THE INSIDER THREAT TO HOMELAND SECURITY: EXAMINING OUR NATION'S SECURITY CLEARANCE PROCESSES

HEARING

BEFORE THE

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

NOVEMBER 13, 2013

Serial No. 113–42

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE
87–372 PDF WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan, *Vice Chair*
PATRICK MEEHAN, Pennsylvania
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
JASON CHAFFETZ, Utah
STEVEN M. PALAZZO, Mississippi
LOU BARLETTA, Pennsylvania
CHRIS STEWART, Utah
RICHARD HUDSON, North Carolina
STEVE DAINES, Montana
SUSAN W. BROOKS, Indiana
SCOTT PERRY, Pennsylvania
MARK SANFORD, South Carolina
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
YVETTE D. CLARKE, New York
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
RON BARBER, Arizona
DONDALD M. PAYNE, JR., New Jersey
BETO O'ROURKE, Texas
TULSI GABBARD, Hawaii
FILEMON VELA, Texas
STEVEN A. HORSFORD, Nevada
ERIC SWALWELL, California

GREG HILL, *Chief of Staff*
MICHAEL GEFFROY, *Deputy Chief of Staff/Chief Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

PETER T. KING, New York, *Chairman*

PAUL C. BROUN, Georgia
PATRICK MEEHAN, Pennsylvania, *Vice Chair*
JASON CHAFFETZ, Utah
CHRIS STEWART, Utah
MICHAEL T. MCCAUL, Texas *(ex officio)*
BRIAN HIGGINS, New York
LORETTA SANCHEZ, California
WILLIAM R. KEATING, Massachusetts
BENNIE G. THOMPSON, Mississippi *(ex officio)*

KERRY ANN WATKINS, *Subcommittee Staff Director*
DENNIS TERRY, *Subcommittee Clerk*
HOPE GOINS, *Minority Staff Director*

CONTENTS

THE INSIDER THREAT TO HOMELAND SECURITY: EXAMINING OUR NATION'S SECURITY CLEARANCE PROCESSES

Wednesday, November 13, 2013

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE,
Washington, DC.

The subcommittee met, pursuant to call, at 2:29 p.m., in Room 311, Cannon House Office Building, Hon. Peter T. King [Chairman of the subcommittee] presiding.

Present: Representatives King, Higgins, and Keating.

Mr. KING. This Monday, our Nation celebrated Veteran's Day to honor the men and women who have fought, and continue to fight, for our country. In addition to these brave individuals, other Federal employees from the Department of Homeland Security, FBI, CIA, the NSA, and many other agencies work every day to protect Americans and U.S. interests from threats. These patriots deserve our gratitude for their tireless work.

The unfortunate reality is that they must also guard against internal threats. Appalling events over recent years involving trusted individuals who have damaged National security or committed tragic acts of violence have put a spotlight on the need for reforms and rigorous oversight over the security clearance process and programs to detect insider threats.

PFC Bradley Manning is serving a 35-year sentence for leaking Classified information to WikiLeaks. The next step is to prosecute Julian Assange who published the documents.

In May, media outlets reported that former CIA analyst and current NSA contractor Edward Snowden had fled to Hong Kong and released a large amount of data on Classified NSA surveillance programs.

On September 16, barely 2 months ago, Aaron Alexis, a DOD contractor, shot his way into the Washington, DC Navy Yard and killed 12 people.

All of these individuals were trusted, vetted U.S. security professionals who abused that trust and committed heinous acts. It is vital that more be done to identify potential insider threats.

While none of these examples involve DHS or DHS personnel, the Department of Homeland Security has over 120,000 employees with a security clearance. It is vital that we continually evaluate the internal processes and procedures for how those clearances are investigated, adjudicated, and reviewed.

In addition to our review of DHS security practices, today's witnesses will be asked to evaluate the quality and standards for security clearance investigations and adjudications, as well as address potential problems limiting information sharing between agencies on employees with clearances.

For example, in the Snowden case the after-action review completed by the ODNI disclosed that the 2011 background check was incomplete. According to press reports, the investigation did not verify Snowden's account of a security violation while at the CIA, review travel to India Snowden failed to disclose, and include interviews with anyone outside of his mother and girlfriend. If the investigation had been done properly it could have impacted Snowden's clearance. This also raises serious questions about what standards are used in reviewing the background investigation and adjudicating a case, and why one wasn't sent back to the investigator for a more thorough review.

There were nearly 5 million U.S. Government employees or contractors with security clearances, including over 1.4 million with a Top Secret clearance.

Now is the time to reinforce the message that a security clearance is a privilege granted so that individuals can protect the United States from threats. Not only can a clearance be revoked for cause, but violations must be prosecuted to the fullest extent of the law.

There are a number of reviews underway in the aftermath of the Manning, Snowden, and Alexis incidents. It is vital that necessary reforms are implemented expeditiously to detect and disrupt future insider threat situations.

These reforms must include an update to the Federal guidance for background investigations. in a post-9/11 world, security clearances must address evolving threats such as radical Islam and cyber crime. Had investigators looked differently into Snowden's background they might have identified disturbing trends that made him unfit to hold a clearance of any kind and a potential insider threat to U.S. National security.

I look forward to hearing more from the witnesses on these efforts, including whether or not the 5-year reinvestigation for Top Secret clearance-holders is appropriate, what additional periodic or continuous monitoring capability exists, and what more can be done to safeguard our Classified information technology systems from abuse.

I want to thank all the witnesses for being here today and for your work to detect and prevent insider threats.

[The statement of Chairman King follows:]

STATEMENT OF CHAIRMAN PETER T. KING

This Monday our Nation celebrated Veteran's Day to honor the men and women who have fought, and continue to fight, for our country. In addition to these brave individuals, other Federal employees from the Department of Homeland Security, FBI, CIA, the NSA, and many other agencies work every day to protect Americans and U.S. interests from threats. These patriots deserve our gratitude for their tireless work.

The unfortunate reality is that they must also guard against internal threats. Appalling events over recent years involving trusted individuals who have damaged National security or committed tragic acts of violence have put a spotlight on the

need for reforms and rigorous oversight over the security clearance process and programs to detect insider threats.

- PFC Bradley Manning is serving a 35-year sentence for leaking Classified information to WikiLeaks. The next step is to prosecute Julian Assange who published the documents.
- In May, media outlets reported that former CIA analyst and current NSA contractor Edward Snowden had fled to Hong Kong and released a large amount of data on Classified NSA surveillance programs.
- On September 16, just shy of 2 months ago, Aaron Alexis—a DOD contractor shot his way into the Washington, DC Navy Yard and killed 12 people.

All of these individuals were vetted, trusted U.S. security professionals who abused that trust and committed heinous acts. It is vital that more is done to identify potential insider threats.

While none of those examples involved DHS or DHS personnel, the Department of Homeland Security has over 120,000 employees with a security clearance. It is vital that we continually evaluate the internal processes and procedures for how those clearances are investigated, adjudicated, and reviewed.

In addition to our review of DHS security practices, today's witnesses will be asked to evaluate the quality and standards for security clearance investigations and adjudications, as well as address potential problems limiting information sharing between agencies on employees with clearances. For example, in the Snowden case the after-action review completed by the Office of the Director of National Intelligence (ODNI) disclosed that the 2011 background check was incomplete. According to the *Wall Street Journal,* the investigation did not verify Snowden's account of a security violation while at the CIA, review travel to India Snowden failed to disclose, and include interviews with anyone outside of his mother and girlfriend. If the investigation had been done properly it could have impacted Snowden's clearance. This also raises serious questions about what standards are used in reviewing the background investigation and adjudicating a case, and why this one wasn't sent back to the investigator for a more thorough review.

There are nearly 5 million U.S. Government employees or contractors with security clearances, including over 1.4 million with a Top Secret.

Now is the time to reinforce the message that a security clearance is a privilege granted so that individuals can protect the United States from threats. Not only can a clearance be revoked for cause, but violations must be prosecuted to the fullest extent of the law.

There are a number of reviews underway in the aftermath of the Manning, Snowden, and Alexis incidents. It is vital that necessary reforms are implemented expeditiously to detect and disrupt future insider threat situations.

These reforms must include an update to the Federal guidance for background investigations. In a post-9/11 world, security clearances must address evolving threats such as radical Islam and cyber crime. Had investigators looked differently into Edward Snowden's background they might have identified disturbing trends that made him unfit to hold a clearance of any kind and a potential insider threat to U.S. National security.

I look forward to hearing more from the witnesses on these efforts, including whether or not the 5-year reinvestigation for Top Secret clearance holders is appropriate, what additional periodic or continuous monitoring capability exists, and what more can be done to safeguard our classified information technology (IT) systems from abuse.

Mr. KING. I now recognize the Ranking Member, Mr. Higgins, for his opening statement, and thank him and his staff for their cooperation in preparing for this subcommittee hearing.

Mr. HIGGINS. Thank you, Mr. Chairman.

I would like to thank Chairman King for holding today's hearing. I would also like to thank the witnesses for their testimony and for their public service.

This summer the public became very concerned about the surveillance tactics the National Security Agency currently takes in the interest of security. Former National Security Agency contractor Edward Snowden revealed details about the National Security Agency surveillance program that collects phone calls and monitors records of millions of Americans.

This prompted Americans to become very interested in whether the right to privacy trumps the need for National security. Finding this balance is difficult, and according to the director of the National Security Agency, General Keith Alexander, these Classified programs have been successful. According to Alexander, people like Snowden, who reveal sensitive information about this country, can cause a grave damage to the Nation.

The widespread questions remain, however: How could Snowden have this type of access to National security secrets? Was there anything in his background that showed a lack of integrity? What does it take to get a security clearance?

As Congress and the Executive branch were searching for answers, a few blocks from the U.S. Capitol Aaron Alexis, a lone gunman, took up arms against fellow employees at the Navy Yard. Alexis, a contractor, not only had a security clearance, but also had a history of arrests and gun infractions.

As we have pervasive incidents such as these, it is imperative that we look at the security clearance process. According to the Office of Personnel Management, 4.9 million Federal workers and contractors are eligible to hold security clearance. At Department of Homeland Security, approximately 124,000 employees hold clearances.

These vast numbers grow year by year. It lends to the conversation of how these clearances are determined and given.

In its report to the Ranking Member of the full committee, the Government Accountability Office found that the Office of Director of National Intelligence has not provided agencies with a clearly-defined guidance and procedures to determine if a position requires a security clearance. The GAO also noted that since the 1990s, quality in the security clearance investigations has not been a priority. These are just two detrimental flaws in the security clearance process.

I am pleased to hear that the Office of Management and Budget is heading a 120-day review of the Federal clearance process. However, it seems a little bit too little, too late. The intelligence community has grown greatly since September 11 and there are examples of their outstanding work.

In August the efforts of the intelligence community, along with Royal Canadian Mounted Police, disrupted a terrorist plot in Western New York. Unfortunately, the lack of consistency and quality in the security clearance process can place the international community in great danger from an insider threat.

We expect quality performance from our Federal employees. Holding a security clearance should be a privilege. It is my hope that this hearing can yield solutions that can be included in the restoration of the security clearance process.

I look forward to the witnesses' testimony.

With that I yield back.

[The statement of Ranking Member Higgins follows:]

STATEMENT OF RANKING MEMBER BRIAN HIGGINS

NOVEMBER 13, 2013

This summer, the public became very concerned about surveillance tactics that the National Security Agency currently takes in the interest of security. Former Na-

tional Security Agency contractor, Edward Snowden, revealed details about National Security Agency surveillance programs that collect phone calls and monitor records of millions of Americans.

This prompted Americans to become very interested in whether the right to privacy trumps the needs of the country. Finding this balance is difficult and according to the director of the National Security Agency, General Keith Alexander, these Classified programs have been successful. According to Alexander, people like Snowden who reveal sensitive information about this country can cause grave damage to the Nation.

The widespread questions remain, however: How could Snowden have this type of access to National security secrets? Was there anything in his background that showed a lack of integrity? What does it take to get a security clearance?

As Congress and the Executive branch were searching for answers, a few blocks from the U.S. Capitol, Aaron Alexis, a lone gunman took up arms against fellow employees at the Navy Yard. Alexis, a contractor, not only had a security clearance, but also had a history of arrests and gun infractions. As we have pervasive incidents such as these, it is imperative that we look at the security clearance process.

According to the Office of Personnel Management 4.9 million Federal workers and contractors are eligible to hold a security clearance. At the Department of Homeland Security, approximately 124,000 employees hold clearances.

These vast numbers grow year by year. It lends to the conversation of how these clearances are determined and given. In its report to the Ranking Member of the Full committee, the Government Accountability Office found that the Office of the Director of National Intelligence has not provided agencies with clearly-defined guidance and procedures to determine if a position requires a security clearance.

GAO has also noted that since the 1990s quality in the security clearance investigations has not been a priority. These are just two detrimental flaws in the security clearance process. I am pleased to hear that the Office of Management and Budget is heading a 120-day review of the Federal clearance process. However, it seems as if this is a "better late than never" opportunity.

The intelligence community has grown greatly since September 11 and there are examples of their outstanding work. In August, the efforts of the intelligence community, along with the Royal Canadian Mounted Police, disrupted a terrorist plot in Western New York.

Unfortunately, the lack of consistency and quality in the security clearance process can place the IC in grave danger from an insider threat. We expect quality performance from our Federal employees. Holding a security clearance should be a privilege. It is my hope that this hearing can yield solutions that can be included in the restoration of the security clearance process.

Mr. KING. I thank the Ranking Member, Mr. Higgins, for his statement.

Other Members of the committee, whether here or not, are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

NOVEMBER 13, 2013

My years in leadership on this committee have given me great insight into the American public's evolving interest in homeland security. Matters such as aviation security and emergency preparedness usually remain at the forefront of the minds of vast majority of Americans, while employment matters may usually strike those who are affected. After September 11, the public wanted to know what could be done to make sure that another devastating attack did not take place.

The public also wanted to know how they could help this country through either military or civilian service. As the Government began to develop solutions, the Department of Homeland Security was established to secure the Nation from the many threats it faces. Other Executive Orders increased the Government's ability to track Americans who engaged with people overseas.

A sweeping change came to the Federal workforce. The 9/11 Commissioners recommended that the United States improve its intelligence-gathering and information-sharing activities. More and more civilians began to be employed in positions that allowed access to Classified information that required them to have security clearances.

Ten years after September 11, the sheer volume of Americans holding security clearances was astonishing. According to the Government Accountability Office, in 2011, the Office of the Director of National Intelligence, the Nation's executive security agent, reported that over 4.9 million Federal contractors and Government workers held or were eligible to hold a security clearance. Many people contact Congress and inquire about the clearance process. For some, successful completion of the clearance process is a badge of honor. For others, due to various circumstances, obtaining a clearance was a hurdle to employment. Some questioned why clearances were necessary to perform certain duties that may not involve access to Classified material.

Some long-time Federal employees were concerned that they might be required to redo the process when they switch employment at different agencies within the Federal Government. The volume of security clearances gave me pause. Last summer, I asked the Government Accountability Office to conduct an investigation into security clearances. GAO found that throughout the Federal Government that there are essentially no agreed-upon standards for requiring security clearances for Federal jobs. The lack of clear criteria and commonly-accepted standards may contribute to the exponential growth in Federal jobs requiring a security clearance. GAO also found that security clearance requirements for Federal jobs that do not involve handling National security information may hinder transparency and openness in Government. The security clearance issue was at the forefront of my mind and the minds of employment-seekers the past few years; however, May 2013 changed the game.

An overwhelming number of Americans became concerned when former NSA contractor Edward Snowden leaked the details of classified programs to the British newspaper *The Guardian*. Snowden's security clearance was vetted by an outside contractor and, in hindsight, many still wonder if Snowden should have had access to such sensitive information. There are several reports that Snowden may have omitted or embellished information on his personnel background form.

The same firm that vetted outside contractor Edward Snowden vetted Navy Yard shooter Aaron Alexis. On September 16, Alexis, a civilian contractor, opened fire at Navy Yard here in Washington, DC. After the Navy Yard shooting, it was discovered that Alexis failed to disclose information about felony charges, and a Federal personnel report had no information about a his previous arrests.

It is difficult to believe that the Executive branch spends over $1 billion dollars on background investigations for suitability and security clearances, but could not yield Alexis's felony gun charges. Despite GAO's insistence, it took leaks and a horrific lone gunman to get an Executive branch review. I look forward to the panel's review and remind them that access to National security information is a privilege that should be regarded with the highest integrity.

There needs to be uniformity with how security clearances are given and in how they are revoked. If revocation or suspension is the rule for leaking information, it needs to be applied across the board.

Mr. KING. Right now we are pleased to have a very distinguished panel of witnesses before us today on this vital topic.

Mr. Merton Miller serves as the associate director of investigations for the Office of Personnel Management Federal Investigative Services. OPM's Federal Investigative Services is the Federal Government's largest provider of background investigations and services, supporting more than 100 Federal agencies' personnel security programs. He is responsible for FIS operations, policy development, and contract oversight of OPM's investigations program, which completes over 2 million investigations annually.

Before joining OPM FIS, Mr. Miller served in the United States Air Force, reaching the rank of full colonel before his retirement in 2005. During his career, Colonel Miller served with the Air Force Office of Special Investigations, specializing in criminal counterintelligence, counterterrorism, and security investigations and operations. Upon his retirement from the military Colonel Miller joined the Department of Defense's counterintelligence field activity, directing DOD's counterintelligence programs.

Mr. Gregory Marshall is the chief security officer for the Department of Homeland Security. In this capacity Mr. Marshall is responsible for security-related issues affecting the Department's personnel security, physical security, special security, special access programs, and security training and awareness.

Mr. Marshall began his Federal career as a police officer with the United States Capitol Police in 1984 and later transferred to the Howard County, Maryland Police Department, where he retired in 2007. He returned to Federal service when he joined DHS as the deputy chief of physical security and was later promoted to deputy chief security officer.

Mr. Brian Prioletti is the assistant director for the Special Security Directorate and the National counterintelligence executive in the Office of the Director of National Intelligence. Mr. Prioletti is responsible for the policies and procedures governing the conduct of investigations as well as assisting the DNI on determining which agencies conduct background investigations and determine eligibility for access to Classified information. Prior to joining the ODNI, Mr. Prioletti worked at the Central Intelligence Agency from 1981 until 2013.

Ms. Brenda Farrell is a director in the Government Accountability Office's Defense Capabilities and Management, a position she has held since 2007. Her work focuses on military and civilian personnel issues, including personnel security clearance process concerns.

Ms. Farrell began her career with GAO in 1981 and has served in a number of issue areas associated with National security. Prior to her appointment as director, she served as an acting director for GAO's strategic issues team, where she was responsible for overseeing three major bodies of work related to strategic human capital management, Government regulation, and decennial census issues.

I want to thank all of the witnesses for being here today.

We will begin with Mr. Miller, who is recognized for 5 minutes. Thank you.

STATEMENT OF MERTON W. MILLER, ASSOCIATE DIRECTOR OF INVESTIGATIONS, FEDERAL INVESTIGATIVE SERVICES, U.S. OFFICE OF PERSONNEL MANAGEMENT

Mr. MILLER. Thank you, Chairman King, Ranking Member Higgins. I want to thank you for letting me testify here today. I share your commitment and that of my colleagues here to examine the processes and procedures for determining who shall be allowed access to our Nation's secrets, granted the privilege of serving in a position of public trust, and given routine physical and logical access to our Federal facilities.

Presently, there is a series of steps that must be taken to determine whether an individual should be granted a security clearance. The process begins when a Federal agency determines whether the duties of a particular Federal civilian position, military position, or contract position requires access to Classified information to perform their duties.

Once an agency determines that an individual will perform work requiring access to Classified information and also has determined

the level of access—either Confidential, Secret, or Top Secret—the agency submits a request to OPM to perform a background investigation. The background investigation we conduct must conform to Government-wide rules that meet investigative standards, adjudicative guidelines, and reciprocity mandates.

The Federal Investigative Standards outline the required elements of the investigation. These elements include the completion of a questionnaire by the applicant and specify investigative leads to be performed by OPM depending on the level of clearance sought.

The completion of a background investigation is dependent in part on the voluntary cooperation of sources and of record providers. In some instances, essential personnel are not available for an interview; members of the public, such as former employers or educational institutions are unwilling to provide interviews to investigators or to complete forms or make records available. For OPM investigators who have performed work on the investigative process, they are required to perform and complete a detailed summary of the work they accomplished.

Once the investigator completes his or her work and the results are reviewed for completeness and delivered to the customer agency, OPM's role in the process is complete. Following investigative phase of the process, the agency which requested the investigation moves into the adjudicative phase. It is during this adjudicative phase when a determination is made on whether an individual is eligible for access to Classified information.

The decision that an individual shall receive access to Classified information is the responsibility of the head of the agency employing the individual or his or her designee. The agency for which the work is to be performed makes the decision to grant eligibility based in part upon the background investigation and in part upon other information that may be available to the agency, such as the results of a polygraph examination if that is required for the position.

Although there are considerable processes and procedures in place today to vet individuals for a security clearance, the recent tragic events of the Navy Yard and the high-profile security breaches highlights the need to be ever-vigilant in assuring that individuals entrusted with access to Classified information and individuals with physical and logical access to Federal facilities do not present a risk of harm to National security or to the safety of our employees.

At the President's direction and under the leadership of OMB, OPM is presently working with its colleagues to identify potential improvements in suitability fitness, clearance determination procedures, and anything that might help enhance employee safety and National security.

I want to thank you again for the opportunity to testify regarding this important issue. I look forward to answering any questions you might have.

[The prepared statement of Mr. Miller follows:]

PREPARED STATEMENT OF MERTON W. MILLER

NOVEMBER 13, 2013

Chairman King, Ranking Member Higgins, and Members of the subcommittee, thank you for asking me to be here today.

To that end, this subcommittee has asked the Office of Personnel Management (OPM) questions about security clearances. I appreciate the opportunity to give you a better understanding of OPM's role in the security clearance process.

1. THE SECURITY CLEARANCE PROGRAM

There is a series of steps that must be taken to determine whether an individual should be granted a security clearance. The process begins when a Federal agency determines whether the duties of a particular Federal civilian position or position in the military will require the incumbent to have access to Classified information, or that an employee of a contractor will require access to Classified information in order to perform work under a Government contract. If such a determination is made, and if there is no prior eligibility determination that is sufficient, under applicable directives, to meet that need, the agency will need to determine such eligibility itself.

OPM conducts 95 percent of the Government background investigations. Once an agency determines that the subject will perform work that requires a demonstrated, foreseeable need for access to Classified information, and that an investigation is required, the agency submits a request to OPM that it perform the background investigation. OPM performs the investigation on a reimbursable basis in accordance with established investigative standards and then delivers the report of investigation to the requesting agency.

I want to emphasize that OPM is not charged with deciding whether an individual should or will be found eligible for access to Classified information or even with making any recommendation with respect to that decision. The decision that an individual should receive access to Classified information is ultimately, pursuant to Executive Order 12968, the exclusive responsibility of the head of the agency employing the individual, or his or her designee, following a National security adjudication (either by that agency or by a central adjudicative facility working on its behalf). The agency for which the work is to be performed makes the decision to grant eligibility, based, in part, upon the background investigation, and, in part upon other information that may be available to the agency, such as a polygraph if required for the position. Further, the agency can reopen the investigation or order additional investigative work from OPM if it does not have enough information to make a determination.

The security clearance process must conform with Government-wide rules that include investigative standards (which may vary, based on the level of Classified information to which the individual will have access), adjudicative guidelines, and reciprocity mandates. The standards outline the required elements of the investigation. These elements include the completion of a questionnaire by the applicant and specified record and other checks to be performed by OPM depending on the level of clearance sought.

Background investigations are dependent on the voluntary cooperation of sources and of records providers, as well as the availability and accessibility of references and records. In some instances, essential personnel are not available for an interview (for example, when members of the Armed Forces are deployed in dangerous locations overseas); members of the public are unwilling to provide interviews to investigators or to complete inquiry forms; or records are not made available (for example, Federal, State, and local records may not be accessible to our investigators for a variety of reasons).

Each OPM investigator who has performed work on the investigation prepares a report of investigation that details all work attempted and all work completed. These reports of investigation are combined with the results of records checks that OPM conducts of record repositories specified in the investigative standards. Further, OPM uses "issue codes" to alert the sponsoring agency of areas of potential adjudicative concern. Once the investigator completes his or her work, OPM reviews the results package for completeness (and, when efforts to complete items were unsuccessful, reporting those efforts) and delivers it to the customer agency. The delivery is generally accomplished by electronic means to support electronic adjudication processes in place at Federal agencies. Once OPM has completed its work and transmitted the final investigation file to the customer agency, OPM's role in the investigation concludes.

2. STAFFING AND OVERSIGHT OF INVESTIGATIONS

Adapting to change within the background investigation program is not new to the investigative community. For example, during the Clinton administration, the decision was made to move large amounts of the background investigations work performed by OPM to a contractor workforce. The decision was made that OPM should absorb a background investigations function performed by the Department of Defense (DoD) (with a Federal workforce) into the OPM workforce, leaving OPM with a blended workforce of investigators. Today, OPM continues to use a combination of Federal employees and contractors to complete background investigations. The background investigation workforce has dealt with factors that have driven down the need for background investigations—for example, declines in the size of the Federal workforce that have limited hiring, and thus the need for new background investigations to factors that have dramatically driven up the need for background investigations—for example, background investigation security needs following September 11, 2001. OPM and its partners in the background investigation community are aware of shifting demands for the investigation workforce, and working with a blend of contractors and Federal employees allows OPM to adjust its needs according to the demands of its customers.

OPM's contract investigators must conduct investigations to the same Federal investigative standards as their Federal counterparts. The training curriculum is the same for both. OPM employs a professional Federal cadre of certified instructors and instructional system specialists to develop and provide an accredited Background Investigator Training program, recognized by the Executive branch as the National training standard. All of OPM's trainers and a number of the other agencies' trainers for the contract investigators attend courses at OPM's Federal Investigative Services' National Training Center and then administer the same courses to the employees of the contractors. OPM conducts oversight to ensure all the terms of the contract are being met, including review of contract quality control plans, audits, and inspections, including "check rides" to observe investigators during the investigation process. OPM is vigilant about the potential for fraud and falsification both by Government employees and by employees of contractors. OPM has taken affirmative steps to detect and root out abuses. When instances of fraud or falsification are found, OPM takes all appropriate steps to address them. We also work closely with our Inspector General and the Department of Justice to cooperate with any subsequent investigations. We have taken steps in recent years to prevent and detect fraud and falsification both through improved workforce training and through additional levels of reviews to ensure the integrity of background security clearance investigations.

The agencies for which work is being performed control who has access to their buildings and systems, not OPM, and if an agency has concerns relating to a particular employee of a contractor, there are avenues available for that agency to take action. The agency may revoke the individual's credential and, if appropriate, direct the contractor to remove that individual from work on the contract. The agency also may request that OPM conduct a reimbursable investigation. And, of course, there are avenues for agencies to alert oversight or other law enforcement entities if there are potential criminal conduct concerns.

3. STEPS GOING FORWARD

During the last 5 years, the Office of Management and Budget (OMB), OPM, DoD, and the Office of the Director of National Intelligence (ODNI) have worked together on a reform effort to ensure that there is an efficient, aligned system for assessing suitability or fitness for Federal employment, eligibility for logical and physical access to Federal systems and facilities, eligibility for access to Classified information, or fitness to perform work under a Federal contract (where required by the contract) through background investigations and appropriate adjudications. At the direction of Executive Order 13467, the Performance Accountability Council (PAC), including OPM, OMB, and ODNI, was established to ensure that the work of security clearance reform be accomplished in this context and throughout the Executive branch.

Our work together with the PAC has done much to improve reciprocity so that agencies can place individuals who have already been vetted into new positions without delay and without further expense. In the last 3 years, we have enhanced OPM's Central Verification System, established as directed by the Intelligence Reform and Terrorism Prevention Act to support reciprocity, by expanding the reporting of credentialing, suitability, and security determinations from agencies, adding new data fields, and enabling enterprise access for intelligence community users to search relevant details. We have enhanced and professionalized the training of investigators and adjudicators to ensure consistency across the Executive branch and

promote confidence when reciprocity is applied. And our work to create an aligned system for investigations will enable greater reciprocity opportunities as we now begin to implement revised investigative standards.

Pursuant to Executive Order 13467, the Director of National Intelligence, as the Security Executive Agent, provides guidance and oversight of the process that Government agencies use to make determinations of eligibility for access to Classified information and may amend the current adjudicative criteria (established by the President) if the need arises. In addition, the Security Executive Agent is responsible for establishing the criteria governing the conduct of background investigations related to determinations of eligibility for access to Classified information.

OPM, DoD, and ODNI co-chair the interagency working group chartered with establishing the first Federal standards for assessing the quality of National security and suitability background investigations Government-wide. The proposed standards are currently under Department and agency review with a pilot exercise to be initiated in this year to validate ease and consistency in application of the standards.

At the President's direction, under the leadership of the Director of OMB, OPM is working with its colleagues on the PAC to review the oversight, nature, and implementation of National security, credentialing, and fitness standards for individuals working at Federal facilities. Our review is focused on steps that can be taken to strengthen these processes and implementation of solutions identified during the course of recent reform efforts. In particular, we recognize that evolution of the security clearance process must include the ability to obtain and easily share relevant information on a more frequent or real-time basis.

4. CONCLUSION

Thank you for this opportunity to testify, and I would be happy to answer any questions you may have.

Mr. KING. Thank you, Mr. Miller.

Mr. Marshall, you are recognized. Thank you.

STATEMENT OF GREGORY MARSHALL, CHIEF SECURITY OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. MARSHALL. Thank you, Chairman King, Ranking Member Higgins. Good afternoon.

Thank you for the opportunity to provide testimony on personnel security vetting for Federal employees and contract personnel for the U.S. Department of Homeland Security. I am Greg Marshall, chief security officer of Homeland Security. I lead the dedicated men and women who make up the Office of the Chief Security Officer.

I am a career official with nearly 30 years of law enforcement experience.

The mission of my office is to safeguard the Department's people, property, and information. Accordingly, I am responsible for security-related issues affecting more than 235,000 DHS employees that comprise the Department.

The security oversight and guidance authority of my office applies across the Department. However, DHS operational components play a significant role in managing their workforce, including personnel vetting.

The diverse missions and responsibilities of the Department and the personnel used to meet these missions underscore the challenges involved with the personnel security discipline. The tragic events of Monday, September 16 at the Navy Yard have placed the issues of physical security, access control, and personnel vetting front and center in the minds of security professionals across the Federal landscape.

I need to make clear, however, that security aims to manage risk, not eliminate it. Our job is to do everything we can to keep our employees safe, and in doing so we have the benefit of policies and procedures, processes and technologies, both proven and emerging, to guide and improve our key security programs.

When we consider the security for a Federal facility, including access control, we follow the Interagency Security Committee standards. Facilities are assessed for risk and appropriate countermeasures are employed. The outcome of these risk assessments drive the level of protection to include an appropriate access control posture. A one-size security solution does not and cannot fit all.

For employees to qualify for access to facilities they must undergo a background investigation to establish suitability for employment. These investigations are, for the most part, conducted by OPM. Contractors are screened in a similar process to determine fitness to work on a DHS contract and have facility access.

Background investigations for suitability and fitness examine character and conduct, and based upon all available information, we make an adjudicative decision concerning a person's suitability or fitness for employment or access to Classified information.

It is important to note that any background investigation, no matter how rigorous, is no guarantee that all relevant information is known, available, or has been included. Also, a background investigation may not reliably predict future behavior. A background investigation is an exercise in risk management establishing some basic facts, but cannot guarantee any individual's continuing fitness to carry out their duties or to behave in a lawful or safe manner.

Recent improvements in our ability to manage these inherent risks include Homeland Security Presidential Directive 12, which mandated a Government-wide standard for secure and reliable credential to be used when accessing Federal facilities. This credential, known as a PIV card, represents a marked improvement over legacy identity cards.

The background investigation process itself is undergoing major Government-wide reform with phased implementation to begin this fiscal year. The concept of continuous evaluation has been developed to supplement normal reinvestigation reviews with a process that examines conduct between normal reinvestigation time frames. Relevant security information, like a recent arrest, would become available in near-real time, helping to ensure that Classified information and/or Federal facilities are appropriately safeguarded.

Finally, this administration's recent information-sharing and safeguarding initiative, also known as Insider Threat, seeks to complement background investigations and continuous evaluation with continuous monitoring. This program will incorporate and analyze data in near-real time from a much broader set of sources. Its focus is the protection of Classified information but its applicability to suitability and contractor fitness is evident.

To conclude, suitability and clearance determinations and access control to Federal facilities remains a work in progress but are evolving towards dramatic improvement. We have made progress

but managing employee and facility risks will continue to be a challenge.

Thank you again for the opportunity to testify today and I look forward to your questions.

[The prepared statement of Mr. Marshall follows:]

PREPARED STATEMENT OF GREGORY MARSHALL

NOVEMBER 13, 2013

Chairman King, Ranking Member Higgins, Members of the committee, good morning and thank you for the opportunity to provide testimony on personnel security.

I am Greg Marshall, chief security officer of the U.S. Department of Homeland Security (DHS). I lead the dedicated men and women who make up the Office of the Chief Security Officer. My office is an element of the Department's Management Directorate, and I report to the under secretary for management.

The mission of our office is to safeguard the Department's people, property, information, and systems. Accordingly, the DHS chief security officer is responsible for security-related issues affecting the more than 235,000 DHS employees that compose the Department. I exercise DHS-wide security program authorities in the areas of personnel security, physical security, administrative security, special security, identity management, special access programs, and security training and awareness. I also support the chief information officer in the area of IT security policy and the under secretary for intelligence and analysis in the protection of intelligence sources and methods, and accreditations of Classified facilities.

The security oversight and guidance authority of my office applies across the Department. However, Operational components play a significant role in managing the facilities which they inhabit, including access to those facilities. The diverse missions and responsibilities of the Department underscore the challenges involved within the physical security and access control disciplines.

The tragic events of Monday, September 16 at the Washington Navy Yard have placed the issue of physical security, access control, and personnel vetting front and center in the minds of security professionals across the Federal landscape.

Shortly after the Navy yard incident, I convened a meeting of the Department's Chief Security Officer Council. Each component chief security officer (CSO) acknowledged the significance of the Navy Yard tragedy to access control and the underlying vetting processes and each CSO commented on the complexities of vetting and access, including the costs involved. With this in mind, the Department remains committed to ensuring that only those persons with a legitimate need to access any given facility are allowed to enter, that those persons possess no prohibited items, and that the backgrounds of those persons who do enter have been vetted to an appropriate level of rigor.

I would make clear, however, that security involves risk management. Our job is to do everything we can to reduce the risk and keep our employees safe. In pursuit of our mission, please be assured that DHS security leadership and the professionals we manage have the benefit of extensive knowledge, training, and experience. We also have the benefit of comprehensive policies, procedures, processes, and emerging technologies to help guide and improve our key security programs.

For example, when we consider the security posture for a Federal facility, including access control, we at DHS follow Interagency Security Committee standards. During this process, facilities are assessed for risk, and appropriate countermeasures are employed to mitigate the risks. Using a decision matrix involving mission criticality, the sensitivity of the activities conducted, threats to the facility, facility population of persons who work and visit there, and other factors, an appropriate Federal Security Level is assigned to each facility. Accordingly, the outcomes of these risk assessments drive the level of protection for each facility, to include an appropriate access control posture. Simply put, a one-size security solution does not and cannot fit all facilities.

For our employees to qualify for access to a Federal DHS facility, an employee must undergo a background investigation to establish his or her suitability for employment. These investigations are, for the most part, conducted by OPM on behalf of DHS. Contractors are screened in a process similar to employees in order to determine their fitness to work on a DHS contract and have unescorted access to DHS facilities. Background investigations for suitability and fitness examine character and conduct behaviors, such as criminal history, alcohol and drug use, and employment history, among others. Based upon all available information, a personnel secu-

rity specialist makes an adjudicative decision concerning a person's suitability or fitness for employment, including access to facilities.

It is important to understand that a background investigation for suitability and one for a security clearance processes with multiple levels of investigation dependent upon the access required and level of risk. A security clearance allows access to Classified information, while a favorable suitability or fitness determination allows employment and access to facilities. On its own, a background investigation for suitability does not permit access to Classified information.

It is also important to note that a background investigation for either a suitability determination or a security clearance, no matter how rigorous, is no guarantee that every bit of relevant information about the individual is available or has been included. For example, prior criminal convictions and/or arrest information may not be reported in State and/or Federal repositories, often simply due to data entry resource constraints. It is these types of checks that are basic elements of any Federal employment background investigation.

Also, it is important to note that a background investigation may not be an indicator of future behavior. Even those who have successfully undergone the most rigorous set of background checks available—even a comprehensive polygraph examination—may someday prove untrustworthy. Ultimately, a Federal background investigation only examines past behavior and is sometimes based on limited available information.

A Federal background investigation is an exercise in risk management, establishing some basic facts such as identity, citizenship, criminal history, etc. However, a background investigation cannot be characterized, in and of itself, does not guarantee any single individual's continuing day-to-day fitness to carry out his or her employment responsibilities or to behave in a lawful and safe manner.

With these limitations in mind, there have been several recent improvements to the ability of the Government to manage these inherent risks.

First, Homeland Security Presidential Directive 12 (HSPD–12) mandated the development and implementation of a Government-wide standard for a secure and reliable Personal Identity Verification (PIV) card for gaining access to Federally-controlled facilities. To date, DHS Headquarters and components have issued over 250,000 PIV cards to Federal employees and contractors. For the first time, this process has effectively linked the completion of a person's background investigation with the issuance to that person of a unique Federal identity credential. The PIV card represents a marked improvement over the various legacy access/identity cards, but is only a part of any solution. As a result, Federal facility access control processes use this PIV card and its various authentication mechanisms to verify the identity of the holder, link the holder to the card, and link the card itself to a database of valid employees and contractors having legitimate business at any given facility.

Second, the background investigation process itself is undergoing a major Government-wide reform effort, to include revised Federal investigative standards signed jointly by the Director of National Intelligence and the Director of the Office of Personnel Management in 2012, and phased implementation to begin this fiscal year. With the Federal investigative standards, the concept of "continuous evaluation" is being developed to supplement the normal re-investigation reviews of employees which, under the revised standards, will be in 5-year increments, with a Government-led process that examines a person's conduct within his or her normal re-investigation time frames. As such, relevant security information like a recent arrest or conviction for a crime outside of the Federal system, for example, would become available on a timelier basis to security officials responsible for assessing a person's eligibility for access to Classified information, thereby helping to ensure that Classified information and/or Federal facilities are appropriately safeguarded. "Continuous evaluation" represents a significant process improvement over current capabilities and will mitigate some of the limitations in the existing background investigation process discussed above.

Finally, this administration's recent Information Sharing and Safeguarding initiative, also known as "Insider Threat," seeks to complement background investigations and continuous evaluation with continuous monitoring. Continuous monitoring will incorporate data in near-real time from a much broader set of data sources, as compared to information that was previously available in the background investigation process. The initiative focuses on monitoring certain IT systems and incorporates analysis and collation software to aid in the identification of behavioral trends that could be indicative of an insider threat problem. Strict referral protocols are in place to investigate abnormalities. The aim is the detection and mitigation of threats to Classified information before any damage can be done. The focus of

this program is the protection of Classified information, but its applicability to other behavioral issues, including suitability and contractor fitness, is evident.

In conclusion, the suitability determinations of and access control to Federal facilities by Federal employees and contractors remains a work in progress, but is evolving toward dramatic improvement. It is our responsibility as DHS security leaders, with the support of Congress, to ensure a safe and secure workplace. We have made important strides, but assessing and managing employee and facility risks will continue to be a challenge in the future. We will continue to work every day to meet these challenges. Thank you again for the opportunity to testify today.

Mr. KING. Thank you, Mr. Marshall.

Mr. Prioletti please, 5 minutes. Again, if you go over 5 minutes don't worry about it. Just a general guideline.

STATEMENT OF BRIAN A. PRIOLETTI, ASSISTANT DIRECTOR, SPECIAL SECURITY DIRECTORATE, NATIONAL COUNTERINTELLIGENCE EXECUTIVE, OFFICE OF DIRECTOR OF NATIONAL INTELLIGENCE

Mr. PRIOLETTI. Chairman King, Ranking Member Higgins, and distinguished Members of the subcommittee, thank you for the invitation to provide information on the Government's practices and procedures regarding security clearances and background investigations. My statement will address the role of the DNI—Director of National Intelligence, as a security executive agent, his authorities and responsibilities for oversight of the security clearance process across the Government, areas in need of attention in the current process, and initiatives underway to address those areas.

Pursuant to Executive Order 13467, the DNI, as the security executive agent, is responsible for the development and oversight of effective, efficient, uniform policies and procedures governing the timely conduct of investigations and adjudications for eligibility to access Classified information or eligibility to hold a sensitive position. The security executive agent also serves as the final authority to designate agencies to conduct background investigations and determine eligibility for access to Classified information, and ensures reciprocal recognition of investigations and adjudication determinations among agencies.

A background check is an essential component of the security clearance process. It is required prior to making a determination for eligibility for access to Classified or eligibility to occupy a sensitive position. The 1997 Federal Investigative Standards, as amended in 2004, are the current standards used to conduct background investigations. The scope of the background investigation is dependent upon the level of security clearance required.

For example, a Secret clearance includes National agency, local agency, and credit checks. An interview with an individual being considered for the clearance is conducted if necessary to resolve issues resulting from the required checks.

A Top Secret clearance requires the above checks as well as interviews of the individual being considered for the clearance, his or her references, coworkers, supervisors, neighbors, and other individuals.

Regardless of the type of clearance involved, identified issues must be fully investigated and resolved prior to any adjudication.

The adjudicative guidelines issued by the White House in 2005 currently serve as the Government-wide guide for most eligibility

decisions. The DNI has issued separate adjudicative guidelines for sensitive compartmented information, known as SCI, and Special Access Program access. Adjudicative decisions are made by utilizing the whole-person concept, which is a careful weighing of available, reliable information about the person, past and present, favorable and unfavorable.

Recent events involving individuals with clearances have further emphasized the importance of a robust security clearance program and areas in need of attention in the current security clearance process. Under the direction of the Performance Accountability Council, known as the PAC, the ODNI, in collaboration with OMB, OPM, DOD, and other Federal partners, have been leading security clearance reform efforts for several years. Although these efforts are still a work in progress, when mature they will mitigate adjudicative gaps and enhance the Nation's security posture.

One critical element for a robust security clearance process is to establish an effective capability to assess an individual's continuing eligibility on a more frequent basis. Under current policies and practices, an individual's continued eligibility for access to Classified information relies heavily on a periodic reinvestigation—essentially a background investigation and adjudication conducted every 5 years for a Top Secret clearance or every 10 years for Secret clearances.

The time interval between periodic reinvestigations leaves the U.S. Government potentially uninformed as to the behavior that could pose a security or counterintelligence risk. Continuous evaluation, known as C.E., is a tool that will assist in closing this information gap. Per Executive Order 13467 and the revised Federal Investigation Standards, which were signed in 2012, C.E. allows for a review at any time of an individual with eligibility or access to Classified information or in a sensitive position to ensure that that individual continues to meet the requirements for eligibility.

C.E., as envisioned in the reformed security clearance process, includes automated record checks of commercial databases, Government databases, and other information lawfully available. Manual checks are inefficient and resource-intensive. The C.E. initiative currently under development will enable us to more reliably determine an individual's eligibility to hold a security clearance or a sensitive position on an on-going basis.

The DNI's C.E. tool must provide an enterprise-wide solution that will ensure timely sharing of relevant information across security elements of the Federal Government as appropriate. There are a number of on-going pilot studies to assess the feasibility of selected automated record checks and the utility of publicly-available electronic information to include social media sites in the personnel security process.

While we fully recognize the value of publicly-available electronic information and its relevancy from an adjudicative perspective, there are resource, privacy, and civil liberty concerns that must be addressed as we incorporate such checks into our security processes.

In addition to supporting security clearance determinations, robust C.E. initiatives will also support and inform the Insider Threat programs. Damage assessments regarding individuals in-

volved in unauthorized disclosures of Classified information or acts of workplace violence have uncovered information that was not discovered during the existing security clearance process. Timely knowledge of such information might have prompted a security review or increased monitoring of that individual.

We must build an enterprise-wide C.E. program that will promote the sharing of trustworthiness, eligibility, and risk data within and across agencies to ensure the information is readily available for analysis and action.

Consistency in the quality of these investigations and adjudications is another area in need of attention. The revised Federal Investigative Standards will provide clear guidance on issue identification and resolution. They will also create an aligned system for consistent assessment of suitability, fitness, or eligibility for access to Classified information for Federal employment or to perform work under a Federal contract.

These standards will be implemented through a phased approach beginning in 2014 and continuing through 2017. In addition, the ODNI, OPM, and DOD are co-chairing a working group to develop common standards and metrics for evaluating quality and comprehensiveness for background investigations. In addition, the DNI has hosted a working group to refine the adjudicative guidelines, and recommendations regarding these guidelines are in the policy development stage.

Another initiative supporting a more robust security clearance process was the development of the National Training Standards, which were approved in August 2012 by the DNI and the director of OPM. These training standards create uniform training criteria for background investigators, National security adjudicators, and suitability adjudicators. Personnel mobility makes the application of uniform standards for conducting a background investigation and rendering an eligibility determination essential.

The training standards and revised investigative standards complement each other and, when both begin implementation in 2014, will result in a more robust security clearance process that supports security clearance reciprocity.

As a final note, OMB, the DNI, and OPM are engaged in two further initiatives that will enhance security clearance processing. We are currently revising 5 Code of Federal Regulation 732, which will be reissued as 1400, to provide clarifying guidance to departments and agencies when designating National security-sensitive positions.

Guidance from the reissued regulation will be used to update OPM's position designation tool. This will assist departments and agencies in determining position sensitivity and the type of clearance processing that will be required for each position.

The DNI is also working with OMB and OPM to revise the Standard Form 86, which is the questionnaire for National security positions. This form is completed by individuals requiring security clearances and is a starting point for the security background investigation.

In accordance with the President's directive, OMB is conducting a 120-day review of the security and suitability processes. In support of that effort, the DNI, as security executive agent, will work

in coordination with OPM, DOD, and the other agencies to review the policies, procedures, and processes related to the initiation, investigation, and adjudication of background investigations for personnel security, suitability for employment, and fitness for perform on a contract.

I want to emphasize the DNI's resolve to lead these initiatives discussed today and to continue the collaborative efforts established with OMB, DOD, OPM, and our other Federal partners. Thank you for the opportunity to update the subcommittee.

[The prepared statement of Mr. Prioletti follows:]

PREPARED STATEMENT OF BRIAN A. PRIOLETTI

NOVEMBER 13, 2013

Chairman King, Ranking Member Higgins, and distinguished Members of the subcommittee, thank you for the invitation to provide information on the Government's practices and procedures regarding security clearances and background investigations. My statement will address the role of the Director of National Intelligence (DNI), as Security Executive Agent, his authorities and responsibilities for oversight of the security clearance process across Government, areas in need of attention in the current process, and initiatives underway to address those areas.

THE DNI'S ROLE IN THE SECURITY CLEARANCE PROCESS

Pursuant to Executive Order 13467, the DNI, as the Security Executive Agent, is responsible for the development and oversight of effective, efficient, uniform policies and procedures governing the timely conduct of investigations and adjudications for eligibility for access to Classified information or eligibility to hold a sensitive position. The Security Executive Agent also serves as the final authority to designate agencies to conduct background investigations and determine eligibility for access to Classified information, and ensures reciprocal recognition of investigations and adjudication determinations among agencies.

THE RELATIONSHIP BETWEEN BACKGROUND CHECKS AND THE SECURITY CLEARANCE PROCESS

A background check is an essential component of the security clearance process. It is required prior to making a determination for eligibility for access to Classified information or eligibility to occupy a sensitive position. The 1997 Federal Investigative Standards, as amended in 2004, are the current standards used to conduct background investigations. The scope of the background investigation is dependent upon the level of security clearance required. A SECRET clearance includes National agency, local agency, and credit checks. An interview with the individual being considered for the clearance is conducted if necessary to resolve issues resulting from the required checks. A TOP SECRET clearance requires the above checks as well as interviews of the individual being considered for the clearance, and his or her references, co-workers, supervisors, neighbors, and other individuals. Regardless of the type of clearance involved, identified issues must be fully investigated and resolved prior to any adjudication.

THE ODNI'S STANDARDS AND POLICIES FOR ADJUDICATING SECURITY CLEARANCE APPLICATIONS

The Adjudicative Guidelines issued by the White House in 2005, currently serve as the Government-wide guide for most eligibility decisions. The DNI has issued separate Adjudicative Guidelines for Sensitive Compartmented Information (SCI) and Special Access Program access. Adjudicative decisions are made by utilizing the whole-person concept, which is the careful weighing of available, reliable information about the person, past and present, favorable and unfavorable.

AREAS OF THE SECURITY CLEARANCE PROCESS IN NEED OF ATTENTION AND POTENTIAL SOLUTIONS

Recent events involving individuals with clearances have further emphasized the importance of a robust security clearance program and areas in need of attention in the current security clearance process. Under the direction of the Performance Accountability Council, the ODNI, in collaboration with OMB, OPM, DoD, and other

Federal partners, has been leading security clearance reform efforts for several years. Although these efforts are still a work in progress, when mature, they will mitigate adjudicative gaps and enhance the Nation's security posture.

One critical element for a robust security clearance process is to establish an effective capability to assess an individual's continuing eligibility on a more frequent basis. Under current policies and practices, an individual's continued eligibility for access to Classified information relies heavily on a periodic reinvestigation; essentially a background investigation and adjudication conducted every 5 years for Top Secret clearances or every 10 years for Secret clearances. The time interval between periodic reinvestigations leaves the U.S. Government potentially uninformed as to behavior that poses a security or counterintelligence risk.

Continuous Evaluation (CE) is a tool that will assist in closing this information gap. Per Executive Order 13467 and the revised Federal Investigative Standards signed in 2012, CE allows for a review at any time of an individual with eligibility or access to Classified information, or in a sensitive position, to ensure that the individual continues to meet the requirements for eligibility.

CE, as envisioned in the reformed security clearance process, includes automated records checks of commercial databases, Government databases, and other information lawfully available. Manual checks are inefficient and resource-intensive. The CE initiative currently under development will enable us to more reliably determine an individual's eligibility to hold a security clearance or sensitive position on an ongoing basis. The DNI's CE tool must provide an enterprise-wide solution that will ensure timely sharing of relevant information across security elements of the Federal Government, as appropriate. There are a number of on-going pilot studies to assess the feasibility of select automated records checks and the utility of publicly available electronic information, to include social media sites, in the personnel security process. While we fully recognize the value of publicly-available electronic information and its relevancy from an adjudicative perspective, there are resource, privacy, and civil liberty concerns that must be addressed as we incorporate such checks into our security processes.

In addition to supporting security clearance determinations, robust CE initiatives will also support and inform Insider Threat Programs. Damage assessments regarding individuals involved in unauthorized disclosures of Classified information or acts of workplace violence have uncovered information that was not discovered during the existing security clearance process. Timely knowledge of such information might have prompted a security review or increased monitoring of the individual. We must build an enterprise-wide CE program that will promote the sharing of trustworthiness, eligibility, and risk data within and across agencies to ensure that information is readily available for analysis and action.

Consistency in the quality of investigations and adjudications is another area in need of attention. The revised Federal Investigative Standards will provide clear guidance on issue identification and resolution. They will also create an aligned system for consistent assessment of suitability, fitness, or eligibility for access to Classified information for Federal employment or to perform work under a Federal contract. The standards will be implemented through a phased approach beginning in 2014 and continuing through 2017. In addition, ODNI, OPM, and DOD are co-chairing a working group to develop common standards and metrics for evaluating quality and comprehensiveness of background investigations. Furthermore, ODNI has hosted a working group to refine the Adjudicative Guidelines; recommendations regarding these guidelines are in the policy development phase.

Another initiative supporting a more robust security clearance process was the development of the National Training Standards, which were approved in August 2012 by the DNI and Director of OPM. These training standards create uniform training criteria for background investigators, National security adjudicators, and suitability adjudicators. Personnel mobility makes the application of uniform standards for conducting a background investigation and rendering an eligibility determination essential. The training standards and the revised investigative standards complement each other and when both begin implementation in 2014, will result in a more robust security clearance process that support security clearance reciprocity.

As a final note, OMB, the ODNI, and OPM are engaged in two further initiatives that will enhance security clearance processing. We are currently revising 5 Code of Federal Regulation 732, which will be reissued as 1400, to provide clarifying guidance to departments and agencies when designating National security sensitive positions. Guidance from the reissued regulation will be used to update OPM's Position Designation Tool. This will assist departments and agencies in determining position sensitivity and the type of security clearance processing that will be required for each position. ODNI is also working with OMB and OPM to revise the Standard Form 86, *Questionnaire for National Security Positions.* This form is completed by

individuals requiring security clearances and is the starting point for a background investigation. It is imperative that we collect accurate information pertinent to today's security and counterintelligence concerns.

THE DNI'S ROLE IN THE PRESIDENT'S DIRECTIVE FOR INTER-AGENCY REVIEW OF THE CLEARANCE PROCESS

In accordance with the President's directive, OMB is conducting a 120-day review of security and suitability processes. In support of that effort, the DNI, as Security Executive Agent, will work in coordination with the OPM, DoD, and other agencies to review the policies, processes, and procedures related to the initiation, investigation, and adjudication of background investigations for personnel security, suitability for employment, and fitness to perform work on a contract.

CLOSING

Over the last 5 years, significant strides have been made in improving the security clearance process, particularly in the terms of timeliness and aligned National policies that provide the framework for consistency across Government. I want to emphasize the DNI's resolve to lead the initiatives discussed today and to continue the collaborative efforts established with OMB, DoD, OPM, and our other Federal partners. I thank you for the opportunity to update the subcommittee at this time and ODNI looks forward to working with you on these matters.

Mr. KING. Thank you, Mr. Prioletti.

Ms. Farrell, you are recognized. Thank you.

STATEMENT OF BRENDA S. FARRELL, DIRECTOR, DEFENSE CAPABILITIES AND MANAGEMENT, MILITARY AND DOD CIVILIAN PERSONNEL ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Ms. FARRELL. Chairman King, Ranking Member Higgins, thank you for the opportunity to be here today to discuss the quality of the Federal Government's personnel security clearance process. Let me briefly summarize my written statement for the record.

Personnel security clearances allow for access to Classified information on a need-to-know basis. Recent events, such as unauthorized disclosures of Classified information, have shown that there is much more work to be done by Federal agencies to help ensure the process functions effectively and efficiently so that only trustworthy individuals hold security clearances.

Over the years, GAO has conducted a broad body of work on personnel security clearance issues that gives us a unique historical perspective. My remarks today are based on our reports issued between 2008 and 2013 on DOD's personnel security clearance program and Government-wide reform efforts. My main message today is that quality—and importantly, quality metrics—should be built into every step of the process.

My written statement is divided into three parts. The first addresses the roles and responsibilities of several Executive branch agencies involved in the security clearance process.

For example, in 2008 Executive Order 13467 designated the DNI as the security executive agent. As such, the DNI is responsible for policies and procedures to help ensure the effective, efficient, and timely completion of background investigations and adjudications related to determinations of eligibility for access to Classified information. Importantly, since 2008 reform efforts to improve the personnel security clearance process throughout the Government have been principally driven and overseen by the Performance Accountability Council, which is chaired by the deputy director for manage-

ment at OMB. Executive Order 13467 established this governance structure.

The second part of my written statement addresses the different phases of the clearance process. Executive branch agencies rely on a multi-phased process that includes requirements determination; application; investigation; adjudication; appeals, if applicable, where a clearance has been denied; and reinvestigation for renewals or upgrade of an existing clearance.

The first step of the process is for the Executive branch agency, such as Homeland Security, to determine whether a position requires access to Classified information. After an individual has been selected for a position that requires a personnel security clearance he or she submits an application for a clearance. OPM—often contractors—conducts the background investigation. Adjudicators from the requesting agency use the resulting OPM investigation report and consider Federal guidelines to determine whether an applicant is eligible for a clearance.

The last part of my written statement addresses the extent to which the Executive branch assesses quality of the process. For more than a decade GAO has emphasized the need to build and monitor quality throughout the clearance process to promote oversight and positive outcomes, such as maximizing the likelihood that individuals who are security risk will be scrutinized more closely.

For example, in 2009 we reported concerns with the quality of OPM's investigations. We reported that with respect to initial Top Secret clearances adjudicated in July 2008 for DOD, documentation was incomplete for most of OPM's investigative reports.

We independently estimated that 87 percent of 3,500 investigative reports that DOD adjudicators used to make a clearance eligibility decisions were missing some required documentation, such as the verification of all of the applicant's employment. We also estimated that about 12 percent of the 3,500 reports did not contain the required applicant's interview.

In 2009 we recommended that OPM measure the frequency with which its investigative reports met Federal Investigative Standards in order to improve the quality of the investigative documentation. As of August 2013 OPM had not implemented this recommendation.

In summary, the large number of personnel eligible to hold clearances—over 4.9 million—coupled with risk to National security underscores the need for a high-quality personnel security clearance process.

Mr. Chairman, this concludes my remarks. I will be pleased to take questions when you are ready.

[The prepared statement of Ms. Farrell follows:]

PREPARED STATEMENT OF BRENDA S. FARRELL

NOVEMBER 13, 2013

GAO HIGHLIGHTS

Highlights of GAO–14–186T, a testimony before the Subcommittee on Counterterrorism and Intelligence, Committee on Homeland Security, U.S. House of Representatives.

Why GAO Did This Study

In 2012, the DNI reported that more than 4.9 million Federal Government and contractor employees held or were eligible to hold a personnel security clearance. Furthermore, GAO has reported that the Federal Government spent over $1 billion to conduct more than 2 million background investigations in fiscal year 2011. A high-quality process is essential to minimize the risks of unauthorized disclosures of Classified information and to help ensure that information about individuals with criminal activity or other questionable behavior is identified and assessed as part of the process for granting or retaining clearances. Security clearances may allow personnel to gain access to Classified information that, through unauthorized disclosure, can in some cases cause exceptionally grave damage to U.S. National security. Recent events, such as unauthorized disclosures of Classified information, have illustrated the need for additional work to help ensure the process functions effectively and efficiently.

This testimony addresses the: (1) Roles and responsibilities of different Executive branch agencies involved in the personnel security process; (2) different phases of the process; and (3) extent that agencies assess the quality of the process. This testimony is based on GAO work issued between 2008 and 2013 on DOD's personnel security clearance program and Government-wide suitability and security clearance reform efforts. As part of that work, GAO: (1) Reviewed statutes, Executive Orders, guidance, and processes; (2) examined agency data on timeliness and quality; (3) assessed reform efforts; and (4) reviewed samples of case files for DOD personnel.

PERSONNEL SECURITY CLEARANCES.—OPPORTUNITIES EXIST TO IMPROVE QUALITY THROUGHOUT THE PROCESS

What GAO Found

Several agencies in the Executive branch have key roles and responsibilities in the personnel security clearance process. Executive Order 13467 designates the director of National Intelligence (DNI) as the Security Executive Agent, who is responsible for developing policies and procedures for background investigations and adjudications. The Office of Personnel Management (OPM) conducts investigations for most of the Federal Government. Adjudicators from agencies, such as the Departments of Defense (DOD) and Homeland Security, that request background investigations use the investigative report and consider Federal adjudicative guidelines when making clearance determinations. Reform efforts to enhance the personnel security process throughout the Executive branch are principally driven and overseen by the Performance Accountability Council, which is chaired by the Deputy Director for Management at the Office of Management and Budget (OMB).

Executive branch agencies rely on a multi-phased personnel security clearance process that includes requirements determination, application, investigation, adjudication, appeals (if applicable, where a clearance has been denied), and reinvestigation (for renewal or upgrade of an existing clearance). In the requirements determination phase, agency officials must determine whether positions require access to Classified information. After an individual has been selected for a position that requires a personnel security clearance and the individual submits an application for a clearance, investigators—often contractors—from OPM conduct background investigations for most Executive branch agencies. Adjudicators from requesting agencies use the information from these investigations and consider Federal adjudicative guidelines to determine whether an applicant is eligible for a clearance. If a clearance is denied or revoked by an agency, appeals of the adjudication decision are possible. Individuals granted clearances are subject to reinvestigations at intervals that are dependent on the level of security clearance.

Executive branch agencies do not consistently assess quality throughout the security clearance process, in part because they have not fully developed and implemented metrics to measure quality in key aspects of the process. For example, GAO reported in May 2009 that, with respect to initial Top Secret clearances adjudicated in July 2008 for DOD, documentation was incomplete for most of OPM's investigative reports. GAO also estimated that 12 percent of the 3,500 reports did not contain the required personal subject interview. To improve the quality of investigative documentation, GAO recommended that OPM measure the frequency with which its reports met Federal investigative standards. OPM did not agree or disagree with this recommendation, and as of August 2013 had not implemented it. Further, GAO reported in 2010 that agencies do not consistently and comprehensively track the reciprocity of personnel security clearances, which is an agency's acceptance of a background investigation or clearance determination completed by any authorized investigative or adjudicative agency. OPM created a metric in early 2009 to track reciprocity, but this metric does not track how often an existing security clearance was

successfully honored. GAO recommended that OMB develop comprehensive metrics to track reciprocity. OMB agreed with the recommendation, but has not yet fully implemented actions to implement this recommendation.

Chairman King, Ranking Member Higgins, and Members of the subcommittee: Thank you for the opportunity to be here to discuss the quality of the Federal Government's personnel security clearance process. In 2012, the Director of National Intelligence (DNI) reported that more than 4.9 million Federal Government and contractor employees held or were eligible to hold a security clearance,[1] posing formidable challenges to those responsible for deciding who should be granted a clearance. Personnel security clearances allow for access to Classified information on a need-to-know basis. Federal agencies also use other processes and procedures to determine if an individual should be granted access to certain Government buildings or facilities or be employed as a military, Federal civilian, or contractor employee for the Federal Government. Separate from, but related to, personnel security clearances are determinations of suitability that the Executive branch uses to ensure individuals are suitable, based on character and conduct, for Federal employment in their agency or position. We have reported that the Federal Government spent over $1 billion to conduct more than 2 million background investigations (in support of both personnel security clearances and suitability determinations for Government employment outside of the intelligence community) in fiscal year 2011.[2]

A high-quality process is essential in order to minimize the risks of unauthorized disclosures of Classified information and to help ensure that information about individuals with criminal activity or other questionable behavior is identified and assessed as part of the process for granting or retaining clearances. Security clearances may allow personnel to gain access to Classified information that, through unauthorized disclosure, can in some cases cause exceptionally grave damage to U.S. National security. Recent events, such as unauthorized disclosures of Classified information, have illustrated both the potential consequences of such disclosures and the need for additional work on the part of Federal agencies to help ensure the process functions effectively and efficiently, so that only trustworthy individuals obtain and keep security clearances and the resulting access to Classified information that clearances make possible. We have an extensive body of work on issues related to the personnel security clearance process going back over a decade. Since 2008, we have focused on the Department of Defense's (DOD) clearance program and the Government-wide effort to reform the security clearance process, and have reported repeatedly on the need to build quality into the process.

My testimony today will focus on three topics related to personnel security clearances: (1) The roles and responsibilities of the different Executive branch agencies involved in the personnel security clearance process, (2) the different phases of the security clearance process that are typically followed by most Executive branch agencies, and (3) the extent that Executive branch agencies assess the quality of the security clearance process during these different phases.

This testimony is based on our reports and testimonies issued from 2008 through 2013 on DOD's personnel security clearance program and Government-wide suitability and security clearance reform efforts. A list of these related products appears at the end of my statement. As part of the work for these products, we reviewed relevant statutes and Executive Orders, Federal guidance, and processes; examined agency personnel security clearance policies; examined agency data on the timeliness and quality of investigations and adjudications; assessed reform efforts; and reviewed a sample of investigative and adjudication files for DOD personnel. Further, as part of our on-going effort to determine the status of agency actions to address our prior recommendations, we reviewed the current proposal to revise a relevant Federal regulation regarding position designation.

The work upon which this testimony is based was conducted in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Additional details about the scope and methodology can be found in each of these related products.

---

[1] Office of the Director of National Intelligence, *2012 Report on Security Clearance Determinations* (January 2013).

[2] GAO, *Background Investigations: Office of Personnel Management Needs to Improve Transparency of Its Pricing and Seek Cost Savings,* GAO–12–197 (Washington, DC: Feb. 28, 2012).

AGENCIES' ROLES AND RESPONSIBILITIES IN THE PERSONNEL SECURITY CLEARANCE PROCESS

Several agencies in the Executive branch have key roles and responsibilities in the Federal Government's personnel security clearance process. In a 2008 memorandum, the President called for a reform of the security clearance and suitability determination processes and subsequently issued Executive Order 13467,[3] which designates the Director of National Intelligence (DNI) as the Security Executive Agent. As such, the DNI is responsible for developing policies and procedures to help ensure the effective, efficient, and timely completion of background investigations and adjudications relating to determinations of eligibility for access to Classified information and eligibility to hold a sensitive position. Positions designated as sensitive are any positions within a department or agency where the occupant could bring about, by virtue of the nature of the position, a material adverse effect on National security.

Further, Executive Order 13467 established a Suitability and Security Clearance Performance Accountability Council, commonly called the Performance Accountability Council, that is accountable to the President for achieving the goals of the reform effort, which include an efficient, practical, reciprocal, and aligned system for investigating and determining eligibility for access to Classified information. Under the Executive Order, this council is responsible for driving implementation of the reform effort, including ensuring the alignment of security and suitability processes, holding agencies accountable for implementation, and establishing goals and metrics for progress. The Order also appointed the Deputy Director for Management at the Office of Management and Budget (OMB) as the chair of the council.[4] In addition, the Executive Order states that agency heads shall assist the Performance Accountability Council and executive agents in carrying out any function under the Order, as well as implementing any policies or procedures developed pursuant to the Order.

Executive branch agencies that request background investigations use the information from investigative reports to determine whether an applicant is eligible for a personnel security clearance. Two of the agencies that grant the most security clearances are DOD and the Department of Homeland Security (DHS). DOD accounts for the majority of all personnel security clearances, and spent $787 million on suitability and security clearance background investigations in fiscal year 2011.[5] Investigators—often contractors—from Federal Investigative Services within the Office of Personnel Management (OPM)[6] conduct the investigations for most of the Federal Government.[7] DOD is OPM's largest customer, and its Under Secretary of Defense for Intelligence (USD(I)) is responsible for developing, coordinating, and overseeing the implementation of DOD policy, programs, and guidance for personnel, physical, industrial, information, operations, chemical/biological, and DOD Special Access Program security. Additionally, the Defense Security Service, under

---

[3] Executive Order No. 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information* (June 30, 2008).

[4] The Performance Accountability Council is comprised of the Director of National Intelligence as the Security Executive Agent, the Director of OPM as the Suitability Executive Agent, and the Deputy Director for Management, Office of Management and Budget, as the chair with the authority to designate officials from additional agencies to serve as members. As of June 2012, the council included representatives from the Departments of Defense, Energy, Health and Human Services, Homeland Security, State, Treasury, and Veterans Affairs, and the Federal Bureau of Investigation.

[5] GAO, *Background Investigations: Office of Personnel Management Needs to Improve Transparency of Its Pricing and Seek Cost Savings*, GAO–12–197 (Washington, DC: Feb. 28, 2012).

[6] OPM's Federal Investigative Services employs both Federal and contract investigators to conduct work required to complete background investigations. The Federal staff constitutes about 25 percent of that workforce, while OPM currently also has contracts for investigative fieldwork with several investigation firms, constituting the remaining 75 percent of its investigative workforce.

[7] In 2005, the Office of Management and Budget designated OPM as the agency responsible for, among other things, the day-to-day supervision and monitoring of security clearance investigations, and for tracking the results of individual agency-performed adjudications, subject to certain exceptions. However, the Office of the Director of National Intelligence can designate other agencies as an "authorized investigative agency" pursuant to 50 U.S.C. § 3341(b)(3), as implemented through Executive Order 13467. Alternatively, under 5 U.S.C. § 1104(a)(2), OPM can redelegate any of its investigative functions subject to performance standards and a system of oversight prescribed by OPM under 5 U.S.C. § 1104(b). Agencies without delegated authority rely on OPM to conduct their background investigations while agencies with delegated authority—including the Defense Intelligence Agency, National Security Agency, National Geospatial-Intelligence Agency, Central Intelligence Agency, Federal Bureau of Investigation, National Reconnaissance Office, and Department of State—have been authorized to conduct their own background investigations.

the authority, direction, and control of USD(I), manages and administers the DOD portion of the National Industrial Security Program [8] for the DOD components and other Federal agencies by agreement, as well as providing security education and training, among other things.

DHS spent more than $57 million on suitability and security clearance background investigations in fiscal year 2011. Within DHS, the Chief Security Officer develops, implements, and oversees the Department's security policies, programs, and standards; delivers security training and education to DHS personnel; and provides security support to the DHS components. The Chief of DHS's Personnel Security Division, under the direction of the Chief Security Officer, has responsibility for personnel security and suitability policies, programs, and standards, including procedures for granting, denying, and revoking access to Classified information as well as initiating and adjudicating personnel security and suitability background investigations and periodic reinvestigations of applicants. Within the DHS components, the component Chief Security Officers implement established personnel security directives and policies within their respective components.

The personnel security clearance process has also been the subject of Congressional oversight and statutory reporting requirements. Section 3001 of the Intelligence Reform and Terrorism Prevention Act of 2004 [9] prompted Government-wide suitability and security clearance reform. The act required, among other matters, an annual report to Congress—in February of each year from 2006 through 2011—about progress and key measurements on the timeliness of granting security clearances. It specifically required those reports to include the periods of time required for conducting investigations and adjudicating or granting clearances. However, the Intelligence Reform and Terrorism Prevention Act requirement for the Executive branch to report annually on its timeliness expired in 2011. More recently, the Intelligence Authorization Act of 2010 [10] established a new requirement that the President annually report to Congress the total amount of time required to process certain security clearance determinations for the previous fiscal year for each element of the intelligence community.[11] The Intelligence Authorization Act of 2010 additionally requires that those annual reports include the total number of active security clearances throughout the United States Government, to include both Government employees and contractors. Unlike the Intelligence Reform and Terrorism Prevention Act of 2004 reporting requirement, the requirement to submit these annual reports does not expire.

PHASES OF THE PERSONNEL SECURITY PROCESS

To help ensure the trustworthiness and reliability of personnel in positions with access to Classified information, Executive branch agencies rely on a personnel security clearance process that includes multiple phases: Requirements determination, application, investigation, adjudication, appeals (if applicable, where a clearance has been denied), and reinvestigation (where applicable, for renewal or upgrade of an existing clearance). Figure 1 illustrates the steps in the personnel security clearance process, which is representative of the general process followed by most Executive branch agencies and includes procedures for appeals and renewals. While different departments and agencies may have slightly different personnel security clearance processes, the phases that follow are illustrative of a typical process.[12] Since 1997, Federal agencies have followed a common set of personnel security investigative standards and adjudicative guidelines for determining whether Federal civilian workers, military personnel, and others, such as private industry personnel contracted by the Government, are eligible to hold a security clearance.

---

[8] The National Industrial Security Program was established by Executive Order 12829 to safeguard Federal Government Classified information that is released to contractors, licensees, and grantees of the United States Government. Executive Order 12829, *National Industrial Security Program* (Jan. 6, 1993, as amended).

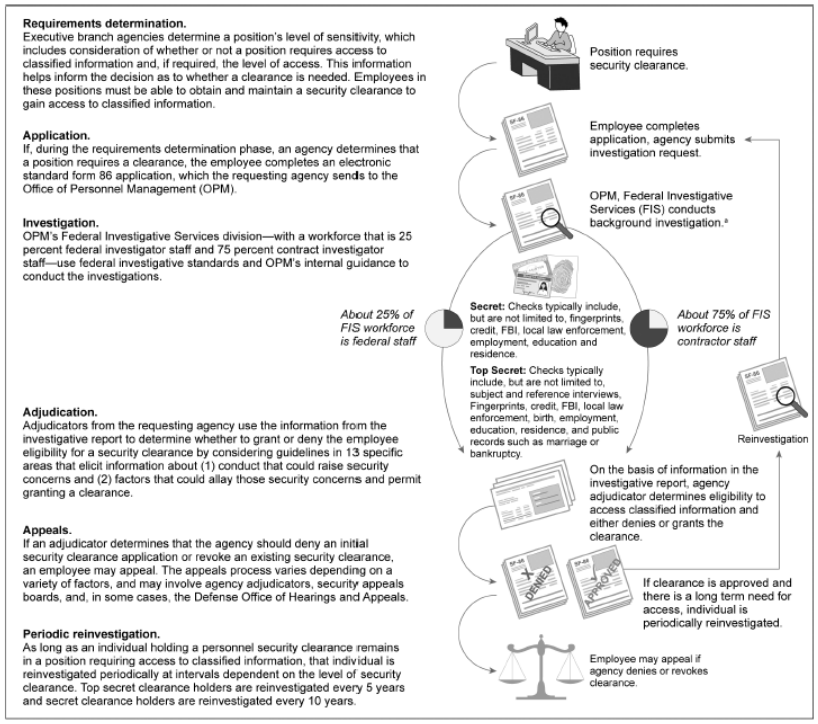
[9] Pub. L. No. 108–458 (2004) (relevant sections codified at 50 U.S.C. § 3341).

[10] Pub. L. No. 111–259, § 367 (2010) (codified at 50 U.S.C. § 3104).

[11] This timeliness reporting requirement applies only to the elements of the intelligence community; it does not cover non-intelligence agencies that were covered by the reporting requirements in the Intelligence Reform and Terrorism Prevention Act of 2004.

[12] The general process for performing a background investigation for either a Secret or Top Secret clearance is the same; however, the level of detail and types of information gathered for a Top Secret clearance is more substantial than a Secret clearance.

Figure 1: Phases of the Personnel Security Clearance Process



Source: GAO analysis.

[a]OPM provides background investigation services to over 100 executive branch agencies; however, others, including some agencies in the Intelligence Community, have been delegated authority from the Office of the Director of National Intelligence, OPM, or both, to conduct their own background investigations.

Requirements Determination Phase

Executive branch agencies first determine which of their positions—military, civilian, or private-industry contractors—require access to Classified information and, therefore, which people must apply for and undergo a personnel security clearance investigation. This involves assessing the risk and sensitivity level associated with that position, to determine whether it requires access to Classified information and, if required, the level of access. Security clearances are generally categorized into three levels: Top Secret, Secret, and Confidential.[13] The level of classification denotes the degree of protection required for information and the amount of damage that unauthorized disclosure could reasonably be expected to cause to National defense.[14]

A sound requirements process is important because requests for clearances for positions that do not need a clearance or need a lower level of clearance increase investigative workloads and costs. A high volume of clearances continue to be processed and a sound requirements determination process is needed to effectively manage costs, since agencies spend significant amounts annually on National security and other background investigations. In addition to cost implications, limiting the

[13] A Top Secret clearance is generally also required for access to Sensitive Compartmented Information—Classified intelligence information concerning or derived from intelligence sources, methods, or analytical processes that is required to be protected within formal access control systems established and overseen by the Director of National Intelligence.

[14] Unauthorized disclosure could reasonably be expected to cause: (1) "Damage," in the case of confidential information; (2) "serious damage," in the case of secret information; and (3) "exceptionally grave damage," in the case of Top Secret information. Exec. Order No. 13526, 75 Fed. Reg. 707 (Dec. 29, 2009).

access to Classified information and reducing the associated risks to National security underscore the need for Executive branch agencies to have a sound process to determine which positions require a security clearance.

Agency heads are responsible for designating positions within their respective agencies as sensitive if the occupant of that position could, by virtue of the nature of the position, bring about a material adverse effect on National security.[15] In addition, Executive Order 12968, issued in 1995, makes the heads of agencies—including Executive branch agencies and the military departments—responsible for establishing and maintaining an effective program to ensure that access to Classified information by each employee is clearly consistent with the interests of National security. This order also states that, subject to certain exceptions, eligibility for access to Classified information shall only be requested and granted on the basis of a demonstrated, foreseeable need for access. Further, part 732 of Title 5 of the Code of Federal Regulations provides requirements and procedures for the designation of National security positions, which include positions that: (1) Involve activities of the Government that are concerned with the protection of the Nation from foreign aggression or espionage, and (2) require regular use of or access to Classified National security information.[16]

Part 732 of Title 5 of the Code of Federal Regulations also states that most Federal Government positions that could bring about, by virtue of the nature of the position, a material adverse effect on National security must be designated as a sensitive position and require a sensitivity level designation. The sensitivity-level designation determines the type of background investigation required, with positions designated at a greater sensitivity level requiring a more extensive background investigation. Part 732 establishes three sensitivity levels—special-sensitive, critical-sensitive, and noncritical-sensitive—which are described in figure 2. According to OPM, positions that an agency designates as special-sensitive and critical-sensitive require a background investigation that typically results in a Top Secret clearance. Noncritical-sensitive positions typically require an investigation that supports a Secret or Confidential clearance. OPM also defines non-sensitive positions that do not have a National security element, and thus do not require a security clearance, but still require a designation of risk for suitability purposes. That risk level informs the type of investigation required for those positions. Those investigations include aspects of an individual's character or conduct that may have an effect on the integrity or efficiency of the service.

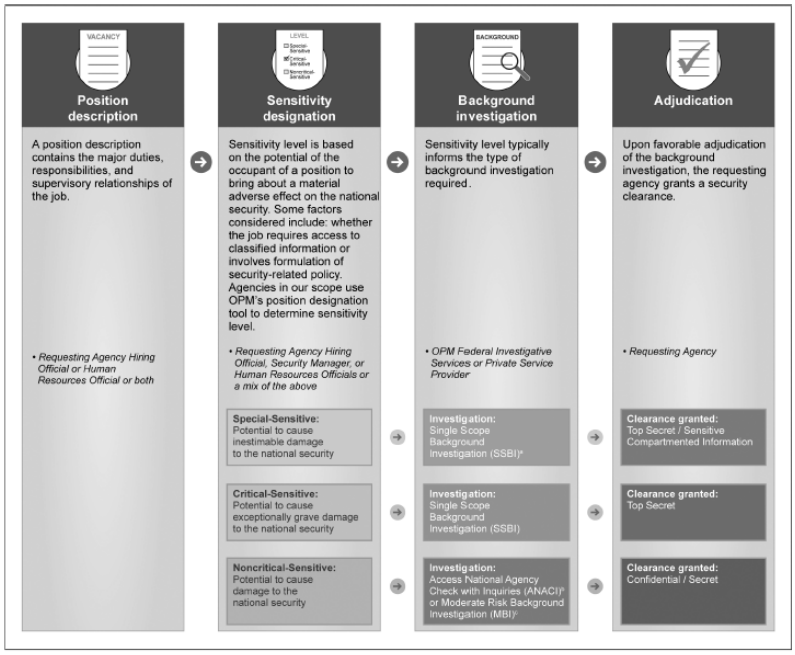
Figure 2 illustrates the process used by both DOD and DHS to determine the need for a personnel security clearance for a Federal civilian position generally used Government-wide.

---

[15] Sensitivity level is based on the potential of the occupant of a position to bring about a material adverse effect on National security. Some factors include whether the position requires access to Classified information or involves the formulation of security-related policy. The sensitivity level of a position then informs the type of background investigation required of the individual in that position. The relationship between sensitivity and resulting clearances is detailed in Figure 2.

[16] Those requirements in Part 732 apply to National security positions in the competitive service, Senior Executive Service positions filled by career appointment within the Executive branch, and certain excepted service positions.

Figure 2: Typical Security Clearance Determination Process for Federal Civilian Positions in the Departments of Defense and Homeland Security



Source: GAO analysis of Department of Homeland Security (DHS) and Department of Defense (DOD) data.

[a]A Single Scope Background Investigation (SSBI) is conducted so that an individual can obtain a top secret clearance (including Sensitive Compartmented Information) and includes a review of the locations where an individual has lived, attended school, and worked. In addition, an SSBI includes interviews with four references who have social knowledge of the subject, interviews with former spouses, and a financial record check.

[b]An Access National Agency Check and Inquiries (ANACI) is used for the initial investigation for federal employees at the confidential and secret access levels. It consists of employment checks,

Application Phase

Once an applicant is selected for a position that requires a personnel security clearance, the applicant must obtain a security clearance in order to gain access to Classified information. To determine whether an investigation would be required, the agency requesting a security clearance investigation conducts a check of existing personnel security databases to determine whether there is an existing security clearance investigation underway or whether the individual has already been favorably adjudicated for a clearance in accordance with current standards. If such a security clearance does not exist for that individual, a security officer from an Executive branch agency: (1) Requests an investigation of an individual requiring a clearance; (2) forwards a personnel security questionnaire (Standard Form 86) to the individual to complete using OPM's electronic Questionnaires for Investigations Processing (e–QIP) system or a paper copy; (3) reviews the completed questionnaire; and (4) sends the questionnaire and supporting documentation, such as fingerprints and signed waivers, to OPM or its investigation service provider.

Investigation Phase

During the investigation phase, investigators—often contractors—from OPM's Federal Investigative Services use Federal investigative standards and OPM's internal guidance to conduct and document the investigation of the applicant. The scope of information gathered in an investigation depends on the needs of the client agency and the personnel security clearance requirements of an applicant's position, as well as whether the investigation is for an initial clearance or a reinvestigation to renew a clearance. For example, in an investigation for a Top Secret clearance, investigators gather additional information through more time-consuming efforts, such as traveling to conduct in-person interviews to corroborate information about an ap-

plicant's employment and education. However, many background investigation types have similar components. For instance, for all investigations, information that applicants provide on electronic applications are checked against numerous databases. Both Secret and Top Secret investigations contain credit and criminal history checks, while Top Secret investigations also contain citizenship, public record, and spouse checks as well as reference interviews and an Enhanced Subject Interview to gain insight into an applicant's character. Table 1 highlights the investigative components generally associated with the Secret and Top Secret clearance levels. After OPM, or the designated provider, completes the background investigation, the resulting investigative report is provided to the requesting agencies for their internal adjudicators.

Type of Information Gathered by Component	Type of Background Investigation	
	Secret	Top Secret
(1) Personnel security questionnaire: The reported answers on an electronic SF–85P or SF–86 form	X	X
(2) Fingerprints: Fingerprints submitted electronically or manually	X	X
(3) National agency check: Data from Federal Bureau of Investigation, military records, and other agencies as required (with fingerprint).	X	X
(4) Credit check: Data from credit bureaus where the subject lived/worked/attended school for at least 6 months.	X	X
(5) Local agency checks: Data from law enforcement agencies where the subject lived/worked/attended school during the past 10 years or—in the case of reinvestigations—since the last security clearance investigation.	X	X
(6) Date and place of birth: Corroboration of information supplied on the personnel security questionnaire		X
(7) Citizenship: For individuals born outside of the United States, verification of U.S. citizenship directly from the appropriate registration authority.		X
(8) Education: Verification of most recent or significant claimed attendance, degree, or diploma	M	X
(9) Employment: Review of employment records and interviews with workplace references, such as supervisors and coworkers.	M	X
(10) References: Data from interviews with subject-identified and investigator-developed leads	M	X
(11) Data from Federal Bureau of Investigation, military records, and other agencies as required (without fingerprint).		X
(12) Former spouse: Data from interview(s) conducted with spouse(s) divorced within the last 10 years or since the last investigation or reinvestigation.		X
(13) Neighborhoods: Interviews with neighbors and verification of residence through records check	M	X
(14) Public records: Verification of issues, such as bankruptcy, divorce, and criminal and civil court cases		X
(15) Enhanced Subject Interview: Collection of relevant data, resolution of significant issues or inconsistencies.	[1]	X

Source.—DOD and OPM.

Note.—The content and amount of information collected as part of a personnel security clearance investigation is dependent on a variety of case-specific factors, including the history of the applicant and the nature of the position; however, items 1–15 are typically collected for the types of investigations indicated.

M=Components with this notation are checked through requests for information sent by OPM's Federal Investigative Services through the mail.

[1] The Enhanced Subject Interview was developed by the Joint Reform Team and implemented by OPM in 2011 and serves as an in-depth discussion between the interviewer and the subject to ensure a full understanding of the applicant's information, potential issues, and mitigating factors. It is included in a Minimum Background Investigation, one type of suitability investigation, and can be triggered by the presence of issues in a Secret-level investigation.

In December 2012, the Office of the Director of National Intelligence (ODNI) and OPM jointly issued a revised version of the Federal investigative standards for the conduct of background investigations for individuals that work for or on behalf of the Federal Government. According to October 31, 2013 testimony by an ODNI official, the revised standards will be implemented through a phased approach beginning in 2014 and continuing through 2017.[17]

Adjudication and Appeals Phases

During the adjudication phase, adjudicators from the hiring agency use the information from the investigative report along with Federal adjudicative guidelines to determine whether an applicant is eligible for a security clearance.[18] To make clearance eligibility decisions, the adjudicative guidelines specify that adjudicators consider 13 specific areas that elicit information about: (1) Conduct that could raise security concerns and (2) factors that could allay those security concerns and permit granting a clearance.[19] The adjudication process is a careful weighing of a number of variables, to include disqualifying and mitigating factors, known as the "whole-person" concept. For example, when a person's life history shows evidence of unreliability or untrustworthiness, questions can arise as to whether the person can be relied on and trusted to exercise the responsibility necessary for working in a secure environment where protecting National security is paramount. As part of the adjudication process, the adjudicative guidelines require agencies to determine whether a prospective individual meets the adjudicative criteria for determining eligibility, including personal conduct and financial considerations. If an individual has conditions that raise a security concern or may be disqualifying, the adjudicator evaluates whether there are other factors that mitigate such risks (such as a good-faith effort to repay a Federal tax debt). On the basis of this assessment, the agency may make a risk-management decision to grant the security-clearance eligibility determination, possibly with a warning that future incidents of a similar nature may result in revocation of access.

If a clearance is denied or revoked, appeals of the adjudication decision are generally possible. We have work underway to review the process for security clearance revocations. We expect to issue a report on this process in the spring of 2014.

Reinvestigation Phase

Once an individual has obtained a personnel security clearance and as long as they remain in a position that requires access to Classified National security information, that individual is reinvestigated periodically at intervals that are dependent on the level of security clearance. For example, Top Secret clearance-holders are reinvestigated every 5 years, and Secret clearance-holders are reinvestigated every 10 years. Some of the information gathered during a reinvestigation would focus specifically on the period of time since the last approved clearance, such as a check of

---

[17] Brian A. Prioletti, Assistant Director, Special Security Directorate, National Counterintelligence Executive, Office of the Director of National Intelligence, *Statement for the Record: Open Hearing on Security Clearance Reform,* testimony before the Senate Committee on Homeland Security and Governmental Affairs, 113th Cong., 1st sess., October 31, 2013.

[18] For industry personnel, the Defense Security Service (DSS) adjudicated clearance eligibility for DOD and 24 other Federal agencies, by agreement, using OPM-provided investigative reports. However, DOD is in the process of consolidating its adjudication facilities, including those for industry personnel. Per DOD 5220.22–M, *National Industrial Security Program: Operating Manual* (Feb. 28, 2006 incorporating changes Mar. 28, 2013), those agencies are: (1) National Aeronautics and Space Administration; (2) Department of Commerce; (3) General Services Administration; (4) Department of State; (5) Small Business Administration; (6) National Science Foundation; (7) Department of the Treasury; (8) Department of Transportation; (9) Department of the Interior; (10) Department of Agriculture; (11) Department of Labor; (12) Environmental Protection Agency; (13) Department of Justice; (14) Federal Reserve System; (15) U.S. Government Accountability Office; (16) U.S. Trade Representative; (17) U.S. International Trade Commission; (18) U.S. Agency for International Development; (19) Nuclear Regulatory Commission; (20) Department of Education; (21) Department of Health and Human Services; (22) Department of Homeland Security; (23) Federal Communications Commission; and (24) Office of Personnel Management.

[19] Federal guidelines state that clearance decisions require a common-sense determination of eligibility for access to Classified information based upon careful consideration of the following 13 areas: Allegiance to the United States; foreign influence; foreign preference; sexual behavior; personal conduct; financial considerations; alcohol consumption; drug involvement; emotional, mental, and personality disorders; criminal conduct; security violations; outside activities; and misuse of information technology systems. Further, the guidelines require adjudicators to evaluate the relevance of an individual's overall conduct by considering factors such as the nature, extent, and seriousness of the conduct; the circumstances surrounding the conduct, to include knowledgeable participation; the frequency and recency of the conduct; and the individual's age and maturity at the time of the conduct, among others.

local law enforcement agencies where an individual lived and worked since the last investigation.

Further, the Joint Reform Team [20] began an effort to review the possibility of continuous evaluations, which would ascertain on a more frequent basis whether an eligible employee with access to Classified information continues to meet the requirements for access. Specifically, the team proposed to move from periodic review to that of continuous evaluation, meaning annually for Top Secret and similar positions and at least once every 5 years for Secret or similar positions, as a means to reveal security-relevant information earlier than the previous method, and provide increased scrutiny on populations that could potentially represent risk to the Government because they already have access to Classified information. The revised Federal investigative standards state that the Top Secret level of security clearances may be subject to continuous evaluation.

AGENCIES DO NOT CONSISTENTLY ASSESS QUALITY THROUGHOUT THE PERSONNEL SECURITY CLEARANCE PROCESS

Executive branch agencies do not consistently assess quality throughout the personnel security clearance process, in part because they have not fully developed and implemented metrics to measure quality in key aspects of the personnel security clearance process. To promote oversight and positive outcomes, such as maximizing the likelihood that individuals who are security risks will be scrutinized more closely, we have emphasized, since the late 1990s,[21] the need to build and monitor quality throughout the personnel security clearance process. While our work historically was focused on DOD, particularly since we placed DOD's personnel security clearance program on our high-risk list [22] in 2005 because of delays in completing clearances,[23] we have included DHS in our most recent reviews of personnel security clearance issues. Having assessment tools and performance metrics in place is a critical initial step toward instituting a program to monitor and independently validate the effectiveness and sustainability of corrective measures.

Guidance Not Developed for Determining if Positions Require a Clearance or for Reviewing Existing Position Designations

In July 2012, we reported that the DNI, as the Security Executive Agent, had not provided agencies clearly-defined policy and procedures to consistently determine if a position requires a personnel security clearance, or established guidance to require agencies to review and revise or validate existing Federal civilian position designations.[24] As a result, we concluded that DHS and DOD, along with other Executive branch agencies, do not have reasonable assurance that security clearance position designations are correct, which could compromise National security if positions are underdesignated, or create unnecessary and costly investigative coverage if positions are overdesignated.

In the absence of clear guidance, agencies are using a position designation tool that OPM designed to determine the sensitivity and risk levels of civilian positions that, in turn, inform the type of investigation needed.[25] This tool—namely, the Position Designation of National Security and Public Trust Positions—is intended to enable a user to evaluate a position's National security and suitability requirements so as to determine a position's sensitivity and risk levels, which in turn dictate the type of background investigation that will be required for the individual who will occupy that position. Both DOD and DHS components use the tool. In addition,

---

[20] In 2007, DOD and the Office of the Director of National Intelligence (ODNI) formed the Joint Security Clearance Process Reform Team, known as the Joint Reform Team, to improve the security clearance process Government-wide.

[21] GAO, *DOD Personnel: Inadequate Personnel Security Investigations Pose National Security Risks,* GAO/NSIAD–00–12 (Washington, DC: Oct. 27, 1999).

[22] Every 2 years at the start of a new Congress, GAO issues a report that identifies Government operations that are high-risk due to their vulnerabilities to fraud, waste, abuse, and mismanagement, or are most in need of transformation to address economy, efficiency, or effectiveness.

[23] GAO, *High-Risk Series: An Update,* GAO–05–207 (Washington, DC: Jan. 1, 2005).

[24] GAO, *Security Clearances: Agencies Need Clearly Defined Policy for Determining Civilian Position Requirements,* GAO–12–800 (Washington, DC: July 12, 2012).

[25] According to OPM's Federal Investigations Notice No. 10–06, Position Designation Requirements (Aug. 11, 2010), the tool is recommended for all agencies requesting OPM investigations and required for all positions in the competitive service, positions in the excepted service where the incumbent can be noncompetitively converted to the competitive service, and career appointments in the Senior Executive Service.

DOD issued guidance in September 2011[26] and August 2012[27] requiring its personnel to use OPM's tool to determine the proper position sensitivity designation. A DHS instruction requires personnel to designate all DHS positions—including positions in the DHS components—by using OPM's position sensitivity designation guidance, which is the basis of the tool.[28]

OPM audits, however, have found inconsistency in these position designations, and some agencies described problems implementing OPM's tool. For example, during the course of our 2012 review, DOD and DHS officials raised concerns regarding the guidance provided through the tool and expressed that they had difficulty implementing it. Specifically, officials from DHS's U.S. Immigration and Customs Enforcement stated that the use of the tool occasionally resulted in inconsistency, such as over- or under-designating a position, and expressed a need for additional clear, easily-interpreted guidance on designating National security positions. DOD officials stated that they have had difficulty implementing the tool because it focuses more on suitability than security, and the National security aspects of DOD's positions are of more concern to them than the suitability aspects. Further, although the DNI was designated as the Security Executive Agent in 2008, ODNI officials noted that the DNI did not have input into recent revisions of OPM's position designation tool.

As a result, we recommended that the DNI, in coordination with the Director of OPM and other Executive branch agencies as appropriate, issue clearly-defined policy and procedures for Federal agencies to follow when determining if Federal civilian positions require a personnel security clearance. In written comments on our July 2012 report, the ODNI concurred with this recommendation. In May 2013, ODNI and OPM jointly drafted a proposed revision to the Federal regulations on position designation which, if finalized in its current form, would provide additional requirements and examples of position duties at each sensitivity level. We also recommended that once those policies and procedures are in place, the DNI and the Director of OPM, in their roles as executive agents, collaborate to revise the position designation tool to reflect the new guidance. ODNI and OPM concurred with this recommendation and recently told us that they are in the process of revising the tool.

In July 2012, we also reported that the Executive branch did not have a consistent process for reviewing and validating existing security clearance requirements for Federal civilian positions.[29] According to Executive Order 12968, the number of employees that each agency determines is eligible for access to Classified information shall be kept to the minimum required, and, subject to certain exceptions, eligibility shall be requested or granted only on the basis of a demonstrated, foreseeable need for access. During our 2012 review of several DOD and DHS components, we found that officials were aware of the need to keep the number of security clearances to a minimum but were not always subject to a standard requirement to review and validate the security clearance needs of existing positions on a periodic basis. We found, instead, that agencies' policies provided for a variety of practices for reviewing the clearance needs of Federal civilian positions. In addition, agency officials told us that their policies were implemented inconsistently.

DOD's personnel security regulation and other guidance[30] provides DOD components with criteria to consider when determining whether a position is sensitive or requires access to Classified information, and some DOD components also have developed their own guidance. According to DHS guidance, supervisors are responsible for ensuring that: (1) Position designations are updated when a position undergoes major changes (e.g., changes in missions and functions, job responsibilities, work assignments, legislation, or classification standards), and (2) position security designations are assigned as new positions are created. Some DHS components have additional requirements to review position designation more regularly to cover positions other than those newly created or vacant. For example, U.S. Coast Guard guidance[31] states that hiring officials and supervisors should review position descrip-

---

[26] DOD, Washington Headquarters Services, *Implementation of the Position Designation Automated Tool* (Sept. 27, 2011).

[27] DOD Instruction 1400.25, Volume 731, *DOD Civilian Personnel Management System: Suitability and Fitness Adjudication For Civilian Employees* (Aug. 24, 2012).

[28] DHS Management Instruction 121–01–007, *Department of Homeland Security Personnel Suitability and Security Program* (June 2009).

[29] GAO–12–800.

[30] DOD 5200.2–R, *Department of Defense Personnel Security Program* (January 1987, reissued incorporating changes Feb. 23, 1996), as modified by Under Secretary of Defense Memorandum, *Implementation of the Position Designation Automated Tool* (May 10, 2011).

[31] U.S. Coast Guard, CG–121, *Civilian Hiring Guide for Supervisors and Managers,* ver. 2 (June 11, 2010).

tions even when there is no vacancy and, as appropriate, either revise or review them. In addition, according to officials in U.S. Immigration and Customs Enforcement, supervisors are supposed to review position descriptions annually during the performance review process to ensure that the duties and responsibilities on the position description are up-to-date and accurate. However, officials stated that U.S. Immigration and Customs Enforcement does not have policies or requirements in place to ensure any particular level of detail in that review.

During our 2012 review, DOD and DHS officials acknowledged that overdesignating a position can result in expenses for unnecessary investigations. When a position is overdesignated, additional resources are unnecessarily spent conducting the investigation and adjudication of a background investigation that exceeds agency requirements. Without a requirement to consistently review, revise, or validate existing security clearance position designations, we concluded that Executive branch agencies—such as DOD and DHS—may be hiring and budgeting for both initial and periodic security clearance investigations using position descriptions and security clearance requirements that do not reflect National security needs. Moreover, since reviews were not being done consistently, DOD, DHS, and other Executive branch agencies did not have reasonable assurance that they were keeping to a minimum the number of positions that require security clearances on the basis of a demonstrated and foreseeable need for access.

Therefore, we recommended in July 2012 that the DNI, in coordination with the Director of OPM and other Executive branch agencies as appropriate, issue guidance to require Executive branch agencies to periodically review and revise or validate the designation of all Federal civilian positions. In written comments on that report, the ODNI concurred with this recommendation and stated that as duties and responsibilities of Federal positions may be subject to change, it planned to work with OPM and other Executive branch agencies to ensure that position designation policies and procedures include a provision for periodic reviews. OPM stated in its written comments to our report that it would work with the DNI on guidance concerning periodic reviews of existing designations.

ODNI and OPM are currently in the process of finalizing revisions to the position designation Federal regulation. As part of our on-going processes to routinely monitor the status of agency actions to address our prior recommendations, we note that the proposed regulation would newly require agencies to conduct a one-time reassessment of position designations within 24 months of the final regulation's effective date, which is an important step towards ensuring that the current designations of National security positions are accurate. However, the National security environment and the duties and descriptions of positions may change over time, thus the importance of periodic review or validation. The proposed regulation, if finalized in its current form, would not require a periodic reassessment of positions' need for access to Classified information as we recommended. We believe this needs to be done and, as part of monitoring the status of our recommendation, we will continue to review the finalized Federal regulation and any related guidance that directs position designation to determine whether periodic review or validation is required.

Quality of OPM Investigative Reports Not Measured

As of August 2013, OPM had not yet implemented metrics to measure the completeness of its investigative reports—results from background investigations—although we have previously identified deficiencies in these reports. OPM supplies about 90 percent of all Federal clearance investigations, including those for DOD. For example, in May 2009 we reported that, with respect to DOD initial Top Secret clearances adjudicated in July 2008, documentation was incomplete for most OPM investigative reports. We independently estimated that 87 percent of about 3,500 investigative reports that DOD adjudicators used to make clearance decisions were missing at least one type of documentation required by Federal investigative standards.[32] The type of documentation most often missing from investigative reports was verification of all of the applicant's employment, followed by information from the required number of social references for the applicant and complete security forms. We also estimated that 12 percent of the 3,500 investigative reports did not contain a required personal subject interview. Officials within various Executive branch agencies have noted to us that the information gathered during the interview and investigative portion of the process is essential for making adjudicative decisions.

[32] Estimates in our May 2009 report were based on our review of a random sample of 100 OPM-provided investigative reports for initial Top Secret clearances granted in July 2008 by the U.S. Army, U.S. Navy, and U.S. Air Force central adjudication facilities and have margins of error, based on a 95 percent confidence interval, of +/− 10 percentage points or fewer.

At the time of our 2009 review, OPM did not measure the completeness of its investigative reports, which limited the agency's ability to explain the extent or the reasons why some reports were incomplete. As a result of the incompleteness of OPM's investigative reports on DOD personnel, we recommended in May 2009 that OPM measure the frequency with which its investigative reports meet Federal investigative standards, so that the Executive branch can identify the factors leading to incomplete reports and take corrective actions.[33] OPM did not agree or disagree with our recommendation.

In a subsequent February 2011 report, we noted that OMB, ODNI, DOD, and OPM leaders had provided Congressional members with metrics to assess the quality of the security clearance process, including investigative reports and other aspects of the process.[34] For example, the Rapid Assessment of Incomplete Security Evaluations was one tool the Executive branch agencies planned to use for measuring quality, or completeness, of OPM's background investigations.[35] However, according to an OPM official in June 2012, OPM chose not to use this tool. Instead, OPM stated that it opted to develop another tool. In following up on our 2009 recommendations, as of August 2013, OPM had not provided enough details on its tool for us to determine if the tool had met the intent of our 2009 recommendation, and included the attributes of successful performance measures identified in best practices, nor could we determine the extent to which the tool was being used.

OPM also assesses the quality of investigations based on voluntary reporting from customer agencies. Specifically, OPM tracks investigations that are: (1) Returned for rework from the requesting agency, (2) identified as deficient using a web-based customer satisfaction survey, or (3) identified as deficient through adjudicator calls to OPM's quality hotline. However, in our past work, we have noted that the number of investigations returned for rework is not by itself a valid indicator of the quality of investigative work because DOD adjudication officials told us that they have been reluctant to return incomplete investigations in anticipation of delays that would impact timeliness. Further, relying on agencies to voluntarily provide information on investigation quality may not reflect the quality of OPM's total investigation workload. We are beginning work to further review OPM's actions to improve the quality of investigations.

We have also reported that deficiencies in investigative reports affect the quality and timeliness of the adjudicative process. Specifically, in November 2010, we reported that agency officials who utilize OPM as their investigative service provider cited challenges related to deficient investigative reports as a factor that slows agencies' abilities to make adjudicative decisions. The quality and completeness of investigative reports directly affects adjudicator workloads, including whether additional steps are required before adjudications can be made, as well as agency costs. For example, some agency officials noted that OPM investigative reports do not include complete copies of associated police reports and criminal record checks. Several agency officials stated that in order to avoid further costs or delays that would result from working with OPM, they often choose to perform additional steps internally to obtain missing information. According to ODNI and OPM officials, OPM investigators provide a summary of police and criminal reports and assert that there is no policy requiring inclusion of copies of the original records. However, ODNI officials also stated that adjudicators may want or need entire records as critical elements may be left out of the investigator's summary. For example, according to Defense Office of Hearings and Appeals officials, in one case, an investigator's summary of a police report incorrectly identified the subject as a thief when the subject was actually the victim.

Some Steps Taken to Determine Completeness of Adjudicative Files

To address issues identified in our 2009 report regarding the quality of DOD adjudications, DOD has taken some intermittent steps to implement measures to determine the completeness of its adjudicative files. In 2009, we reported that some clearances were granted by DOD adjudicators even though some required data were

---

[33] GAO, *DOD Personnel Clearances: Comprehensive Timeliness Reporting, Complete Clearance Documentation, and Quality Measures Are Needed to Further Improve the Clearance Process,* GAO–09–400 (Washington, DC: May 19, 2009).

[34] GAO, *High-Risk Series: An Update,* GAO–11–278 (Washington, DC: Feb. 2011).

[35] The Rapid Assessment of Incomplete Security Evaluations tool was developed by DOD to track the quality of investigations conducted by OPM for DOD personnel security clearance investigations, measured as a percent of investigations completed that contained deficiencies.

missing from the OPM investigative reports used to make such determinations.[36] For example, we estimated that 22 percent of the adjudicative files for about 3,500 initial Top Secret clearances that were adjudicated favorably did not contain all the required documentation, even though DOD regulations require that adjudicators maintain a record of each favorable and unfavorable adjudication decision and document the rationale for granting clearance eligibility to applicants with security concerns revealed during the investigation.[37] Documentation most frequently missing from adjudicative files was the rationale for granting security clearances to applicants with security concerns related to foreign influence, financial considerations, and criminal conduct. At the time of our 2009 review, DOD did not measure the completeness of its adjudicative files, which limited the agency's ability to explain the extent or the reasons why some files are incomplete.

In 2009, we made two recommendations to improve the quality of adjudicative files. First, we recommended that DOD measure the frequency with which adjudicative files meet requirements, so that the Executive branch can identify the factors leading to incomplete files and include the results of such measurement in annual reports to Congress on clearances. In November 2009, DOD subsequently issued a memorandum that established a tool to measure the frequency with which adjudicative files meet the requirements of DOD regulation. Specifically, the DOD memorandum stated that it would use a tool called the Review of Adjudication Documentation Accuracy and Rationales, or RADAR, to gather specific information about adjudication processes at the adjudication facilities and assess the quality of adjudicative documentation. In following up on our 2009 recommendations, as of 2012, a DOD official stated that RADAR had been used in fiscal year 2010 to evaluate some adjudications, but was not used in fiscal year 2011 due to funding shortfalls. DOD stated that it restarted the use of RADAR in fiscal year 2012.

Second, we recommended that DOD issue guidance to clarify when adjudicators may use incomplete investigative reports as the basis for granting clearances. In response to our recommendation, DOD's November 2009 guidance that established RADAR also outlines the minimum documentation requirements adjudicators must adhere to when documenting personnel security clearance determinations for cases with potentially damaging information. In addition, DOD issued guidance in March 2010 that clarifies when adjudicators may use incomplete investigative reports as the basis for granting clearances. This guidance provides standards that can be used for the sufficient explanation of incomplete investigative reports.

Extent of Clearance Reciprocity Not Measured

Executive branch agencies have not yet developed and implemented metrics to track the reciprocity of personnel security clearances, which is an agency's acceptance of a background investigation or clearance determination completed by any authorized investigative or adjudicative agency, although some efforts have been made to develop quality metrics. Executive branch agency officials have stated that reciprocity is regularly granted, as it is an opportunity to save time as well as reduce costs and investigative workloads; however, we reported in 2010 that agencies do not consistently and comprehensively track the extent to which reciprocity is granted Government-wide.[38] ODNI guidance requires, except in limited circumstances, that all intelligence community elements "accept all in-scope [39] security clearance or access determinations." Additionally, OMB guidance [40] requires agencies to honor a clearance when: (1) The prior clearance was not granted on an interim or temporary basis; (2) the prior clearance investigation is current and in-scope; (3) there is no new adverse information already in the possession of the gaining agency; and (4)

---

[36] GAO, *DOD Personnel Clearances: Comprehensive Timeliness Reporting, Complete Clearance Documentation, and Quality Measures Are Needed to Further Improve the Clearance Process,* GAO–09–400 (Washington, DC: May 19, 2009).

[37] DOD Regulation 5200.2–R, *DOD Personnel Security Program* (Jan. 1987, incorporating changes Feb. 23, 1996).

[38] In addition to establishing objectives for timeliness, the Intelligence Reform and Terrorism Prevention Act of 2004 established requirements for reciprocity, which is an agency's acceptance of a background investigation or clearance determination completed by any authorized investigative or adjudicative Executive branch agency, subject to certain exceptions such as completing additional requirements like polygraph testing. Further, in October 2008, ODNI issued guidance on the reciprocity of personnel security clearances. ODNI, Intelligence Community Policy Guidance 704.4, *Reciprocity of Personnel Security Clearance and Access Determinations* (Oct. 2, 2008).

[39] Although there are broad Federal investigative guidelines, the details and depth of an investigation varies by agency depending upon its mission.

[40] Office of Management and Budget, *Memorandum for Deputies of Executive Departments and Agencies: Reciprocal Recognition of Existing Personnel Security Clearances* (Dec. 12, 2005); Office of Management and Budget, *Memorandum for Deputies of Executive Departments and Agencies: Reciprocal Recognition of Existing Personnel Security Clearances* (July 17, 2006).

there are no conditions, deviations, waivers, or unsatisfied additional requirements (such as polygraphs) if the individual is being considered for access to highly-sensitive programs.

While the Performance Accountability Council has identified reciprocity as a Government-wide strategic goal, we have found that agencies do not consistently and comprehensively track when reciprocity is granted, and lack a standard metric for tracking reciprocity.[41] Further, while OPM and the Performance Accountability Council have developed quality metrics for reciprocity, the metrics do not measure the extent to which reciprocity is being granted. For example, OPM created a metric in early 2009 to track reciprocity, but this metric only measures the number of investigations requested from OPM that are rejected based on the existence of a previous investigation and does not track the number of cases in which an existing security clearance was or was not successfully honored by the agency. Without comprehensive, standardized metrics to track reciprocity and consistent documentation of the findings, decision makers will not have a complete picture of the extent to which reciprocity is granted or the challenges that agencies face when attempting to honor previously granted security clearances.

In 2010, we reported that Executive branch officials routinely honor other agencies' security clearances, and personnel security clearance information is shared between OPM, DOD, and, to some extent, intelligence community databases.[42] However, we found that some agencies find it necessary to take additional steps to address limitations with available information on prior investigations, such as insufficient information in the databases or variances in the scope of investigations, before granting reciprocity. For instance, OPM has taken steps to ensure certain clearance data necessary for reciprocity are available to adjudicators, such as holding interagency meetings to determine new data fields to include in shared data. However, we also found that the shared information available to adjudicators contains summary-level detail that may not be complete. As a result, agencies may take steps to obtain additional information, which creates challenges to immediately granting reciprocity.

Further, in 2010 we reported that because there is no Government-wide standardized training and certification process for investigators and adjudicators, according to agency officials, a subject's prior clearance investigation and adjudication may not meet the standards of the inquiring agency. Although OPM has developed some training, security clearance investigators and adjudicators are not required to complete a certain type or number of classes. As a result, the extent to which investigators and adjudicators receive training varies by agency. Consequently, as we have previously reported, agencies are reluctant to be accountable for investigations and/or adjudications conducted by other agencies or organizations.[43] To achieve fuller reciprocity, clearance-granting agencies seek to have confidence in the quality of prior investigations and adjudications.

Consequently, we recommended in 2010 that the Deputy Director of Management, OMB, in the capacity as chair of the Performance Accountability Council, should develop comprehensive metrics to track reciprocity and then report the findings from the expanded tracking to Congress. Although OMB agreed with our recommendation, a 2011 ODNI report found that intelligence community agencies experienced difficulty reporting on reciprocity. The agencies are required to report on a quarterly basis the number of security clearance determinations granted based on a prior existing clearance as well as the number not granted when a clearance existed. The numbers of reciprocal determinations made and denied are categorized by the individual's originating and receiving organizational type: (1) Government-to-government, (2) government-to-contractor, (3) contractor-to-government, and (4) contractor-to-contractor. The report stated that data fields necessary to collect the information described above do not currently reside in any of the datasets available and the process was completed in an agency-specific, semi-manual method. Further, the Deputy Assistant Director for Special Security of the Office of the Director of National Intelligence noted in testimony in June 2012 that measuring reciprocity is difficult, and despite an abundance of anecdotes, real data is hard to come by. To address this problem, ODNI is developing a web-based form for individuals to submit their experience with reciprocity issues to the ODNI. According to ODNI, this will

---

[41] GAO, *Personnel Security Clearances: Progress Has Been Made to Improve Timeliness but Continued Oversight Is Needed to Sustain Momentum,* GAO–11–65 (Washington, DC: Nov. 19, 2010).

[42] GAO–11–65.

[43] GAO, *Personnel Clearances: Key Factors to Consider in Efforts to Reform Security Clearance Processes,* GAO–08–352T (Washington, DC: Feb. 27, 2008).

allow them to collect empirical data, perform systemic trend analysis, and assist agencies with achieving workable solutions.

Recent Efforts and Sustained Leadership Could Facilitate Progress in Assessing Quality

Several efforts are underway to review the security clearance process, and those efforts, combined with sustained leadership attention, could help facilitate progress in assessing and improving the quality of the security clearance process. After the September 16, 2013 shooting at the Washington Navy Yard, the President directed the Office of Management and Budget, in coordination with ODNI and OPM, to conduct a Government-wide review into the oversight, nature, and implementation of security and suitability standards for Federal employees and contractors. In addition, in September 2013, the Secretary of Defense directed an independent review to identify and recommend actions that address gaps or deficiencies in DOD programs, policies, and procedures regarding security at DOD installations and the granting and renewal of security clearances for DOD employees and contractor personnel. The primary objective of this review is to determine whether there are weaknesses in DOD programs, policies, or procedures regarding physical security at DOD installations and the security clearance and reinvestigation process that can be strengthened to prevent a similar tragedy.

As previously discussed, DOD and DHS account for the majority of security clearances within the Federal Government. We initially placed DOD's personnel security clearance program on our high-risk list in 2005 because of delays in completing clearances.[44] It remained on our list until 2011 because of on-going concerns about delays in processing clearances and problems with the quality of investigations and adjudications. In February 2011, we removed DOD's personnel security clearance program from our high-risk list largely because of the Department's demonstrated progress in expediting the amount of time processing clearances.[45] We also noted DOD's efforts to develop and implement tools to evaluate the quality of investigations and adjudications.

Even with the significant progress leading to removal of DOD's program from our high-risk list, the Comptroller General noted in June 2012 that sustained leadership would be necessary to continue to implement, monitor, and update outcome-focused performance measures.[46] The initial development of some tools and metrics to monitor and track quality not only for DOD but Government-wide were positive steps; however, full implementation of these tools and measures Government-wide have not yet been realized. While progress in DOD's personnel security clearance program resulted in the removal of this area from our high-risk list, significant Government-wide challenges remain in ensuring that personnel security clearance investigations and adjudications are high-quality. However, if the oversight and leadership that helped address the timeliness issues focuses now on the current problems associated with quality, we believe that progress in helping Executive branch agencies to assess the quality of the security clearance process could be made.

In conclusion, to avoid the risk of damaging, unauthorized disclosures of Classified information, oversight of the reform efforts to measure and improve the quality of the security clearance process are imperative next steps. The progress that was made with respect to expediting the amount of time processing clearances would not have been possible without committed and sustained Congressional oversight and the leadership of the Performance Accountability Council. Further actions are needed now to fully develop and implement metrics to oversee quality at every step in the process. We will continue to monitor the outcome of the agency actions discussed above to address our outstanding recommendations.

Chairman King, Ranking Member Higgins, and Members of the subcommittee, this concludes my prepared statement. I would be pleased to answer any questions that you or other Members of the subcommittee may have at this time.

Mr. KING. Thank you, Ms. Farrell.

Let me thank all the witnesses for their testimony and their level of cooperation. I appreciate it very much.

You may have covered this in some of your testimonies, but let me just start. There are several cases I am aware of where a person receives a security clearance while they are at one agency and

[44] GAO, *High-Risk Series: An Update,* GAO–05–207 (Washington, DC: Jan. 1, 2005).
[45] GAO, *High-Risk Series: An Update,* GAO–11–278 (Washington, DC: Feb. 2011).
[46] GAO, *Personnel Security Clearances: Continuing Leadership and Attention Can Enhance Momentum Gained from Reform Effort,* GAO–12–815T (Washington, DC: June 21, 2012).

then they transfer to another agency. In the mean time, the first agency is advised of a problem that has developed and that was not passed on to the second agency. Then the individual may leave the second agency and go to the private sector but they still maintain their clearance.

In other words, how much cooperation is there between one Federal agency and another? If you learned something about an employee that was in that particular agency or department who had a clearance and they moved on to another one. In other words, does it follow the clearance or does it, you know, just stay with the departments? Am I making it clear what I am saying?

I don't want to go into the specifics of the case, but there is at least one individual who was with a particular agency, got his clearance, moved onto another one. After he went to the second agency the first agency was advised of problems that may have prevented him from getting a clearance in the first place, but those problems were never passed on to the second agency. Then he went to the private sector after that, again, keeping the same Top Secret clearance.

So I am going to just go across the board and see if any of you have any—yes?

Ms. FARRELL. I believe you are talking about reciprocity, which is honoring the investigation conducted when one transfers from one agency to another, and that is an issue that we have raised. The extent to which reciprocity is met is unknown because there are no metrics that tell us how many people are accepted or how many people are stopped.

Reciprocity is important because by statute, the Intelligence Reform Terrorism Prevention Act of 2004 stated that agencies should honor one another's investigations and adjudications to the extent possible. There have been other guidance from the DNI, from OMB, making it clear when there are exceptions to such granting of those clearances, but we do not know how well it works.

There are anecdotes, as you have anecdotes. There are stories of someone who has a clearance and it is not accepted and they have three clearances done in a year, especially with contractors. But the extent to which these clearances are accepted, are not accepted is really unknown.

Mr. KING. Well, let's say a person has the clearance, moves onto another agency with that clearance, and the first agency then is advised that something has come up after the clearance was given. I assume that agency is supposed to pass that on to the second, right?

Ms. FARRELL. That is something that is specified in guidance, that when the attention comes of new information, if it is disclosed to the gaining agency then that would be a reason not to honor such a clearance. But how often—again, how often information is passed along is unknown.

Mr. KING. Anybody else want to comment on this?

Mr. Prioletti.

Mr. PRIOLETTI. I just wanted to add to what Brenda said that there is an on-going research right now going on through the DNI's office where we are meeting with the 16 members of the I.C. and gaining information on their reciprocity—how was it enacted? How

did they make the guidelines? How did they determine which people are going to be crossover and which ones are not—to try to get a better feel and to gain some of the very metrics that Brenda is referring to there, sir.

Mr. KING. Mr. Marshall or Mr. Miller.

Mr. Marshall.

Mr. MARSHALL. Yes, sir. Thank you.

In DHS we obviously accept reciprocity on its face by Executive Order. When we can point to an existing investigation, an in-scope investigation, we will honor it on its face.

One of the gaps that we see within DHS is that we are not allowed to do any additional checks unless we have derogatory information to the contrary. So it would be critical in the situation that you describe that that first agency pass that information along to the second agency in order for us to take an action with respect to the clearance.

Mr. KING. Mr. Miller.

Mr. MILLER. Chairman King, your question is spot-on, the issue of where the gaps exist once an investigation has closed and then there is a reciprocity decision. For instance, somebody with a Top Secret clearance can go 5 years without a reinvestigation; however, that doesn't preclude potential new criminal history record information, financial problems, or other things developing. However, if that information is not reported in some way or captured, that remains a gap.

So, as Greg mentioned, within DHS you can only go—make a reciprocity decision based on the last investigation and not knowing what may have developed in the mean time. So that 5-year window becomes a gap, and potentially information could be developed that may result in, actually, a different adjudication being made if you were aware of it.

Mr. KING. Ms. Farrell and Mr. Prioletti I think both mentioned guidance. Is that a directive? Is that required or is it just suggested?

Ms. FARRELL. The statute that I mentioned, IRTPA 2004, did require that reciprocity be honored. There is guidance in OMB guidelines that has certain exceptions that can be extended, such as the clearance background investigation is not up-to-date or additional information has come to light regarding the individual.

There is also DNI guidance that specifies things such as the particular position requires a different type of scope of background investigation. So there are exceptions for the agencies to consider when they are—before they grant such a reciprocity.

Mr. KING. Mr. Higgins.

Mr. HIGGINS. Thank you, Mr. Chairman.

Just, you know, for the whole panel, you know, according to the Office of Personnel Management, almost 5 million Federal workers and contractors are eligible to hold a security clearance, and at the Department of Homeland Security approximately 125,000 employees hold clearances. Given the fact that this Aaron Alexis, a lone gunman, took up arms against fellow employees at the Navy Yard, Alexis was a contractor and he had security clearance but he also had a history of arrests—plural. More than one. He had a history of gun infractions—plural. More than one.

In published reports there were other incidences calling into question, you know, his mental health. So I suppose my question is, how did he get a security clearance in the first place?

Go ahead.

Mr. MARSHALL. Yes, sir. I will start. Thank you.

With respect to Mr. Alexis, and based on what I understand, and granted, I don't have any first-hand knowledge; I wasn't particularly briefed on it, but based on what I know from media accounts and some anecdotal conversations I have had with some other folks who had some information, it appears that he had a clearance with the Navy and that when he left the Navy and went to the contracting firm the clearance was accepted on reciprocity, because they had an investigation that they can point to.

In that context let me explain how we do it in Department of Homeland Security. The Department of Homeland Security does all the fitness adjudications for contractors in the Department. The actual adjudication of the investigations, however, reside in the Department of Defense.

So while we have the ability to do the fitness determination, the adjudication is done there. So that is how it works in Homeland Security.

Mr. HIGGINS. Anybody else?

Go ahead.

Mr. MILLER. Yes. I would like to make a comment just as background on Alexis. The investigation that was completed for him was completed in 2007. In fact, he was adjudicated in 2008 by the Department. I am sorry DOD is not here to respond.

Some of the criminal history information you refer to occurred after that 2007 completed investigation, and that is the gap. In fact, Mr. Alexis was not due for reinvestigation until 10 years after the completion of the case in 2007, so that would have been 2017 before there would have been any review of what may have developed once he had been cleared.

Now, Mr. Prioletti has talked about the continuous evaluation, the critical need to be able to fill the gap, and that is one of the solutions being proposed not only by the DNI but by the community is to be able to capture any new criminal history record information that might come about.

Mr. HIGGINS. Go ahead.

Mr. MILLER. I just wanted to say, one of the initiatives on-going right now—if the FBI were here they would talk about a program called Rap Back. Rap Back is going to provide a capability within the Department—within the Executive branch and across Federal Government—that if there has been a fingerprint check done on an individual for a background investigation and in the future should new criminal history information become developed, the FBI will be notifying, actually the OPM to notify the Federal agency that you have new results. So that could occur a week after the close of an investigation, a year, 2 years.

So with Alexis, that criminal history record that was developed in Texas of that incident with a weapon would have been notified through the FBI back to the Department to let them know there is an individual that has new criminal history record information.

So that is part of the C.E. solution in the future and we are looking to find other ways to provide information to fill those gaps.

Mr. HIGGINS. Yes. I would say, look, this is not an exact science, but it is a pretty sensitive issue when you process people for security clearance. That should be a pretty tight criteria. My sense is that while it is good that they are looking at ways to tighten that up, I am shocked that, you know, somebody that has a security clearance that any arrest incident prospectively would not trigger something to the respective authorities to remove or at least suspend that clearance so that, you know, the issue could be adjudicated.

It just seems to me, again, that when you are issuing so many of these or making eligible so many people for security clearances that, forget about reinvestigations, there should be a better process in place to ensure that instantaneously, should something occur that would, you know, result in somebody being denied clearance, that information should be made available to determine whether or not that clearance can be continued and/or at least suspended until such time as there is a clarity about, you know, what had occurred here.

That is all I have, Mr. Chairman.

Mr. KING. Gentleman from Massachusetts, Mr. Keating.

Mr. KEATING. Thank you, Mr. Chairman.

I guess the best person that I would ask is Mr. Prioletti this question: What essential information do background checks neglect to include in the existing process, which largely depends on a huge component of self-reporting by persons applying for it? Are there things that you can highlight that might be more helpful or areas that are, you know, not included but that—could you share with us the reason for that?

Mr. PRIOLETTI. Sir, the information that is gained during the investigative process is based upon the adjudicative standards that we mentioned earlier that came out in 2005 from the White House, and they cover 13 generic areas ranging from finances to foreign national contacts and everything in between. We do our adjudicative—excuse me—we do the investigative process based upon information that will gain us insight into those areas so that we can make an informed adjudicative decision.

I don't believe it is the areas that we are missing as much as the comprehensiveness of gaining that information. I believe Mr. Marshall and Mr. Miller both have commented on the ability to get that information, and there are some areas where we could improve on.

One of the biggest areas, I believe, where we need to improve on are some of our National and local agency checks—the ability to get criminal responses on individuals. Based on a conversation earlier, there are somewhere in the area of 17,000-plus local law enforcement and Federal law enforcement agencies that have information on individuals. They are not all electronically connected to an ability to get that information and that would certainly help improve our ability.

Mr. KEATING. Yes. I was thinking, I was a prosecutor before I was here in office, and sometimes we would have cases and they would reflect on a person's status in State government and there

really wasn't that linkage there either electronically, as well. We would affirmatively do that but it is not a precise science because there was not a requirement.

So I think we have an idea that everything can be done electronically and technologically today, but it just doesn't work that well. Particularly if you are dealing with State crimes or State activities, the process of that often is so slow just to get into the State, let alone to try and link it to the Federal. There would be quite serious delays.

Here is one more question I think I have a sense of, but in the last stage of appeals on security clearance issues it leaves DHS and goes to the Secret Service. Is that correct?

Could you explain, anyone, why that decision was made there instead of keeping it in a panel within DHS or—and why Secret Service would be that last? How cumbersome is that, given the staffing there?

Mr. MARSHALL. Yes, sir. I can answer that.

It varies. There are three stages to the security appeal process. There is the personnel security chief; and then it goes to the second-level deciding authority, and in my organization I am that person; and then if it is not resolved at the second level it goes to the, what I call the three-judge panel at the Secret Service.

The reason it is in the Secret Service is because that is where it was when DHS was formed. Obviously we are a legacy agency comprised of many organizations and they already had that function within the Secret Service, so it just made sense at the time to, because it was already a functioning body and already had their policies and procedures in place, just to leave it there.

I know there has been some question since on whether or not that is appropriate and whether they should be rotated in and out and made up of members of other agencies who may sit on that, and that is still being discussed. But that is how it evolved to the three-judge panel at the Secret Service.

Mr. KEATING. Thank you. It is amazing the legacy issues with Homeland Security.

I will yield back, Mr. Chairman.

Mr. KING. Thank you, Mr. Keating.

As a follow-up to what Mr. Keating was asking you about, you know, the electronic records, assuming that everything could be done electronically, how cooperative do you find State and local governments in giving you the information if you ask for it?

Mr. PRIOLETTI. Well, sir, quite honestly, I believe that I would have to defer to Mr. Miller on that one, as he directly deals with those organizations.

Mr. KING. Mr. Miller.

Mr. MILLER. Chairman King, it varies candidly with over 17,000-plus law enforcement entities out there. It varies from from location to location, State to State. In fact, there are different statutes.

There is a 5 U.S. Code 9101 actually requires agencies to share criminal history record information with the Federal Government. However, 9101 doesn't go far enough to actually outline specifically the information, so the preponderance of the information being shared today actually just addressed the charge and the disposi-

tion, not necessarily the facts surrounding and the circumstances of the arrest.

So again, it varies from State to State. In fact, not to go over old history, but we actually had to go to court in one location to actually force the local government to share criminal history record information with the Federal Government, and we were successful.

Mr. KING. Anybody else wish to comment on that?

Ms. Farrell.

Ms. FARRELL. I think Mr. Miller can speak to the actual information sharing, but we are aware when we did our work in 2010 and at other times, agency adjudicators—and this is from a number of agencies—12, 14—would comment to us that the summary information in the background investigations did not give the details regarding police or criminal records that was available, that that information had been summarized by the OPM investigator to a point that it raised a lot of questions for the adjudicators.

So this goes back to the issue of quality with what is required. Are we getting the best quality from what is required before we start expanding it and adding additional requirements?

Mr. KING. On a separate issue on this, without starting any interdepartmental feuds or anything else, but are there any agencies within the intelligence community or within the Federal Government who are not willing to cooperate as far as giving personnel records of their former employees—like, for instance, going from one intelligence component to another or to somebody else in the Federal Government? Is it your experience that anyone is more reluctant than others to fully cooperate as far as giving personnel information?

Mr. PRIOLETTI. Sir, to the best of my knowledge they all are cooperating at various levels, depending upon the information to be shared. But I have not encountered any specific incidences where one I.C. organization would not share with another.

Mr. KING. Yes.

Ms. FARRELL. I can add to that.

During the course of our work with the I.C. we are aware that they use the Scattered Castles database, and nothing was brought to our attention within the I.C. community having access to that. I think the issues evolve more when you are crossing from the non-I.C. world into the I.C. and what is shared and what is not shared or back from the I.C. to a non-I.C.

Because there are different databases. OPM has a database; DOD has a database; the I.C. has a database. That sometimes can present issues with reciprocity and some of the issues that we have discussed.

Mr. KING. Apart from the need for improvement on the actual investigative reports, do you think any improvements are needed on the adjudicative end as to what standards should be used, what thresholds there should be?

Ms. FARRELL. Our work is concentrated at DOD on the adjudication portion and we have found issues with the adjudication when we did our work back in 2006 and 2008. We found similar issues with the adjudication files as we did with OPM's investigative files.

We made recommendations regarding guidance that was needed to document when perhaps an applicant was not available for an

interview, to document what attempts had been made to do so and why that applicant was not available. DOD developed such guidance. DOD also took steps to measure the frequency for which their adjudication reports met the Federal adjudicative guidelines and other actions to monitor and oversee that adjudication process.

I cannot speak to the Homeland Security adjudication process.

Mr. KING. Mr. Marshall.

Mr. MARSHALL. Yes, sir. Thank you.

One of the issues that is troubling to me and a gap that I recognize—and it is probably something that we are all going to be working on in this 120-day review that the President ordered—is a gap I see in suitability adjudication. Mental health is not one of the adjudicative criteria within suitability or fitness and I really think that needs to be addressed.

It is addressed in the revised guidelines for National security clearances, and Mr. Prioletti mentioned that. But we—it doesn't appear in 5 CFR 731 for suitability, and the suitability like criteria we apply to contractors, and I really think it needs to be.

Mr. KING. You know, considering the large number—I think Mr. Higgins and I said 4.9 million, 5 million people with these clearances, and obviously a lot of the investigative work is done by private contractors. We have seen that. Can any of you comment on whether there is a different level of quality—better or worse—between the Government carrying out the investigation or private contractors? Are there other standards for the private contractors? Are they uniform standards?

Mr. MILLER. I can speak to that.

Mr. KING. Yes, sir.

Mr. MILLER. I managed the contract at Federal workforce. First off, there is no difference in the way we clear contract workforce versus Federal workforce relative to background investigations. Second is the quality of investigations are the same. They have got to investigate to the same standards and they have got to meet the same quality standards, both Federal and contract employees.

Mr. KING. Anybody else wish to comment?

Yes, Ms. Farrell.

Ms. FARRELL. Our work has found that the—it is unknown, really, the extent to the quality of investigations. We have data that does show incompleteness when you look at OPM's investigations compared to the Federal Investigative Guidelines.

Is there a difference between the oversight when a contractor conducts the investigation and a Federal employee? What we are saying is there are not measures or steps put in place to make sure that that background investigation does meet Federal standards regardless of whether it is conducted by a contractor or a Federal employee.

Mr. KING. What standards are there in selecting a contractor to carry out the investigation? Are they uniform?

Mr. MILLER. Yes. The standards are uniform for contractors that perform background investigative work. They all have to be trained to the same level, and obviously through the contract process, when they come in to actually compete for the work they all have to meet the same standards when they are selected to do contract work for the Government.

Mr. KING. Mr. Higgins.

Mr. HIGGINS. I have no further questions. Does the staff have any suggested questions?

Mr. KING. Okay. I want to thank you for your testimony today. Sorry for the delay at the beginning. We got called over for votes. It seems it never fails. There are never any votes until we have witnesses here to testify at a hearing, so I regret that.

I want to thank you for your patience. I want to thank you for your testimony.

Again, I think all of us appreciate—I am sure I can speak for Mr. Higgins on this—the level of cooperation and the fact that all of you appreciate the importance and the significance of this and the cooperation you have given to the staff. So I thank you for your testimony.

Brian, do you have anything?

Mr. HIGGINS. Nope.

Mr. KING. Okay. With that, without objection, the subcommittee stands adjourned. Thank you very much.

[Whereupon, at 3:28 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM HONORABLE PETER T. KING FOR MERTON W. MILLER

Question 1. As I understand it, the adjudicating agency only gets a summary of the information that has been gathered during the background investigation. What entity does the actual packaging of the summary that is in turn submitted to the adjudicating agency?

Answer. Response was not received at the time of publication.

Question 2. In terms of the background investigators themselves, whether they are a Government employee or a contracted employee, what types of standards are they held to in order to complete their jobs? In other words, have these individuals been subjected to the scrutiny of background investigations?

Answer. Response was not received at the time of publication.

Question 3. Are the forms that applying individuals use to fill out during the background investigation phase considered antiquated? If so, what types of updates to these forms may be necessary to address the needs of background investigators to adequately gather pertinent and meaningful information?

Answer. Response was not received at the time of publication.

Question 4. Is there a current backlog in background investigations for security clearances? If so, how numerous is the backlog and what effect does the sequestration have on this process?

Answer. Response was not received at the time of publication.

Question 5. How much of OPM's work is contracted out to private companies to complete background checks? How often are these contractors reviewed by OPM, in terms of quality control of their product?

Answer. Response was not received at the time of publication.

Question 6. What difficulties are created by the substantial dependence of OPM on contractors to execute background checks and what are the benefits of that dependence?

Answer. Response was not received at the time of publication.

QUESTIONS FROM HONORABLE PETER T. KING FOR GREGORY MARSHALL

Question 1. How successful has DHS been at producing quality results in security clearance background checks and by what measure do use to make this assessment?

Answer. DHS has a successful and robust suitability and security program. To measure the quality of the background investigations, DHS relies on its trained adjudicative staff to review the investigative product for completeness and to render the adjudicative determination. DHS has incorporated levels of review in the adjudicative process whereas senior-level adjudicators, including managers, review the work of the lesser-experienced adjudicators to ensure quality and adherence to policy and guidelines.

In addition, DHS, as an authorized investigative agency, adheres in the conduct of its security investigations to the Federal Investigative Standards. DHS is also an active participant in an Office of Personnel Management (OPM) and Office of the Director for National Intelligence Quality Assessment Working Group which was established to create a standard by which all investigating entities would assess quality investigations and develop a tool to make the assessment.

Question 2. Where does DHS stand with regard to security clearance reciprocity, i.e. are you completely accepting security clearances at all levels for individuals coming from other Federal agencies? If not, what is your reasoning for not yielding to reciprocity?

Answer. DHS accepts security clearance reciprocity at all levels for individuals coming from other Federal agencies. However, based on the responsibilities of the positions, additional higher levels of investigation may be required, consistent with the OMB memoranda of December 12, 2005, July 17, 2006, and November 14, 2007,

and the Intelligence Community Policy Guidance Number 704.4. Also, some law enforcement organizations utilize the polygraph for employment screening and personnel investigations for positions requiring a polygraph examination prior to entry into the position.

Security reciprocity should not be confused with suitability or fitness for appointment, or, alternatively, the ability to meet a qualification standard in the hiring process. There are additional considerations that may need to be addressed in order for an applicant to gain employment. The following is a list of considerations that the Department must address:

- Due to their mission, components that enforce drug laws—e.g., the U.S. Immigration and Customs Enforcement (ICE) and the U.S. Customs and Border Protection (CBP)—must adhere to more stringent guidelines on frequency and recency of illegal drug use than other components.
- Components that have weapon-carrying positions (e.g., ICE, CBP, TSA, USSS, and FLETC) must adhere to the "Lautenberg Amendment", which provides that it is unlawful "for any person to sell or otherwise dispose of any firearm or ammunition to any person knowing or having reasonable cause to believe that such person has been convicted in any court of a misdemeanor crime of domestic violence." 18 U.S.C. 992(d)(9). If an applicant were to be prohibited from possessing a firearm or ammunition, under the Lautenberg Amendment, that applicant would therefore be ineligible for the weapon-carrying position.
- TSA is required to consider 28 statutory criminal types of "Disqualifying offenses that, if committed, would disqualify an individual from employment with the agency." See listed in 49 U.S.C. § 44936(b)(1)(B), eligible for employment with TSA.
- OPM's regulations on suitability reciprocity contain exceptions when, for example, the investigative record shows conduct that is incompatible with the core duties of the position. See 5 C.F.R. 731.202(d).

While the Department adheres to security reciprocity, it must also comply with other laws affecting employment and suitability related to the specific requirements of the position.

Question 3. It is the committee's understanding that the last stage of appeals for suspensions and revocations of security clearances are heard before a panel at the U.S. Secret Service for all security clearance-holders at DHS headquarters and its components. Why is this the case and why has this authority not been given to a panel comprised of DHS headquarter officials?

Answer. In accordance with the requirement under Executive Order 12968 that Federal agencies provide applicants and employees denied clearances the opportunity to appeal the decision, DHS leveraged the U.S. Secret Service as the Department's Security Appeals Board. The U.S. Secret Service has a robust and longstanding functioning Appeals Board. As the Board performed the functions appropriately and in accordance with all Federal guidelines, there was not an immediate need to change the composition of the Board. We will revisit the composition of the Board and determine potential adjustments to the practice.

Question 4. Do you think that existing policies and processes related to reinvestigations of individuals who hold security clearances meet the "appropriate level of rigor" mentioned in your earlier testimony?

Answer. DHS believes there are gaps in the process that create vulnerabilities to the Department. For one, the current interval for periodic reinvestigations (5, 10, 15 years depending on the level of clearance) is insufficient, though this has been addressed in the 2012 Federal Investigative Standards approved and signed in December 2012, and will be implemented fully by 2017. Also, based on the level of reinvestigation and records collected, security offices are not always provided relevant information on individuals of incidents occurring in their employment. Another large gap is the lack of participation and timeliness of local law enforcement jurisdictions reporting criminal activity into the State and National repositories on which security investigators rely. We note that Congress expressed awareness of this issue when it recently passed the National Defense Authorization Act, 2014, section 907 of which establishes a task force on records access composed of both Federal and State and local law enforcement officials to make recommendations for improving the degree of cooperation and records sharing. This issue is also being examined as part of the "120-day review" of security and suitability policies and procedures now underway that the President has directed.

Question 5. In your view, are reinvestigations currently conducted with the appropriate frequency (currently, 15, 10, and 5 years for Confidential-, Secret-, and Top Secret-level clearances, respectively), or should reinvestigations occur more frequently?

Answer. The current policies for reinvestigations are not stringent enough due to the current time frames. Those policies had been in place since the late 1990s and were in need of reform. In December 2012 the Office of the Director of National Intelligence and the Office of Personnel Management jointly issued new Federal investigative standards establishing a 5-year reinvestigation cycle even for Confidential and Secret clearances. The new standards are subject to an implementation plan. Further, ODNI has been given authority under Executive Order 13467 to develop the Continuous Evaluation (CE) program to evaluate National security risks involving cleared personnel between periodic reinvestigations, and the December 2012 Federal investigative standards require CE for Top Secret-cleared personnel. Likewise OPM is piloting the "Rap Back" program by which the FBI furnishes real-time arrest information on current employees. Full implementation of the 2012 revised standards is expected by 2017. DHS is an active participant in Federal personnel security community discussions and activities to address the need for a more frequent/current review of individuals who hold security clearances, including continuous evaluation.

Question 6. As you noted in your earlier testimony, background investigations only examine past behavior and may be an inadequate predictor of future behavior. One potential element of the Insider Threat Program is the use of analytics to identify and even predict potential breaches of information systems based on an individual's pattern of system access. Have you or other members of DHS's Chief Security Officer Council explored the possibility of using similar analytics or behavioral modeling techniques as part of the security clearance adjudication process?

Answer. As personnel security is an integral part of the Insider Threat Program, DHS recognizes the need to use analytics in its personnel security process. Under the concept of Continuous Evaluation and Continuous Monitoring, personnel security will be more proactive in making individual assessments than the traditional reactive approach. The Continuous Evaluation will be a tool to evaluate patterns of behavior. DHS is awaiting guidance from the Office of the Director for National Intelligence (ODNI), as the Security Executive Agent, to release policy on the execution of the Continuous Evaluation model. ODNI, through the National Insider Threat Task Force, convenes various forums to assist departments and agencies as they work to establish their insider threat programs under Executive Order 13587 and the President's National insider threat policy and minimum standards. In the interim, the Department has held discussions with private firms that look at behavioral modeling through continuous evaluation to explore automated options and their availability/compatibility with current systems. DHS participated in a Department of Defense hosted Behavioral Analysis/Insider Threat Tabletop Exercise (TTX) to review best practices, including programs outside the U.S. Government, to determine whether elements of those programs could be adopted to detect persons who may pose a threat; as well as review leading edge tools and technologies that augment existing security processes and capabilities. A range of predictive analytics and risk assessment tools were discussed. For example, the Identity Management Enterprise Services Architecture (IMESA) was identified as a potential capability to continuously monitor personnel that have authorized access to DoD installations and assets against authoritative data sources. IMESA will enable the sharing of identity and physical access control information complementing on-going continuous evaluation concept demonstration efforts.

QUESTIONS FROM HONORABLE PETER T. KING FOR BRIAN A. PRIOLETTI

Question 1. Under Section 6 of Executive Order 13587, the Interagency Insider Threat Task Force is to conduct "independent assessments" of agencies' insider threat programs. What is the status of the task force's effort to develop procedures for these assessments? How many assessments has the task force conducted?

Answer. Response was not received at the time of publication.

Question 2. Could you summarize the results of those assessments? In your response, could you discuss the following: How many agencies have acceptable programs? How many do not? For agencies that do not have acceptable insider threat programs, what are the deficiencies?

Answer. Response was not received at the time of publication.

Question 3. What differences, if any, exist regarding the threat to National security posed by contractor employees with access to Classified material and Federal employees with access to Classified material?

Answer. Response was not received at the time of publication.

Question 4. Is there a need to expand the areas of risk factors when adjudicating security clearance applicants to address the issues that we have seen in recent events?

Answer. Response was not received at the time of publication.

Question 5. In your testimony, you mentioned the need for Continuous Evaluation for those persons that hold security clearances. Would this process be regulated by time frames or will they be triggered by information discovered about a security clearance holder by the agency security office?

Answer. Response was not received at the time of publication.

Question 6. What essential information do background checks neglect to include in the existing process, which depends largely on self-reporting by the persons applying for a security clearance?

Answer. Response was not received at the time of publication.

QUESTIONS FROM HONORABLE PETER T. KING FOR BRENDA S. FARRELL

Question 1. You mentioned in your testimony that agencies are "revisiting the Federal investigative standards." Can you explain the investigative standards that are currently being revisited by Federal agencies? Is the proposed OPM/ODNI rule one of the agency actions referred to in your statement?

Answer. Response was not received at the time of publication.

Question 2. What possible impact, if any, could the proposed OPM/ODNI rule have on the overall security clearance background investigation process?

Answer. Response was not received at the time of publication.

Question 3. What elements of the security clearance process do you find the most problematic with regards to conducting fair and thorough background investigations?

Answer. Response was not received at the time of publication.

Question 4. In your research, have you found that agencies are fully complying with the guidelines for reciprocity? If not, what are the reasons for non-compliance?

Answer. Response was not received at the time of publication.

Question 5. In your testimony, you mentioned that your study involved looking into the metrics needed to measure quality of the security clearance process. Are there any agencies in particular that stood out as doing at least a fairly exceptional job with measuring its process quality and if so, why is this the case with that particular agency and not others?

Answer. Response was not received at the time of publication.