANKFORD. Thank you, Mr. Chairman.

Mr. Reid, has DOD done its own background investigations and work before and then handed that back over to the whole of government?

Mr. REID. Yes, sir. Prior to 2005, we had responsibility for our background investigations at what's now the Defense Security Service.

Senator LANKFORD. So what's the lesson learned there? So why is this time going to be better, because last time it was turned over and then now it's coming back? Give me the key lessons learned?

Mr. REID. Mr. Payne touched on one of those, sir. That is, having the comprehensive process in place to deal with the volume and the scale of investigative items. The continuous evaluation tools that we have now are different, the risk-grading and automated record checks; additional tools that we are developing to streamline the submission process within the Department. If you look at the current process and you look at past practice, there's a high percentage of drag in the system between submission and investigation, just to get the submission clean and get all the data. We have tools in place already to improve upon that.

I talked about the streamlined background investigations and then the centrality and the positioning of our consolidated adjudications facility, which did not exist at that time either. So we have in place, or we will have in place when we move investigations back, all three pieces of this enterprise—submissions, investigations, and adjudications—all under a single organization, with the authority and the resources and the mission focus.

I would just say currently, sir, Deputy Secretary Shanahan, the number one reform agenda for him is this clearance reform. Secretary Mattis firmly, firmly, actively involved in pushing us to better solutions and to make this functionality not a back office thing that someone does in the Department, not an administrative thing, but the security focus that exists in the leadership team now—I can't say what it was in 2005—it could not be any higher today, and we have the pieces aligned to put this into action.

Senator LANKFORD. So give me two goals that are the nickels and noses type goals here? Will this drive down costs? And will this speed up the process?

Mr. REID. Yes and yes.

Senator LANKFORD. Give me a ballpark of what that means?

Mr. REID. In terms of speeding the process, again, current timelines, we're experiencing 150 or so days for a SECRET-level reinvestigation. We will eliminate that requirement completely. So there's a time improvement there.

Current background investigation field activities, field work, our studies and our pilots and everything we put into place now, using aggregated data tools that I've talked about can get us 90 percent of everything we're getting now from the field investigation on the front end; and then the tools can focus on the last 10 percent. We will still have to go out and do some field work, but 90 percent of the field work can be handled through automated processes. So that will drive down the capacity needed to do those field investigations, and therefore drive down the cost per unit that we currently provide to OPM.

Senator LANKFORD. You had said first-time approval is still at 150 days. That's still your assumption, first time, new person, new hire?

Mr. REID. That's the reinvestigation. But currently it's about the same for the initial SECRET, at the SECRET level.

Senator LANKFORD. And you assume it's going to still stay, that 150 days?

Mr. REID. Pardon me, sir?

Senator LANKFORD. You assume that it will still stay 150 days? Currently it's 150 days. You assume when you transition it over it will still be 150 days for a first-time hire, brand-new investigation?

Mr. REID. No, sir, no. That's the current standard. I don't know today how fast we'll be able to do a SECRET. My anticipation is it can be done in a matter of days. There's processes in place now to gain access to certain programs and facilities even here in the D.C. area, that run a series of automated checks that are very thorough, and it takes 20 minutes. I don't know that we're going to be at 20 minutes. And you always are going to have things you have to go check.

Senator LANKFORD. Back to the Chairman's question when he talked about the 22-year-old, when he asked you specifically on that how long it's going to take, that's when you gave him the answer of 150 days. So I'm trying to be able to—

Mr. REID. That's the current standard, sir. I apologize.

Senator LANKFORD. All right. So you're thinking it's not going to be 150 days; it could be a couple of weeks?

Mr. REID. Absolutely. At the SECRET level, absolutely. No reason why that can't be.

Senator LANKFORD. Mr. Payne, do you concur on that?

Mr. PAYNE. I do. I think some of the things that we have in place right now, again as Mr. Reid outlined, using continuous evaluation—maybe I want to finesse that a little bit: continuous evaluation as opposed to continuous vetting. So continuous evaluation, the program set up by the DNI, is designed to look at the risks in between periods of reinvestigation. When we talk about—and they have seven data sources that they're requiring every agency to utilize when they do continuous evaluation.

When I talk about continuous vetting, I'm looking at expanding that into other data sources, data sources within DOD, other data sources within the U.S. Government, other data sources within the public sector, that we can pull all those things together, many of which are required already for the SECRET-level reinvestigations, and do those on a continuous basis.

If we're doing those things on a continuous basis, there is no need to do a reinvestigation on someone at the SECRET level unless you come up with derogatory information. So that's where the significant savings is going to be.

Senator LANKFORD. Thank you.

Thank you, Mr. Chairman.

Chairman BURR. Senator King.

Senator KING. Thank you, Mr. Chairman.

I've been surprised in this hearing that we haven't had to talk much about money. Mr. Phalen, do you have adequate—and Mr. Reid; are there adequate resources in terms of money and people? Is it just management and automation? Or are there shortfalls in terms of the number of people necessary to do these, to work down this backlog?

Mr. PHALEN. Under the current process, in our current operation, we operate in a working capital fund, a revolving fund. Agencies that wish to have an investigation done give us the money to have the investigation done. So from our standpoint, it is: Here's the

money; do an investigation. So we're not short of funding to do these investigations on our end.

I think a better question would be: Are the agencies that need to have an investigation conducted funded appropriately to identify the money to send to us to do the investigation?

Senator KING. Are there sufficient personnel? Are there people? Our economy is pretty tight. Are there people? Is there a shortage of qualified people to do this work?

Mr. PHALEN. The high-end folks to do the investigative work as a population are stressed at this point to hit beyond where we are, although we have encouraged our suppliers and ourselves to continue hiring. So today there are nearly adequate, but we still have much more work to do. And if we don't change today's processes, some of the things you've heard already, then we will still need to continue hiring beyond all that, and that puts even greater stress on the total number of people we have to do it.

Senator KING. So that's an additional imperative to seek technological productivity?

Mr. PHALEN. Yes. It's to make the current people more productive and to reduce the need for having people in there, yes.

Senator KING. I think this could go to any of you. I'll address it to Mr. Reid. Is the portability that we've talked about part of this sort of revamped plan, Mr. Phalen, Mr. Reid, to consider that factor so that we don't have to redo these tests? Let me ask a specific question. We heard about DHS, where you might have to have a whole new investigation to go from one job to another in the same agency. Does that—please tell me that doesn't happen in the Department of Defense.

Mr. REID. No, sir, it does not. But we have single adjudication facility all under one roof. In DHS, the aggregation of independent agencies that were brought together in DHS, they're still operating it differently. But we have for years, had a single adjudication facility within the Department, and external to the Department because—

Senator KING. So the clearances are portable within the Department of Defense?

Mr. REID. Absolutely, sir.

Senator KING. Is the portability issue in other agencies part of this reinvention that's going on?

Mr. REID. The interesting part is that it is mostly today a singular investigation. Any agency can use the investigation we do to conduct an adjudication. But it is up to that agency to do the adjudication. In the example you heard earlier within DHS, with the same set of facts they may decide to ask for more information, ask for a re-adjudication.

Senator KING. So portability isn't a part of the overall structure of the new system. It's an agency by agency decision whether they will accept, whether they will do reciprocity?

Mr. REID. I'd say it's less about structure and more about both empowering them and encouraging them to accept the decisions made by others in previous lives. So a decision made by one agency, for the second agency to accept that that first agency probably did a pretty good job and was honest about how they approached it to accept the results of that first investigation, and not—maybe

another question, but not ask a lot more about it, not reinvestigate it, not—I'm sorry—not re-initiate an investigation.

Senator KING. Thank you.

Mr. REID, why is it that it's taking so long, has taken and apparently will take so long, to transition from the OPM to Department of Defense? You are talking about 2020, I think, and it started last year.

Mr. REID. The Defense Authorization Act requires us to implement the plan by October 2020. We intend to implement the plan in October of 2018. We're projecting a three-year, three-phase plan, starting at the SECRET—

Senator KING. You're going to bring it in on time and under budget?

Mr. REID. Well, it says start by 2020. So we will start now. It didn't tell us how long to finish, but we submitted a three-year plan. So logically the expectation is we take three years.

When we moved it out of DOD last time, it took more than five years. And it's more complicated. But the short answer to your question: We want to do it in a phased, deliberate, and graduated way. We have to keep our partner agency whole. They support a lot of other agencies in the government and they rely on us to do that. It will help them work down their inventory. Once we start processing new cases separately, that will drive down the new work that goes to Mr. Phalen of tens of thousands of cases a week that we are providing them now. We will turn off that spigot, help with the backlog, as we build up our own capacity and capability.

Senator KING. I'm out of time, but, Mr. Payne, very quickly: You used a phrase that struck me. You said: We have to change the standards. What did you mean when you said that? You mean lower the standards?

Mr. PAYNE. I don't necessarily mean lower the standards, but we have to—the Federal investigative standards dictate what steps have to be taken to achieve a SECRET level security clearance or a TOP SECRET level security clearance. Again, as has been outlined, we—

Senator KING. It's the steps that might have to be—

Mr. PAYNE. That's correct.

Senator KING [continuing]. Compressed, not necessarily—

Mr. PAYNE. Not the adjudicative standards necessarily, the investigative standards.

Senator KING. That's what I needed to know. Thank you very much.

Thank you, Mr. Chairman.

Chairman BURR. Senator Wyden.

Senator WYDEN. Thank you very much, Mr. Chairman.

A question for you, Mr. Phalen. I've made a special focus of my work during this Russian inquiry the follow-the-money kinds of questions. I want to ask you a couple of questions relating to that. For you, I think, Mr. Phalen, the question is: Should someone who fails to disclose financial entanglements with a foreign adversary be eligible for a security clearance? That is a yes or no question.

Mr. PHALEN. I'm not sure I have a yes or no answer for you, sir. I believe it would play a prominent role in a decision as to whether

that individual should be granted a clearance, and it is not an inconsequential question to ask.

Senator WYDEN. But how is it not an up or down, yes or no? We're talking about significant financial entanglements with a foreign adversary. Shouldn't somebody who fails to disclose it—I mean, it's one thing if it's disclosed and you have a debate and, like you say, it's balancing. But failure to disclose seems to me a different matter altogether.

So I gather you don't think necessarily that somebody who fails to disclose a significant financial entanglement with a foreign adversary should be denied a security clearance?

Mr. PHALEN. That is not what I meant to say.

Senator WYDEN. Well, go ahead. Tell me what you mean to say?

Mr. PHALEN. Under the adjudicative standards—and I would defer also to Mr. Dunbar to reply to this as well. Under the adjudicative standards, there is nothing that says "If you do this, you can't have a clearance." It says to the adjudicator to take into account all that you know about this individual, make a decision regarding their candor, regarding their entanglements, regarding their families, regarding crime, regarding all sorts of things, and make a decision.

I would say that the scenario you outline would play a prominent thought to be considered during the adjudication. But there's nothing in today's standards that says any of those things by themselves are disqualifying. It would be a very important piece to consider.

Senator WYDEN. Do you believe it ought to be disqualifying?

Mr. PHALEN. I would have a hard time overcoming that.

Senator WYDEN. Great. Thank you.

Okay. Mr. Dunbar, question for you. Jared Kushner's interim access to TOP SECRET–SCI information has raised a variety of questions. Under what circumstances should individuals with an interim clearance get that type of access? That's for you, Mr. Dunbar.

Mr. DUNBAR. Senator, as we've heard earlier today with the industry panel, interim clearances have been used throughout the government for some time, many years. There are two specific governing documents for interim clearances and the guidance that's out there now allows interim clearances at the SECRET level as well as the TOP SECRET level.

There are situations called out in the guidelines which speak to urgency of circumstances, those types of ideas about how when someone might be granted an interim security clearance. I believe an example that would be applicable here is an incoming Administration, which has the need to on-board personnel and get them in positions as soon as possible in order that they can perform the duties of their function.

In regard to Mr. Kushner's specific case, the DNI sets policy, standards, and requirements. As Mr. Phalen has stated, each individual adjudication—and this is contained in the Security Executive Agent No. 4—is treated based on the whole person concept, in which every particular piece of information, positive and negative, past, present, all of those things, are factored into the adjudication.

As Mr. Phalen has stated, in my opinion the issues which you've raised, Senator, would be issues which would need to be thoroughly

vetted in the course of the investigation. I have no reason to doubt that the Federal Bureau of Investigation would not investigate each and every issue very fulsomely.

Senator WYDEN. Let me ask one other question. During our open hearing, in fact I think it was Worldwide Threats, the Vice Chairman, to his credit, mentioned security clearance as being central to the question of protecting sources and methods. I asked FBI Director Wray, with respect to Rob Porter, how that decision was made. I mean, when did the FBI notify the White House? It was clear when you listen to Director Wray's answer, it did not resemble what John Kelly had actually been saying to the American people.

So I'm still very concerned about who makes decisions at the White House. With regard to White House personnel, in your view, Mr. Dunbar, who would make the decision to grant an interim clearance holder access to TOP SECRET-SCI information?

Mr. DUNBAR. Senator, that decision would be made, in my understanding, by the White House Office of Personnel Security, based on an investigation conducted by the FBI.

Senator WYDEN. My time is up. I would only say, I'm not so sure as of now who actually makes that decision, because we've heard Mr. Kelly speak on it. I understand the point that was made by all of you who are testifying. I think it still remains to be seen who would make that decision to grant an interim clearance.

I'm over my time. Thank you for the courtesy, Mr. Chairman.

Chairman BURR. Before I turn to Senator Harris: Mr. Phalen, since you do most of these right now, is it unusual or is it acceptable that if an individual who's filed for a security clearance finds out they left something off their application—are they offered the opportunity to update that for consideration?

Mr. PHALEN. Yes.

Chairman BURR. So if somebody left it off, they could add it on and that would be considered in the whole of the evaluation?

Mr. PHALEN. Yes, it would be, at any time during the investigation. What we frequently find is two scenarios. Number one is: I just forgot when I was filling out the SF-86 to put that on there as an individual issue. And there are times when we will go in and conduct the investigation, have the face-to-face conversation.

Chairman BURR. So that's actually happened more than the one instance that Senator Wyden referred to?

Mr. PHALEN. We find it happens with some regularity.

Chairman BURR. Thank you.

Senator Harris.

Senator HARRIS. Thank you.

Mr. Phalen, it's important I think for the public to understand why these background checks are so important to determining one's suitability to have access to classified information. Can you please explain to the American public why these background checks are so important to national security?

Mr. PHALEN. Yes. In taking a background check, in addition to both the investigative piece and then ultimately a decision by a government agency to grant that person access to information or have some level of public trust, we owe it to—I think we as a government owe it to the American people and to the American taxpayer to ensure that people who are working in the national secu-

rity arena and in areas where there is a public trust, that we have done everything we can within reason, to determine that that person can—that trust can be placed into that person.

I know in an earlier part of the conversation, earlier hearing, there was a conversation about should we reduce the number of people that have clearances? I think there's not so much a counter-argument to that, but when we have people across this particular environment and in the earlier panel where they have access daily to national security information, secrets that give this country an edge in war, in peace, and other sorts of things, and at the same time we have our industrial partners that we work with that are building all those tools that help us fight those wars or keep that peace. This is a very simple thing I've said in other venues: Do you want to have less trust in the guy who is turning bolts on an F-35 assembly line or more trust? My argument is we probably want more trust rather than less.

Senator HARRIS. And in addition to the trust point, isn't it also the case that the Code of Federal Regulations lays out 13 criteria for determining suitability, not only to determine who we can trust, but also to expose what might be weaknesses in a person's background that make them susceptible to compromise and manipulation by foreign governments and adversaries.

Mr. DUNBAR. That is correct. This is a process that is both looking at history to ask if you have—do you already have a record of betraying that trust and, perhaps more importantly, both for initial investigations and for the continuous vetting or continuous evaluation portion, to say, "What is changing in their lives and how do we predict whether they are going to go horribly bad before they get that far?"

Senator HARRIS. So there are 13 criteria, as I've mentioned. One is financial considerations. I'm going to assume that we have these 13 factors because we have imagined scenarios wherein each of them and certainly any combination of them could render someone susceptible to the kind of manipulation that we have discussed.

So can you tell us what we imagine might be the exposure and the weakness of an applicant when we are concerned about their financial interests, and in particular those related to foreign financial considerations?

Mr. DUNBAR. In a nutshell, it would be an individual who has entangled themselves, whether it's foreign or not, in financial obligations that have put them in over their head. And oftentimes this causes people to make bad decisions, bad life decisions. In some of these cases, we've found from the history of espionage it causes them to decide, "Well, I've got something valuable here; let me sell it to somebody."

Senator HARRIS. How much information is an applicant required to give related to foreign financial considerations?

Mr. DUNBAR. They're required to identify foreign financial investigations, foreign financial obligations, foreign property.

Senator HARRIS. Foreign loans?

Mr. DUNBAR. That would be a financial obligation, yes.

Senator HARRIS. Of course.

Mr. DUNBAR. Yes.

Senator HARRIS. When we talk about foreign influence and it is listed as a concern, what exactly does that mean in terms of foreign influence? What are we looking at?

Mr. DUNBAR. It would be, how am I or am I influenced by either a relationship I have with someone who is foreign, a relationship I have with an entity that is foreign? That could be a company. It could be a prior or co-existing citizenship I have with a foreign country. It could be a family member who is someone from a foreign country. And how much influence any of those things would have over my judgment as to whether I'm going to protect or not protect secrets and trust.

Senator HARRIS. Given your extensive experience and knowledge in this area, can you tell us what are the things that individuals are most commonly blackmailed for?

Mr. DUNBAR. It is not—I'd have to go back and do some more research. The instances of blackmail by people committing espionage is not as substantial as the incidence of people who have simply made a bad decision based on financial or other entanglements. They just make a poor decision and decide that, my personal life is worth more than my country.

Senator HARRIS. Then I have one final question, and this is for Mr. Payne. According to press reports last fall, you said, quote: "If we don't do interim clearances, nothing gets done." You continued to say: "I've got murderers who have access to classified information. 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 obviously causes and would cause anyone great concern, the problem of course being that the inference there is that interim clearances don't disclose very serious elements of someone's background. So can you please tell us—and we also know, according to press reports, that there are more than 100 staffers in the Executive Office of the President who are operating on interim clearances—what we are going to do about this?

Mr. PAYNE. I will say that the length of time that someone stays in an interim capacity has to be limited as much as possible. Just to give you an example from DOD's standpoint, in my area of jurisdiction right now is industry, cleared industry. Last year we issued 80,000 interim clearances to industry. Currently there is about 58,000 people on interim clearances.

If you look at the timeline that they have been involved or they have had their interim clearances, it ranges anywhere from six months to two years. But if you look at just the last year in terms of interim clearances, and I'll give you a couple of statistics here, 486 people from industry had their clearances denied last year, their main security clearance, their full security clearance. They were denied. Of those, 165 of those individuals had been granted interim clearances.

Now, during the process of the investigation information was developed during the investigation that resulted in us pulling the interim clearances of 151 of those individuals, and the remainder were individuals who did things after they received their interim clearances. So the risk—you could see the risk that is involved with

interim clearances and the need to reduce the amount of time that we have somebody in an interim capacity as much as possible.

Senator HARRIS. I agree.

Thank you.

Chairman BURR. Vice Chair.

Vice Chairman WARNER. One, I appreciate the panel, and I appreciate your answers, and the first panel as well. This is a high, high priority issue, I think, for all of us; and it is remarkably non-partisan. We've got to get this improved.

I will leave you with one—because it's been a long morning already, I will leave you all with one question for the record, because it was raised in the first panel, but we didn't get a chance to raise it today. I'd like to get a fulsome answer from each of you. I would argue that, particularly in an era of more and more open-source documents, we have to take a fresh look at the need to have over four million-plus people actually have to go through a clearance process of any type, and particularly the tremendous growth of TOP SECRET clearances versus simply SECRET.

So I'd like to hear back in writing from all of you, what can we do and what would be your policy recommendations so that we could not have so many people actually have to funnel through on the demand side on a going-forward basis, where more and more information is going to be out?

Thank you, Mr. Chairman. Thank you again for holding this in an open setting.

Chairman BURR. I thank the Vice Chairman. I thank all of the members. This is one of those issues that the membership of this committee has been extremely engaged on. I want to thank those first, the first panel members who chose to stay and listen to the government witnesses. I'm always shocked at the number of people that have the opportunity to testify and stay and choose not to do that. So I really respect the ones that do take the time to do that.

I thank all four of you for not only providing us your testimony today, but for the jobs you do. Mr. Payne, you've got a big job. Mr. Reid, you've led this charge. Mr. Phalen, you walked in. Not many people would take the job, and you have performed as well as one can do, and that's faced with losing 80 percent of your business down the road, knowing that.

Mr. Dunbar, I'm not sure you knew that you'd signed up for this when Director Coats asked you to come in. But this is—it's important. As we've chatted up here as other members have gotten an opportunity to question you, we're really confident that this might be a model that we're beginning to see that we can replicate and that the energy between you and Mr. Phalen, that exchange is going to happen, and that there's a real opportunity then for Director Coats to coalesce the rest of government towards this model.

The one thing—one word that didn't come up in the second panel, might have come up once or twice, that came up frequently in the first one, was "reciprocity," because there's nothing that either one of you are doing on both ends where it solves the problem of reciprocity within an agency or from agency to agency. I can tell you, we've got a security officer that got her security clearance at the State Department, but when she came to be security officer for us, the State Department said, "We don't have accreditation with

the CIA,” so she had to physically go pick up her paperwork and take it to the agency to be recognized.

You’d think in 2018 something like that wouldn’t exist. It’s bad enough that it does, but I think when we look at why are we doing this, it’s really not to solve that problem; it’s to make sure that the next generation of workers that are going to come through the pipeline actually want to do it and can do it, and they do it in a time frame that they’re accustomed to.

It always mystifies me that somebody is willing to share their entire life story, because they do. Right, Mr. Phalen? Everything’s out there to be exposed, because they believe in what they’re doing. I want to make sure the next generation has just as much passion about doing this.

We wouldn’t be quite as involved as a committee if it wasn’t for the passion of the Vice Chairman. He has been relentless on this. I think it’s safe to say that the committee—and I say this to you, Mr. Dunbar: I will take up with Director Coats—I will offer to Director Coats the committee being involved in the issue of reciprocity and how we bring agencies together to work through some of those things. It’s not that the Director doesn’t have the authority to do it. I think he’s in full agreement with us. But sometimes having a Congressional piece involved in those provides the Director an additional stick that he might not have without us. So I’ll make that offer to Dan, that we will be involved to that degree.

Mr. Reid, I hope that your history with us, which is at least annual updates, if not faster, that you will continue those, and that this committee will have a real inside look into the success of the model you’re setting up. Much of what we’re able to accomplish from this point forward is because of the investment that you’ve made, not only today, but prior to this, and we’re grateful for that.

With this, this hearing is adjourned.

[Whereupon, at 12:25 p.m., the hearing was adjourned.]

Supplemental Material

ENCLOSURE

Reducing the number of cleared positions. Please provide an update on the GAO's 2012 report and your 2013 testimony with regard to government positions requiring security clearances.

a. What progress has the government made and where do the greatest challenges remain? In which departments, agencies, and offices have there been the most progress, and where has there been the least progress?

The government has made some progress in reducing the number of positions that require security clearances in the federal government. As of October 1, 2016—the most recent data available—the Office of the Director of National Intelligence (ODNI) reported that there were approximately 4.08 million government and contractor employees, at nearly 80 executive branch agencies, that were eligible to hold a security clearance.¹ This amounts to a reduction of 20.8 percent since October 1, 2013.

The Intelligence Authorization Act (IAA) for Fiscal Year 2010 requires the President to submit an annual report on security clearance determinations to Congress. As part of this report, ODNI includes information on the number of federal and contractor employees who hold or are eligible to hold a security clearance. Table 1 provides data on the number of total eligible individuals for the four fiscal years for which data are available.

Table 1: Total Number of Federal and Contractor Employees Found Eligible to Hold a Security Clearance

Date	As of October 1, 2013	As of October 1, 2014	As of October 1, 2015	As of October 1, 2016
Number	5,150,379	4,514,576	4,249,053	4,080,726

Source: GAO analysis of ODNI reported data.

ODNI reported that decreases in the overall population that were eligible to hold a security clearance were the result of efforts across the government to review and validate whether an employee or contractor still requires access to classified information.

In our 2012 report,² we found that the Director of National Intelligence (DNI), as the Security Executive Agent, had not provided agencies clearly defined policy and procedures to consistently determine if a position requires a security clearance. Moreover, we found that the DNI had not established guidance to require agencies to review and revise or validate existing federal civilian position designations.

As a result, we made three recommendations to the DNI and the Director of the Office of Personnel Management (OPM) to:

1. issue clearly defined policy and procedures for federal agencies to follow when determining if federal civilian positions require a security clearance;
2. collaborate in their respective roles as Executive Agents to revise the position designation tool to reflect that guidance; and
3. issue guidance to require executive branch agencies to periodically review and revise or validate the designation of all federal civilian positions.

¹ODNI, *Fiscal Year 2016 Annual Report on Security Clearance Determinations*. This report was issued in 2018.

²GAO, *Security Clearances: Agencies Need Clearly Defined Policy for Determining Civilian Position Requirements*, GAO-12-800 (Washington, D.C.: July 12, 2012).

ENCLOSURE

In 2017, we closed all three recommendations as implemented, as described below.

- With regard to the first recommendation to define policy and procedures for federal agencies to follow when determining if a security clearance is required for a position, the DNI and Director of OPM proposed a new chapter and part to the Code of Federal Regulations (CFR) clarifying the position sensitivity designation of national security positions. Part 1400 of 5 CFR, *Designation of National Security Positions*, became effective on July 6, 2015, and provides departments and agencies with more detailed guidance on designating national security positions for federal civilian positions. Specifically, the regulation applies to the designation of executive branch national security positions within 1) the competitive service, 2) the excepted service where the incumbent can be noncompetitively converted to the competitive service, and 3) career appointments in the Senior Executive Service. Subsequently, OPM and ODNI issued an implementing memorandum in May 2016, which outlined actions that agencies must take, such as conducting an initial assessment of covered positions within 24 months of July 6, 2015, to ensure they were properly designated in accordance with the new regulation. Under the regulation, positions may be designated as national security positions whether or not they require eligibility for access to classified information. A need for access to classified information is one factor in designating a position as a national security position and determining the relevant sensitivity level of the position.
- With regard to the second recommendation to revise the position designation tool, in November 2015, OPM released an updated Position Designation Automated Tool that addressed our recommendation. The tool and the accompanying glossary both indicate that they are based, in part, on 5 CFR Part 1400. Specifically the tool restates that each position in the Federal service must be evaluated for a position sensitivity designation commensurate with the responsibilities and assignments of the position as they relate to the impact on national security. Such responsibilities and assignments include, but are not limited to, access to classified information (i.e., Confidential, Secret, or Top Secret).
- With regard to the third recommendation to issue guidance to require executive branch agencies to periodically review and revise or validate the designation of all federal civilian positions, OPM and ODNI issued an implementing memorandum in May 2016. This memorandum outlines actions that agencies must take, such as conducting an initial assessment of covered positions within 24 months of July 6, 2015, to ensure they were properly designated in accordance with the new regulation. In addition, the implementing memorandum's distribution list identifies affected agencies and an attachment identifies changes and differences between 5 CFR Part 1400 and the previous regulation.

We have not independently assessed the progress made by individual agencies or departments in reviewing their respective positions or any corresponding decrease in the number of positions requiring security clearances.

b. What current processes are in place for reducing the number of government positions requiring a security clearance and lowering the clearance level for positions that do require clearances?

As noted in the response to the previous question, OPM and ODNI issued an implementing memorandum in May 2016 regarding designation of national security positions, which would include positions requiring access to classified information. This memorandum outlined actions that agencies must take—such as conducting an assessment of covered positions within 24 months of July 6, 2015—to ensure they were properly designated in accordance with the new regulation, 5 CFR Part 1400. Accordingly, agencies had until July 6, 2017, to determine whether changes in position sensitivity designations were necessary for then-current positions.

Additionally, 5 CFR Part 1400 provides guidance for determining national security positions, and requires the evaluation of positions for a position sensitivity designation commensurate with the responsibilities and assignments of the position as they relate to the impact on national security. National security positions include, but are not limited to, those requiring eligibility for access to classified information.

ENCLOSURE

Furthermore, section 925(h) of the National Defense Authorization Act for Fiscal Year 2018, requires the Secretary of Defense to:

- review Department of Defense (DOD) requirements relating to position sensitivity designations for contractor personnel in order to determine whether such requirements may be reassessed or modified to reduce the number and range of contractor personnel who are issued security clearances in connection with work under contracts with the department; and
- issue guidance to program managers, contracting officers, and security personnel of the department specifying requirements for the review of contractor position sensitivity designations and the number of contractor personnel of the department who are issued security clearances for the purposes of determining whether the number of such personnel who are issued security clearances should and can be reduced.

May 25, 2018

The Honorable Richard Burr
Chairman
Senate Select Committee on Intelligence
211 Hart Senate Office Building
Washington, DC 20510

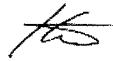
The Honorable Mark Warner
Vice-Chairman
Senate Select Committee on Intelligence
211 Hart Senate Office Building
Washington, DC 20510

Dear Chairman Burr and Vice Chairman Warner:

On behalf of the industry community, we thank you again for your leadership in addressing the critical national security issue of security clearance reform. Below is ManTech's response to your Question for the Record on reciprocity, received May 5, 2018.

I would be happy to discuss any additional questions you may have.

Sincerely,



Kevin Phillips
President & Chief Executive Officer
ManTech International

Q: Reciprocity: The Committee is concerned that the Government policies intended to result in prompt reciprocity may not, in fact, operate promptly in practice. Understanding that there could be proprietary and privacy restrictions on certain data categories, can you please provide data for ManTech, and any companies with whom you coordinated your testimony, regarding how long it takes for personnel to transport clearances issued at the same level between agencies? Can you identify what may contribute to delays, e.g., specific additional investigative requirements at certain agencies?

A: Data: Industry clearance timeline data for the last six months are shown in the table below. The data includes approximately 2,000 instances of clearance cross-overs – from ManTech and five of the other companies who approved ManTech’s SSCI testimony on March 7, 2018. The data was presented to the Industry-PAC/PMO “Tiger Team” on reciprocity. The PAC/PMO team confirmed that this data accurately reflects the general industry experience with crossovers. The data includes both reinstatements within the same agency (i.e. when an employee moves from one contract to another), as well as crossovers between agencies. This tends to actually skew the crossover averages lower. All industry partners that provided data have an excellent pre-screening program, which ensures clean cases are submitted, although Industry does not have access to derogatory information held by the Government. The timelines below start from when the requested paperwork is initiated to when the cleared contractor is briefed into the position.

Gaining Agency	Crossover Industry Average (days)	Crossover Industry Average for Longest 10% of cases (days)
DIA	20	90
NRO	15	67
NSA	30	174
NGA	16	50
CIA	12	32
ODNI	18	44
DHS	87	223
DoD (SCI)	44	300

Conclusion from Data: Industry data confirms the Committee’s concern that government policies intended to ensure prompt reciprocity are not, in fact, resulting in prompt reciprocity in practice. As the table indicates, Industry’s experience is that prompt reciprocity between Government agencies is the exception rather than the rule.

Factors Contributing to Delay: The key contributing factor to delays is that application processes, adjudication standards, and investigative requirements for positions of trust (National Security Access, Suitability & Fitness and Credentialing) vary widely between Government agencies. Moreover, Industry has limited visibility into these standards.

Government agencies do not automatically accept reciprocity from another agency until they review the eligibility database, receive the transfer of the investigative case file, and re-adjudicate against agency specific standards. A current example of this is the extreme delays in transferring individuals cleared for TS/SCI with at least CI polygraph from NSA to U.S. Cyber Command. While we lack extensive data on transfers to the command, one contractor reports that out of 31 crossover cases in the past 6 months, the average approval time for U.S. Cyber Command is 179 days.

Other factors contributing to delays in prompt, reciprocal transfers include:

- Delays in the transfer of security files between Government agencies
- Re-vetting of personnel that hold equivalent or higher eligibility (DHS Suitability & Fitness Determinations)
- Delays in Contractor Officer Representative (COR) coordination and approval for access
- Lack of industry visibility into exceptions, deviations, waivers or derogatory information in Government eligibility systems
- Manual legacy business practices
- Zero defect adjudicative objectives
- Un-adjudicated information in the case file
- Pending incident reports
- Out of Scope investigation or polygraph
- Agency's additional paperwork and processing requirements
- Program-specific, risk-based vetting requirements
- Time to schedule Government briefings after approval
- Adverse or derogatory information in the case file (legitimate factor)

Recommendations to Promote True Reciprocity: Industry strongly recommends one simple, universally-accepted and enforced set of standards for national security access, suitability & fitness and credentialing across all of Government to increase efficiency and promote reciprocity.

The Security and Suitability Executive Agents should ensure that Government agencies implement their policies and procedures uniformly and consistently to ensure appropriate uniformity, centralization, effectiveness and timeliness. These Executive Agents should own the standards overseeing execution – they should not just promulgate the policies. They should ensure reciprocal recognition among agencies and establish mechanisms for crossovers for vetted individuals to be done routinely, timely and automatically. As time matters to the mission, they should minimize any deviations or additions to these uniform standards.

Finally, the Administration and Congress should establish ambitious timeline goals for reciprocity and should routinely track and collect data on cross-over clearances against these goals. This capability should be incorporated into the planned National Background Investigation System (NBIS).

**QUESTIONS FOR THE RECORD
DIRECTOR CHARLES PHALEN JR.
NATIONAL BACKGROUND INVESTIGATION BUREAU, OFFICE OF
PERSONNEL MANAGEMENT
SENATE SELECT COMMITTEE ON INTELLIGENCE
OPEN HEARING ON SECURITY CLEARANCE REFORM
MARCH 6, 2018**

Chairman Burr & Vice Chairman Warner

1. Potential Rise in Prices. What is the anticipated price increase to agencies for your services after DoD personnel background investigations move to the Defense Security Service? What assumptions are you making?

Response: NBIB estimates the prices of investigative products and services performed by NBIB could increase up to 18 percent after DoD completes its 3-year phased transition and assumes full responsibility of their background investigations. This estimate assumes NBIB continues to perform all non-DoD background investigations, which is approximately 30 percent of NBIB's current workload. It also assumes NBIB will retain its current inventory, which includes DoD background investigations.

Since the March 6, 2018 hearing, the Administration has expressed its desire to keep the national-level investigative infrastructure intact and move responsibility for the remaining 30 percent of the NBIB workload to DoD. NBIB has not yet fully assessed the pricing in such a scenario, but strongly believes that top line pricing would remain far more stable with minimal, if any, increases.

2. Public Reporting. How do you share progress on addressing the background investigation inventory with agencies, cleared industry, and other stakeholders?

Response: NBIB takes advantage of all opportunities to share progress on addressing the background investigation inventory with agencies, cleared industry, and other stakeholders. NBIB routinely meets with the Performance Accountability Council (PAC), Background Investigations Stakeholders Group, Customer Advisory Board, and the National Industrial Security Program Policy Advisory Committee to provide updates on the current background investigation inventory and ongoing initiatives to reduce and mitigate the backlog. Additionally, NBIB leverages government and industry forums such as the National Defense Industrial Association (NDIA), Aerospace Industries Association (AIA), National Classification Management Society (NCMS), Professional Services Council (PSC), the Intelligence and National Security Alliance (INSA), and the Center for Strategic and International Studies (CSIS) to communicate mission status and engage directly with industry.

NBIB also provides inventory metrics that are publicly released to Performance.gov on a quarterly basis.

3. Quality of Applicant Investigative Materials. The Committee understands that quality and accuracy of data contained in applications that agencies submit for background investigations can vary. How are you providing incentives for agencies to improve the data submitted with those applications?

Response: In FY17, NBIB initiated a reporting effort focused on improving the quality of packages submitted by customer agencies. NBIB identifies and informs customer agencies of their most common mistakes, enabling each agency to determine actions to improve submission quality.

Additionally, NBIB provides best practice advice to agencies to improve submission quality, which has resulted in a 65 percent decline in unacceptable case receipts from the participating agencies. By March 2018, NBIB was positioned to offer this advice to all customer agencies for their immediate use.

Sen. Martin Heinrich

1. Mr. Phalen, prior to the hearing I was told that about a dozen investigators from the National Background Investigation Bureau (NBIB) were physically on site at Sandia and at Los Alamos and planned to be there for two months.

a. Please provide data indicating the backlog eradication goals of the NBIB team going into both locations and what the teams actually accomplished.

Response: Since October 2016, NBIB has sent teams of agents in intervals, totaling approximately 70 agents, to support the workload mitigation efforts at Sandia and Los Alamos. In total, 1,588 cases have been identified as part of these efforts. Most recently, NBIB, in coordination with the National Nuclear Security Administration (NNSA), conducted simultaneous, focused surges at Los Alamos and Sandia. The goal was to work as many NNSA-identified, mission-critical investigations as possible during the surge. The cases in these efforts were primarily Top Secret initial and reinvestigation cases, which are the most labor-intensive, and were predominately in support of Q-level security clearances.

In Los Alamos, NNSA and NBIB identified approximately 606 cases as targets of opportunity. These cases were prioritized according to need, based on NNSA input, and used a plan formulated to address this population in an initial two-month surge. The 606 cases identified for the first surge contained approximately 10,500 items. As of May 4, 2018, 8,059 (77 percent) items have been completed, including 537 subject interviews, the most time consuming portion of the investigations.

In Sandia, NNSA and NBIB identified approximately 433 cases as targets of opportunity in a two-month initiative, which included 6,311 items. As of May 4, 2018, 5,760 (91 percent) items were completed.

b. Please provide updated data as to remaining backlogs at both sites, in particular related to “Q” clearances.

Response: As of May 7, 2018, the inventory of “Q” clearances at each site is as follows:

- Los Alamos – 3,524
- Sandia – 3,792

2. During the hearing, you told Vice Chairman Warner that NBIB started a “surge” at the Department of Energy, while in other places you've instituted “hubbing.”

a. Please explain the difference between “hubbing” and a “surge.”

Response: Both terms refer to strategies used to accelerate the completion of background investigations efficiently and effectively by moving extra personnel into an area to address concentrations of investigative work. “Hubbing” refers to prioritizing investigations for specific personnel and involves direct collaboration with an agency, industry partner, or facility to centralize locations for staging and conducting background investigations. Among the advantages of this strategy is reduced travel time for investigators, increased accuracy of the paperwork, and more efficient collection of needed documentation and conducting of interviews.

“Surges” represent the targeting of a geographic area for the purpose of general inventory mitigation; to address a specific population of investigations, a concentration of pending investigative work in general, or a specific facility. Surging allows for local assets to be supplemented but involves less direct coordination with one specific facility or customer. NBIB addresses the need to surge by both temporary increases to personnel through TDY and through increased hiring of investigators in traditionally high volume work areas.

b. When do you use one approach instead of another?

Response: These approaches are synergistic, and should be used together when possible. The decision to use a hub or surge is predicated on multiple factors, but is most often dependent upon the needs of the customer and the allocation of NBIB resources at the location(s) in question.

If an agency has a high volume of cases within the vicinity of a major facility, and requires a significant acceleration of those clearance investigations in very high numbers, the hubbing concept will most likely be used.

If an agency requires a specific inventory of investigations be completed, and the geographic location is confined or limited to a specific facility, a surge would be more appropriate.

c. Are these efforts ad hoc, or is there a master plan and dedicated funding to deploy these investigator teams in these particular focused ways?

Response: These efforts are not ad hoc, they are planned in advance based on workload. There is no additional funding needed to support any of these efforts outside of the approved FY2018 budget and pricing.

d. What criteria does NBIB use to select “hubbing”/“surge” sites?

Response: The specific criteria used to select a hub or a surge, in conjunction with the assessment explained within Question 2b, would include:

- The number of cases targeted or requested for prioritization by the customer agency;
- The number of local agent resources available;
- The number of agent resources required to be sent on TDY;
- The existence of a specific facility or campus that could serve as the epicenter of the effort;
- The amount of available interview space to accommodate an increased number of agent resources; and
- The overall purpose of the effort (general backlog reduction or prioritization of specific personnel).

e. How does “hubbing” or a “surge” compare to traditional interview methods, in terms of cost?

Response: Hubbing and Surging provide NBIB an increase in time efficiency and savings to man hours by reducing travel time and focus and maximize effectiveness by targeting areas of concentrated fieldwork across the United States and in select overseas locations. Although there is an additional cost incurred by NBIB by sending agents to locations outside their local offices, these investments generate a measurably higher yield of cases completed. Additionally, the benefit of improved timeliness adds value to the entire process. Investigative resources can also be supplemented with contractor personnel to accommodate larger case inventories and increase the overall yield of a hub. Such reinforcement results in no added cost to NBIB outside the per-case expense paid to the contractors.

f. Please provide data indicating where and when NBIB has used both approaches to date, what NBIB's goals have been going into each “surge” or “hubbing” exercise, and what the actual outcomes have been at each site.

Response: To date, 817 agents have contributed to the overall surge and hub efforts. These initiatives have contributed to the advanced assignment and output of 21,968 cases since April 2016. The locations and dates of each exercise is provided in the following chart.

Surge / HUB	Date	Surge / HUB	Date
Washington, DC (NW)	4/10/2016	Livermore, CA	1/9/2017
Colorado Springs, CO	4/10/2016	Houston, TX	2/6/2017
Washington, DC	4/17/2016	Pentagon	2/6/2017

Washington, DC (NW/VA)	5/1/2016	China Lake, CA	9/1/2017
Washington, DC (NW)	5/31/2016	Dayton, OH	10/1/2017
Washington, DC (NW/VA)	5/31/2016	Groton, CT (Navy)	11/1/2017
Washington, DC (Pentagon)	6/5/2016	Lackland AFB, TX	12/16/2017
Chicago, IL	7/11/2016	Capitol Hill	2/1/2018
Los Angeles, CA	7/11/2016	DOE Lynchburg	2/1/2018
Alexandria, VA	7/11/2016	Sandia	2/1/2018
Livermore, CA	8/8/2016	NASA	2/12/2018
Monterey, CA	8/8/2016	DOE Honeywell	2/26/2018
Arlington, VA	8/8/2016	DOE Oak Ridge	2/26/2018
Northern VA (Field IA)	9/12/2016	Los Alamos, NM	3/1/2018
San Antonio, TX	9/12/2016	Patent & Trademark	3/1/2018
Florida Panhandle	9/12/2016	USAF Academy, CO	3/1/2018
Washington, DC	9/12/2016	AF Warner Robins, GA	3/19/2018
Washington, DC	10/3/2016	Army Fort Bragg, NC	3/26/2018
Hawaii	10/3/2016	Hill AFB, UT	4/1/2018
Seattle, WA	10/3/2016	Los Angeles AFB, CA	4/1/2018
New York City, NY	10/23/2016	Tidewater	4/1/2018
Amarillo, TX	10/23/2016	Education – Nelnet	4/9/2018
Los Alamos, NM	10/23/2016	Navy Corry Station, FL	4/9/2018
New York City, NY	1/9/2017		

3. Mr. Phalen, Sandia National Labs has been exploring a number of avenues to mitigate the impacts of long clearance wait times. One of the efforts has been to submit Mission Critical requests for clearances that have been pending over one year in an attempt to expedite those clearances. Sandia has also begun paying a \$500 fee to prioritize these Mission Critical requests - on top of the other costs associated with a clearance. I am told that the current time to grant a priority Q clearance at Sandia is now 253 days – lower than Sandia's average of 338 days. That is progress, but there is still room for improvement.

a. Please explain how NBIB works with agencies on “mission critical” clearance requests - how are these requests identified and prioritized? What guidance does NBIB provide to agencies on these requests?

Response: NBIB works collaboratively with agencies to identify target investigation populations that warrant the establishment of hub or surge efforts. An assessment is made of available agent resources in a specific area, and a determination of the number of incoming TDY agents to be surged is made to meet the demand of the identified case inventory. Facilities are evaluated for both available interview space and ease of access for agents to use the facilities throughout the effort.

Once the agency identifies its mission-critical needs and target cases are collated, NBIB develops a timeline with which to execute the plan. This involves setting a defined start date, engaging local POCs so they are ready to receive NBIB personnel at their facilities,

planning the assignment and completion of investigations based on the availability of subjects and sources, and allowing for triage when needs of the customer agency change during the effort.

- b. Please explain the fee structure for prioritized requests. Are agencies charged fees for expedited clearances even if the processing time is not significantly reduced? Are agencies promised a specific outcome in return for the fee they pay?

Response: NBIB offers Priority Service for an additional fee for T2S, T4, and T5 case types and their associated reinvestigation case types. For Priority Service, NBIB charges an additional 8 percent above the Standard Service rate. NBIB prioritizes execution of Priority Service requests above all Standard Service requests. Although NBIB does not promise agencies a specific outcome or reduced timeframe to deliver a completed case, a completed Prioritized Service casework request is typically 50 percent to 60 percent faster than a Standard Service request.

NBIB publishes billing rates for Priority Services via Federal Investigative Notices (FIN). The FY2018 Investigations Reimbursable Billing Rates can be found here: <https://nbib.opm.gov/hr-security-personnel/federal-investigations-notices/2017/fin-17-04.pdf>

4. Mr. Phalen, the unique national security mission of the DOE defense labs depends on attracting the best and brightest scientists and engineers. One of the biggest obstacles to recruitment continues to be the long wait times for security clearances. The rate of hiring at the two NNSA labs in New Mexico is about 1,000 per year, and wait times for clearances are averaging well over a year. This makes it difficult for the labs to attract the quality workforce they need to meet critical national security missions.

- c. What action is NBIB taking to specifically address the backlog in DOE Q clearances at the national labs?

Response: In 2018, to address the backlog at the DOE National Labs, NBIB worked closely with DOE NNSA personnel at both Los Alamos and Sandia National Labs to develop a collaborative approach to target mission-critical needs. NBIB and NNSA developed a plan to identify mission-critical cases; organize cases by project and supervisor to optimize investigation efficiency; organize lab support for the effort with administrative staff and interview rooms; and dedicate specific investigative resources to the project. NBIB dedicated a workforce to the labs for a two-month push to accomplish the work on these cases. Although this most recent initiative ended on May 4, 2018, follow-up efforts at both labs will continue in the near future.

Additional focus efforts have taken place at other DOE locations such as Oak Ridge, Lynchburg, and Kansas City. NBIB has also identified Lawrence Livermore National Lab as the next DOE site for a focused effort (surge), potentially in June.

Sen. Ron Wyden

1. Reducing the Number of Cleared Positions. Please describe progress made in reducing the total number of government positions requiring a security clearance and lowering the clearance level for positions that do require clearances. In which departments, agencies and offices have there been the most progress, and where has there been the least progress? Are there target goals to reduce the number of positions requiring a clearance? If yes, what current processes are in place for achieving any of these goals?

Response: The President has designated the Director of National Intelligence as the Security Executive Agent, and made him responsible for the standards governing security clearances. This question would best be directed to the ODNI.

Hearing Date: 6 March 2018
 Committee: SSCI
 Member: Senators Burr and Warner
 Witness: ODNI/NCSC, Mr. Brian D.
 Info Current as of: July 2, 2018

Question 1: Compliance & Enforcement.

Question 1a: Is the Security Executive Agent (SecEA) responsible for reviewing each government agency's compliance with laws, executive orders, and policies regarding the security clearance process? If yes, does this duty include reviewing the policies for reciprocity and/or the robustness of programs for continuous evaluation and insider threat?

Answer: Yes, the Security Executive Agent (SecEA), is responsible for conducting Executive Branch oversight of investigations and adjudications for personnel security clearances. This includes development and implementation of uniform and consistent policies and procedures; standardization of security questionnaires, financial disclosure requirements, polygraph policies and procedures, and reciprocal recognition of accesses to classified information. The SecEA is also the final authority for designating an authorized investigative or authorized adjudicative agency. This oversight includes the establishment of policies for continuous evaluation and insider threat programs, as well as monitoring compliance.

Question 1b: Which agency's processes does the SecEA review? How often is this review conducted?

Answer: In executing SecEA oversight responsibilities, on April 29, 2014, the DNI established the Security Executive Agent National Assessment Program (SNAP) to review department and agency (D/A) personnel security programs in the areas of security clearance initiation, investigation, adjudication, and application of due process. The annual review process assesses select D/A compliance with the policies and procedures governing the conduct of investigations and adjudications of eligibility for access to classified information or eligibility to hold a sensitive position government-wide. In addition, the ODNI regularly reports to Congress, via Congressionally Directed Actions on our processes and performance.

Question 1c: What assessments or reports does the SecEA issue to the agency or to Congress on such compliance?

Answer: The DNI has responded to Congressionally Directed Actions mandated in the 2010-2017 Intelligence Authorization Acts on numerous topics related to security clearance timeliness, backlog, reciprocity, and security clearance determinations for the Executive Branch. The following is a current list of these CDAs: Improving the Periodic Investigation Process, Security Clearance Determinations, Resolution of Backlog of Overdue Periodic Reinvestigations, Assessment of Timeliness of Future Periodic Reinvestigation, Insider Threat, and Continuous Vetting, Enhancing Government Personnel Security Programs - Implementation Plan.

Question 1d: What are the SecEA's means of enforcing compliance at a particular agency (e.g. through budgets, withholding certain certifications)?

Answer: The SecEA is given authority in Executive Order (E.O.) 13467, as amended, to designate an investigative or adjudicative agency. The SecEA may rescind a D/A's investigative or adjudicative authority if it is unable or unwilling to comply with applicable standards. The SecEA personally issues a letter to each agency head to inform them of their annual security program performance. If an agency does not meet performance goals, the agency head is required to submit a Corrective Action Plan with milestones and a

date of completion. The SecEA staff follows up with these organizations regularly until they achieve compliance and the desired end-state.

Hearing Date: 6 March 2018
 Committee: SSCI
 Member: Senators Burr and Warner
 Witness: ODNI/NCSC, Mr. Brian D.
 Info Current as of: July 2, 2018

Question 2: Trusted Workforce 2.0.

Question 2a: Who is involved in the DNI-led "Trusted Workforce 2.0" initiative? Are representatives from industry, think tanks, Government Accountability Office, or Congress involved?

Answer: The Trusted Workforce 2.0 initiative is led by the SecEA and Suitability Executive Agent (SuitEA) in concert with the other Performance Accountability Council (PAC) Principal Organizations, the Office of Management and Budget, the Office of the Undersecretary of Defense (Intelligence) and the National Background Investigations Bureau. Trusted Workforce 2.0, which began in March 2018, is supported by Executive Branch senior leadership, change agents, and innovative thinkers from government and industry.

Question 2b: What is the scope of the "Trusted Workforce 2.0" effort?

Answer: Trusted Workforce 2.0 is a fulsome, "clean slate" review of the vetting enterprise. The initiative will serve as the foundation for a trusted workforce while keeping pace with emerging technologies, capabilities, and opportunities to continuously identify, assess, and integrate key sources of information. Trusted Workforce 2.0 will chart a bold path forward for transforming the vetting enterprise in the areas of policy, governance, business processes and modernization of information technology architecture. This aggressive effort may require additional resources from Congress. We look forward to partnering with agency leadership and private industry to transform our vetting enterprise into a system that protects our nation's sensitive equities and meets the needs of the workforce.

Question 2c: Will the DNI initiative produce any recommendations or policy changes?

Answer: Yes. The intent of Trusted Workforce 2.0 is to identify the way forward in improving the quality, timeliness, and performance of the personnel security vetting process while incorporating new capabilities and approaches. This effort will require changes to existing policies and, potentially, the statutes governing those policies.

Hearing Date: 6 March 2018
 Committee: SSCI
 Member: Senators Burr and Warner
 Witness: ODNI/NCSC, Mr. Brian D.
 Info Current as of: July 2, 2018

Question 3: Reciprocity. Security Executive Agent Directive 4 on reciprocity contains an Appendix C that allows agencies substantial latitude in levying additional requirements before accepting a clearance. The SecEA provides data on reciprocity for the Intelligence Community (IC) pursuant to Sec. 504 of the *Intelligence Authorization Act for Fiscal Year 2014*, but not the rest of government.

Answer: Security Executive Agent Directive (SEAD) 4, *National Security Adjudicative Guidelines*, Appendix C, identifies exceptions to the adjudicative guidelines. These exceptions are defined as “an adjudicative decision to grant initial or continued eligibility for access to classified information ... despite failure to meet the full adjudicative or investigative standards.” Appendix C lists the specific exceptions: Waiver, Condition, Deviation, or Out of Scope. While the existence of an exception in a national security determination can affect the application of reciprocity, the cited SEAD and appendix do not specifically address reciprocity.

NCSC has drafted SEAD 7, *Reciprocity of Background Investigations and National Security Adjudications*. This directive will provide reciprocity guidance and procedures for government-wide use. The requirements of 50 U.S.C. 3341(b, d), and E.O. 13467, as amended, serve as the basis for the DNI to provide reciprocity guidance for agencies. The draft SEAD has cleared internal ODNI review and is currently in the formal OMB policy coordination process.

Question 3a: As the SecEA, can you please detail what additional requirements IC and non-IC agencies require, by agency, at each clearance level?

Answer: The requirements for secret and top secret clearance reciprocity are the same for IC and non-IC agencies and are consistent with OMB and Intelligence Community Policy Guidance. The SecEA issued E/S 01074, “Executive Order 13467 (as amended) and Reciprocal Recognition of Existing Personnel Security Clearances,” dated October 1, 2008. This memorandum endorses the guidance provided in the OMB memorandum. SEAD 7, when issued, will standardize policies and procedures for individuals eligible for access to classified information or eligible to hold a sensitive position across the Executive Branch.

Question 3b: As the SecEA, can you please provide data on the time it takes to for both government and industry personnel at the same level (e.g., SECRET, TOP SECRET, SCI) to transfer a clearance from an IC agency to an agency beyond the IC?

Answer: Currently, the SecEA does not capture clearance cross-over timeliness from the IC to non-IC agencies as reciprocity data is not collected from agencies outside of the IC. SecEA’s reciprocity reporting for the whole of government is pending issuance of SEAD 7. Data from current reporting is limited to the IC, and the cases are Top Secret or Top Secret/SCI. In fiscal year 2017, the average IC processing time for reciprocity was 8.2 days. Once SEAD 7 is issued, it will provide standardized metrics requirements for IC and non-IC agencies.

Question 3c: Why is it possible for clearance delays to exist within an agency when a cleared individual, either government or contractor, switches projects within the same agency?

Answer: Many variables can affect clearance transfers for government employees and contractors. An individual may have a security clearance that is ineligible for reciprocity, the access may not be at the correct

level for the new position, or there may be suitability aspects of the position that require review of the original access determination.

Hearing Date: 6 March 2018
Committee: SSCI
Member: Senators Burr and Warner
Witness: ODNI/NCSC, Mr. Brian D.
Info Current as of: July 2, 2018

Question 4: Government v. Contractor Personnel.

Question 4a: Under existing policy, is a contractor who is "out of scope" for her background investigation treated differently than a government employee who is "out of scope," when moving jobs or contracts? If so, please describe how this treatment differs.

Answer: While the personnel security vetting process is very similar for contractors and government employees, the process is the same for out of scope background investigations between contractors and government personnel. However, individual circumstances and position requirements can impact security determinations. An "out of scope" background investigation can impact eligibility for reciprocity. A contractor with an out of scope background investigation could potentially move from one contract to another with the same sponsoring agency, but may not be accepted on a contract sponsored by another agency. Likewise, a government employee with an out of scope background investigation may be eligible to change jobs within their agency, while their clearance may not be accepted as part of a transfer to another agency. Suitability for employment or fitness for a position may also be a consideration.

Question 4b: Can an agency have one policy for use of the polygraph for its cleared government population and a different policy for its contractor community? If so, please provide an example.

Answer: Yes. The application of polygraph in the national security vetting process is governed by SEAD 2, *Use of Polygraph in Support of Personnel Security Determinations for Initial or Continued Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position*. Consistent with that directive, agencies structure their polygraph programs and may use any of the approved types of polygraph. While SEAD 2 does not prohibit disparate application of a given polygraph technique to government employees and contractors, NCSC would defer to individual agencies to discuss the specifics of their programs.

Hearing Date: 6 March 2018
Committee: SSCI
Member: Senators Burr and Warner
Witness: ODNI/NCSC, Mr. Brian D.
Info Current as of: July 2, 2018

Question 5: Transparency. The ODNI's most recent report on security clearance determinations was marked FOUO, in contrast to the previous version of this report, which was only UNCLASSIFIED.

Question 5a: Can you please explain what caused the change in the handling caveat?

Answer: Yes. The most recent report provided data in greater detail than in prior reports. Due to the sensitivity of the data presented, as well as the potential benefit possession of that data would provide to adversaries, a determination was made that report would be marked FOUO.

Hearing Date: 6 March 2018
 Committee: SSCI
 Member: Senators Burr and Warner
 Witness: ODNI/NCSC, Mr. Brian D.
 Info Current as of: July 2, 2018

Question 6: Clearance Portability. Is there a reason why the government cannot treat security clearances like a 401(k) that travels with the person, rather than holding the clearances at a particular government agency?

Answer: The government actually does treat security clearances in a manner very similar to a 401(k). Clearances are granted and managed by a sponsoring agency. Sponsorship includes managing the security clearance determination, reporting requirements, continuous evaluation, training, and other oversight responsibilities. While sponsorship rests with a single agency, current reciprocity guidelines direct D/As to reciprocally accept the national security determination and/or the background investigation of an individual if it is of a similar type and is within proscribed age limits. D/As are required to check for the existence of a valid background investigation prior to requesting a new one and to utilize a favorable national security determination to meet a national security access requirement. D/As are also required to document background investigations and adjudications in one of the national databases. Thus, an individual's security clearance is accessible and transportable within the existing personnel security vetting process. The issuance of SEAD 7 will support consistent application of reciprocity.

Hearing Date: 6 March 2018
Committee: SSCI
Member: Senator Wyden
Witness: ODNI/NCSC, Mr. Brian D.
Info Current as of: July 2, 2018

Question 1: Transparency. The ODNI released to the public the 2015 Annual Report on Security Clearance Determinations.

Question 1a: Does the ODNI intend to release the 2016 and subsequent reports?

Answer: Yes and did so on the ODNI's website in March of this year.

Question 1b: If not, why not?

Answer: N/A

Hearing Date: 6 March 2018
 Committee: SSCI
 Member: Senator Wyden
 Witness: ODNI/NCSC, Mr. Brian D.
 Info Current as of: July 2, 2018

Question 2: Reducing the Number of Cleared Positions. Please describe progress made in reducing the total number of government positions requiring a security clearance and lowering the clearance level for positions that do require clearances. In which departments, agencies, and offices have there been the most progress, and where has there been the least progress? Are there target goals to reduce the number of positions requiring a clearance? If yes, what current processes are in place for achieving any of these goals?

Answer: The SecEA initiated actions to better manage the size of the cleared national security population. On an ongoing basis, the SecEA reminds D/A heads to review and validate individuals' need for access to classified information. As a result of the SecEA's coordination with agency heads, the eligible national security population has decreased from approximately 5.1 million on October 1, 2013, to roughly 4.0 million on October 1, 2017 -- approximately a 20% decrease in the size of the cleared population. The intent is to ensure the national security population is "right-sized," not simply reduced.

The Department of Defense (DoD) has the largest population of personnel with national security eligibility. A majority of the reduction in the national security population resulted from data integrity efforts at DoD that removed personnel who were no longer affiliated with DoD or no longer required national security eligibility.

There are no target goals for security clearances. Rather, the approach seeks to ensure that the Executive Branch has the correct number of personnel with the appropriate security clearances. In support of these efforts the SecEA and the SuitEA jointly revised Title 5 Code of Federal Regulations Part 732 (5 CFR 732), "National Security Positions," and reissued it as 5 CFR 1400, "Designation of National Security Positions in the Competitive Service, and Related Matters." This effort provided greater clarity for D/As in classifying positions requiring national security eligibility. The OPM Position Designation Tool was revised to incorporate the guidance in 5 CFR 1400, and all Executive Branch D/As were required to review existing position designations using the 5 CFR 1400 standards. These efforts seek to ensure that Executive Branch positions are properly designated and that they validate requirements for national security eligibility. The SecEA continues efforts to ensure there is a sufficient number of individuals with the appropriate clearances to meet mission requirements while ensuring unnecessary clearances are not maintained.

Hearing Date: 6 March 2018
 Committee: SSCI
 Member: Senator Wyden
 Witness: ODNI/NCSC, Mr. Brian D.
 Info Current as of: July 2, 2018

Question 3: Whistleblowers. On June 18, 2014, Senator Grassley and I wrote the DNI about the potential impact of continuous monitoring and continuous evaluation on whistle blower protections. On July 25, 2014, the DNI responded that "some agencies" were training investigators and that the National Insider Threat Task Force had issued guidance emphasizing legal protections afforded whistleblowers. The DNI further wrote that "the Inspector General of the Intelligence Community, in coordination with the Intelligence Community Inspectors General Forum, is currently examining the potential for internal controls that would ensure whistleblower-related communications remain confidential, while also ensuring the necessary UAM [user activity monitoring] occurs." Please detail any guidance, mechanisms, or procedures related to the controls the Intelligence Community and each of its component entities have implemented to ensure that any security-related personnel monitoring does not compromise the confidentiality of whistleblower-related communications.

Answer: On May 17, 2018, Michael Atkinson was sworn in as the second Senate confirmed Inspector General of the Intelligence Community (IC IG). Since that time, Mr. Atkinson has been reviewing the data available to him regarding the IC IG whistleblowing program and, also, the Intelligence Community Inspectors General Forum (IC IG Forum). With respect to this specific question, he has not located records establishing that the Forum undertook an examination of internal controls to ensure whistleblower-related communications remain confidential, while also ensuring the necessary user activity monitoring (UAM) occurs. During his confirmation process, Mr. Atkinson committed to undertake, in coordination with the IC IG Forum, an immediate review of whistleblower complaints being handled currently by the IC IG and other IC IG Forum members to ensure they are receiving appropriate resources, attention, and priority. The IC IG will also work with the ODNI and the IC IG Forum to identify best practices and procedures governing UAM to enable and encourage lawful whistleblowing while respecting the required balance with insider threat monitoring.

The National Insider Threat Task Force (NITTF) incorporates the importance of privacy, civil rights and civil liberties protections into all training and guidance materials, as well as all of its briefings and presentations. Although whistleblower protections were not uniformly addressed separately in earlier documentation, modifications were made within the past few years to do so explicitly in subsequent materials. NITTF has an active partnership with the Defense Security Service's Center for the Development of Security Excellence to develop Insider Threat training materials for the executive branch and these materials also incorporate this guidance. The criticality of Insider Threat Programs incorporating these protections is grounded in Executive Order 13587 and the National Insider Threat Policy. Examples of these NITTF products include: Hub Operations Course; 2013 Guide to Accompany the National Insider Threat Policy and Minimum Standards; 2016 Protect Your Organization from the Insider Out: Government Best Practices; and the 2017 Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards. The most recent presentation given by the Director of the NITTF was at the 25 April 2018 DARPA Defense Industry Security Symposium in San Diego where he stated, "Your leadership and insider threat program personnel need to consult with legal counsel, privacy and civil liberties and whistleblower protection officers from the outset of the insider threat program. They should be an ongoing part of any insider threat program discussions."

Hearing Date: March 07, 2018
 Committee: SSCI
 Member: Chairman Burr & Vice Chairman
 Warner
 Witness: Mr. Garry Reid and
 Mr. Daniel Payne
 Question: 1

Security Clearance Reform

Question: **Limits of Automation.** What are the policy or technical limits on the use of automation to acquire and analyze records that are not yet in digital format (such as certain fingerprints) or are unavailable in state-level repositories (such as certain local criminal records)?

Answer: There are no policy limits on the use of automation to acquire and analyze records that are not yet in digital format; however, there are technical limits on the use of automation to acquire and analyze non-digital records. For example, almost all paper records (e.g., arrest records, fingerprints) may be scanned and converted to digital format; but scanned documents may not lend themselves to automated analysis and fingerprints scanned from paper may not be of sufficient quality to be used. Unfortunately, there are many jurisdictions that do not submit their records to state-level repositories or the National Law Enforcement Telecommunications System (NLETS). While the National Background Investigations Bureau (NBIB) and Department of Defense (DoD) have encouraged states and smaller jurisdictions to make their records available electronically, mandating the reporting of criminal justice information into national repositories through legislation may improve the retrieval of significant criminal records when conducting background investigations.

Hearing Date: March 07, 2018
Committee: SSCI
Member: Chairman Burr & Vice Chairman
Warner
Witness: Mr. Garry Reid and
Mr. Daniel Payne
Question: 2

Security Clearance Reform

Question: **Robustness of the Investigative Industrial Base.** Please provide an analysis of the industrial base's ability to support both the National Background Investigation Bureau and the Defense Security Service as major investigative service providers.

Answer: We assess there will be sufficient capacity of background investigators throughout the transition between DoD and NBIB. Stress on the background investigation (BI) workforce will be mitigated by expanded use of Continuous Evaluation/Automated Records Checks-based investigations that will greatly reduce the requirement for manpower-intensive fieldwork. DoD and NBIB will work closely to coordinate and synchronize actions and avoid placing excessive strains on the BI workforce.

Hearing Date: March 07, 2018
 Committee: SSCI
 Member: Chairman Burr & Vice Chairman
 Warner
 Witness: Mr. Garry Reid and
 Mr. Daniel Payne
 Question: 3

Security Clearance Reform

Question: **Interim Clearances.** Please provide the number of interim clearances, by type, that were granted to industry personnel processed through the Defense Security Service in each of the last two years.

Answer: The Defense Security Service granted a total of 146,589 interim Secret security clearances and a total of 43,255 interim Top Secret security clearances over the last 2.5 years (as of March 2018)

Interim Clearance Eligibility Granted	FY 2016	FY 2017	FY 2018 (through March)
Secret	50,975	60,378	35,236
Top Secret	12,505	19,112	11,638

Hearing Date: March 07, 2018
Committee: SSCI
Member: Senator Ron Wyden
Warner
Witness: Mr. Garry Reid and
Mr. Daniel Payne
Question: 4

Security Clearance Reform

Question: **Reducing the Number of Cleared Positions.** Please describe progress made in reducing the total number of government positions requiring a security clearance and lowering the clearance level for positions that do require clearances. In which departments, agencies and offices have there been the most progress, and where has there been the least progress? Are there target goals to reduce the number of positions requiring a clearance? If yes, what current processes are in place for achieving any of these goals?

Answer: Between FY 2013 and FY 2016, DoD reduced the number of personnel eligible for access to classified information from 4.6M to 3.5M, a decrease of more than 23%. DoD is focusing on validating the need for each cleared position, rather than on setting specific numbers-based goals. DoD will require its Components to validate the need for the level of clearance by each individual as using the Position Designation Tool (PDT) which identifies the level of risk and the security clearance or suitability determination required. The PDT is key to reducing the number of cleared personnel for new or existing positions. Consequently, the PDT is considered the starting point for the end-to-end processes of the National Background Investigation Services (NBIS), the Information Technology infrastructure for personnel vetting.

Hearing Date: March 07, 2018
Committee: SSCI
Member: Senator Wyden
Witness: Mr. Garry Reid and
Mr. Daniel Payne
Question: 5

Security Clearance Reform

Question: **Whistleblowers.** On June 18, 2014, Senator Grassley and I wrote the DNI about the potential impact of continuous monitoring and continuous evaluation on whistleblower protections. On July 25, 2014, the DNI responded that “some agencies” were training investigators and that the National Insider Threat Task Force had issued guidance emphasizing legal protections afforded whistleblowers. The DNI further wrote that “the Inspector General of the Intelligence Community, in coordination with the Intelligence Community Inspectors General Forum, is currently examining the potential for internal controls that would ensure whistleblower-related communications remain confidential, while also ensuring the necessary UAM [user activity monitoring] occurs.” Please detail any guidance, mechanisms, or procedures related to the controls the Intelligence Community and each of its component entities have implemented to ensure that any security-related personnel monitoring does not compromise the confidentiality of whistleblower-related communications.

Answer: The Intelligence Authorization Act for FY 2014 amended the National Security Act of 1947 to provide statutory protections for Intelligence Community (IC) employees who make lawful disclosures of fraud, waste, or abuse in IC programs and activities. These statutory provisions prohibit an employee from taking a personnel action in reprisal or making security clearance access determinations in reprisal against an employee who made a lawful disclosure. Further, these provisions require an inspector general to conduct fact-finding in reviewing allegations of security clearance reprisal.

Presidential Policy Directive – 19 (PPD-19), Protecting Whistleblowers with Access to Classified Information, also provides protections for IC employees against personnel actions taken in reprisal for lawfully participating in the whistleblowing process. In addition, employees and contractors are protected from reprisals in the security clearance adjudication process. PPD-19 requires that the agency Inspector General (IG) review whistleblower reprisal allegations in violation of PPD-19. Further, PPD-19 allows employees and contractors to seek an external review from the IC IG of their reprisal allegations once they have exhausted their own agency’s review process.

An IC employee, assignee, detailee, or contractor, who intends to report to Congress a complaint or information with respect to an urgent concern, may report such complaint or information to the Intelligence Community Inspector General by calling 1-855-731-3260.