DC NAVY YARD SHOOTING: FIXING THE SECURITY CLEARANCE PROCESS

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

FEBRUARY 11, 2014

Serial No. 113–105

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

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

U.S. GOVERNMENT PRINTING OFFICE

87–892 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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

DARRELL E. ISSA, California, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
PATRICK T. MCHENRY, North Carolina
JIM JORDAN, Ohio
JASON CHAFFETZ, Utah
TIM WALBERG, Michigan
JAMES LANKFORD, Oklahoma
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
PATRICK MEEHAN, Pennsylvania
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
DOC HASTINGS, Washington
CYNTHIA M. LUMMIS, Wyoming
ROB WOODALL, Georgia
THOMAS MASSIE, Kentucky
DOUG COLLINS, Georgia
MARK MEADOWS, North Carolina
KERRY L. BENTIVOLIO, Michigan
RON DESANTIS, Florida

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
JACKIE SPEIER, California
MATTHEW A. CARTWRIGHT, Pennsylvania
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
DANNY K. DAVIS, Illinois
PETER WELCH, Vermont
TONY CARDENAS, California
STEVEN A. HORSFORD, Nevada
MICHELLE LUJAN GRISHAM, New Mexico
Vacancy

LAWRENCE J. BRADY, *Staff Director*
JOHN D. CUADERES, *Deputy Staff Director*
STEPHEN CASTOR, *General Counsel*
LINDA A. GOOD, *Chief Clerk*
DAVID RAPALLO, *Minority Staff Director*

CONTENTS

DC NAVY YARD SHOOTING: FIXING THE SECURITY CLEARANCE PROCESS

Tuesday, February 11, 2014,

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

The committee met, pursuant to call, at 9:35 a.m., in Room 2154, Rayburn House Office Building, Hon. Darrell E. Issa [chairman of the committee] presiding.

Present: Representatives Issa, Mica, Turner, Walberg, Lankford, Amash, Meehan, DesJarlais, Farenthold, Woodall, Collins, Bentivolio, DeSantis, Cummings, Maloney, Norton, Tierney, Lynch, Connolly, Speier, Duckworth, Kelly, and Lujan Grisham.

Staff Present: Jen Barblan, Majority Counsel; Molly Boyl, Majority Deputy General Counsel and Parliamentarian; Lawrence J. Brady, Majority Staff Director; Ashley H. Callen, Majority Deputy Chief counsel for Investigations; Caitlin Carroll, Majority Press Secretary; Sharon Casey, Majority Senior Assistant Clerk; John Cuaderes, Majority Deputy Staff Director; Carlton Davis, Majority Senior Counsel; Adam P. Fromm, Majority Director of Member Services and Committee Operations; Linda Good, Majority Chief Clerk; Frederick Hill, Majority Deputy Staff Director for Communications and Strategy; Mark D. Marin, Majority Deputy Staff Director for Oversight; Ashok M. Pinto, Majority Chief Counsel, Investigations; Jessica Seale, Majority Digital Director; Sarah Vance, Majority Assistant Clerk; Peter Warren, Majority Legislative Policy Director; Rebecca Watkins, Majority Communications Director; Jaron Bourke, Minority Director of Administration; Aryele Bradford, Minority Press Secretary; Lena Chang, Minority Counsel; Jennifer Hoffman, Minority Communications Director; Peter Kenny, Minority Counsel; Elisa LaNier, Minority Director of Operations; Juan McCullum, Minority Clerk; and Dave Rapallo, Minority Staff Director.

Chairman ISSA. The committee will come to order.

Today's hearing is entitled DC Navy Yard Shooting: Fixing the Security Clearance Process. I will now recognize myself.

The Oversight Committee exists to secure two fundamental principles: first, Americans have a right to know that the money Washington takes from them is well spent, and, second, Americans deserve an efficient, effective Government that works for them. Our duty on the Oversight and Government Reform Committee is to protect these rights. Our solemn responsibility is to hold Government accountable to taxpayers because taxpayers have a right to know what they get from their Government. It is our job to work

tirelessly in partnership with citizen watchdogs to deliver the facts to the American people and bring genuine reform to the Federal bureaucracy. This is our mission.

I now recognize myself.

Michael Arnold, Kathy Gaarde, John Roger Johnson, Arthur Daniels, Richard Michael Riggell, Martin Bodrog, Vishnu Pandit, Kenneth Bernard Proctor, Mary Francis Knight, Gerald Read, Sylvia Frasier, Frank Kohler. Typically, these 12 public servants who lost their life on September 16, 2013, when a deranged gunman entered Building 197, the headquarters of the Navy Sea Systems Command at the Washington Navy Yard, would not be read in the Halls of Congress. But I think today, as we look into why we are here, we are not here to embarrass the companies, we are not here to embarrass the Office of Personnel Management, but we are here to recognize that a horrendous act of violence occurred, one in which we believe, in all likelihood, best practices in employment could have prevented this.

But more than that, this was a deranged individual who had a security clearance. So more than simply the question of whether or not he should have been employed, or should have been in therapy, or should have been incarcerated, we are asking the question of when we go beyond simply an employment look, but in fact a secured employment look, how could we miss someone who had repeatedly used a weapon in a deranged way: flattening tires with a gun, shooting holes in the roof of his own house simply because someone was making too much noise? These are not the acts that an employer would accept and allow somebody to have access to a building and access to a building in which they committed unspeakable acts.

This hearing will not deal entirely with management practices in hiring of Federal employees; it will primarily deal with the 4.9 million Americans holding security clearances, because the standard for security clearances should be higher than those for employees. But as a former employer, I must tell you I am disappointed that the system is not in place to catch every person of this type of history, no matter whether they had a security clearance or not.

This committee has been conducting a bipartisan investigation into the facts and circumstances surrounding this incident. My partner, Mr. Cummings, and the entire committee staff on both sides, have in fact seen glaring mistakes in the existing Federal security clearance process as a whole. Over the course of our four-month investigation, these questions have come up: Why did the Federal Government grant security clearance to a man with a known violent criminal past, one he attempted to cover up? Why didn't the Federal Government revoke that clearance when his unstable mental condition raised red flags?

We, again, are not here to point fingers specifically at this, but, rather, those 12 names I mentioned are names that should not have died in vain without real change.

I want to thank the ranking member for being my partner in this. I want to make it very clear that this is not a problem created by this Administration; this is a problem of bureaucracy, long-standing, but no longer can we stand for it. We owe that much to the families of each of the victims.

With that, I now recognize Mr. Cummings for his opening statement.

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

There is no doubt that we need to conduct a thorough—and when I say thorough, I mean thorough—investigation to determine how Aaron Alexis was able to obtain and keep a security clearance given his troubling background. We owe this to the families of the 12 people he killed and the others he injured, as well as all Americans who rely on the background check system to protect our national security.

Mr. Chairman, I want to thank you and your staff for a bipartisan approach on this investigation. Our work has the potential, and I do say the potential, to stand as an important part of this committee's legacy if we follow through on these efforts.

Here is what we know so far: First, Alexis obtained a security clearance from the Navy in 2008, and his background investigation was conducted by U.S. Investigation Services, USIS. USIS is the single biggest contractor that performs background investigations for the Office of Personnel Management, completing more than the Government or any other contractor.

Four years before Alexis got his clearance, he was arrested in Seattle for shooting out the tires of someone's car. USIS did not obtain a copy of that 2004 report, and OPM did not require one because the City of Seattle refused to cooperate with similar requests in the past. Something wrong with that picture. Instead, USIS obtained a summary that omitted references to the weapon and said only that Alexis was charged with malicious mischief. If USIS and the Government had obtained a copy of that arrest report, perhaps Alexis's clearance would have been denied. Under its contract, USIS also was required to conduct a quality review of its background investigation of Alexis. However, nobody has confirmed that USIS did that quality review; USIS has not confirmed it, nor has OPM, and, interestingly, nor has the inspector general.

In 2011, a long-time USIS employee, its director of fieldwork services, accused USIS of a massive conspiracy to bilk the United States taxpayers. Let that sink in. Although USIS was required to conduct quality reviews of all of its background investigations, this official reported that USIS was "dumping" unfinished cases and billing OPM for work anyway. Inexplicably, USIS also had a separate contract with OPM to conduct additional quality reviews on behalf of the agency. In other words, USIS was checking its own work.

In January, the committee conducted a transcribed interview with Merton Miller, OPM's associate director of Federal Investigative Services. He accused USIS of using information obtained through its second contract to evade detection of its fraud under the first. He said this: "They circumvented OPM's oversight of their performance of their quality review. I am not splitting hairs, but they knew how we were auditing." He continued, "They knew what kinds of reports we generated to oversee that they were actually performing the activity, so they circumvented our oversight process and they falsified records to help do that."

The Department of Justice has now determined that these allegations have merit and filed a false claims suit seeking more than

$1 billion from USIS, claiming that the company charged taxpayers for work it never performed on, ladies and gentlemen, listen to this, on 665,000 background investigations from 2008 to 2012. We are better than that. The Department stated, "USIS management devised and executed a scheme to deliberately circumvent contractually required quality reviews of completed background investigations in order to increase the company's revenues and profits."

In 2007, USIS was purchased by a private equity firm known as Providence Equity Partners. The committee's investigation revealed that, directly after the acquisition, USIS adopted aggressive new financial incentives to accelerate its work. During this period, USIS executives received huge bonuses, including more than $1 million for the company's CEO, Bill Mixon, and about $470,000 for the company's chief financial officer.

As I close, the Justice Department alleges that both officials were "fully aware of and, in fact, directed the dumping practices." USIS also received millions of dollars in bonus payments from OPM, and I would like to know why that is, for its seemingly incredible progress, including $2.4 million in bonuses in 2008, $3.5 million in bonuses in 2009, and $5.8 million in bonuses in 2010. That is taxpayer dollars. In the wake of this scandal, the company's CEO, CFO, and nearly two dozen other officials have resigned, been terminated, or left the company. In fact, just yesterday, yesterday, USIS informed us that the president of its investigation services division has also now resigned. These revelations cry out for an investigation, but to date the committee has not conducted a single transcribed interview of any USIS employee.

Mr. Chairman, I know you wanted to focus first on OPM's oversight, and I do too, but given what we have now uncovered, these serious allegations must be investigated. While I have no objection to Mr. Phillips being here today, he was hired only last year and has no firsthand knowledge of these allegations. We should investigate, as we should in any case like this, how bonuses and incentives were paid to USIS executives—and, by the way, I want to know that from OPM—as well as the roles played by Providence Equity Partners and Altegrity, the holding company formed to house USIS.

Finally, Mr. Chairman, I appreciate that your staff provided us with a draft of your report last week, but I regret that you issued it yesterday without including most of the information about USIS that we asked to be included. For these reasons, I am issuing my own staff report today that provides that information, and I ask that it may be a part of the record.

Chairman ISSA. Without objection, the minority comments, in addition to the majority staff report, will be joined, and I share with the gentleman that, assuming the Department of Justice will concur, that we will be doing further transcribed interviews.

Mr. CUMMINGS. Thank you very much. I really appreciate that, Mr. Chairman.

Chairman ISSA. Thank you.

All members may have seven days to submit opening statements.

We now welcome our panel of witnesses.

Mr. Sterling Phillips is the CEO of US Investigations Services, LLC; we are joined by the Honorable Katherine Archuleta, who is

the newly named Director of the U.S. Office of Personnel Management, or OPM; Mr. Stephen Lewis is the Deputy Director of Personnel, Industrial and Physical Security Policy at the Department of Defense; the Honorable Patrick McFarland is the Inspector General of the U.S. Office of Personnel Management, again, OPM; and Ms. Susan Ordakowski is the Vice President of Contracts and Compliance at KeyPoint Government Solutions; and we are joined by Mr. Michael Rhodes, who is the Executive Vice President, Mission Systems and Services Business Group, for CACI International, Inc.

Pursuant to the rules, I would ask that you all please rise and take the oath, and raise your right hands, please. Do you solemnly swear or affirm that the testimony you are about to give will be the truth, the whole truth, and nothing but the truth?

[Witnesses respond in the affirmative.]

Chairman ISSA. Please be seated. Let the record reflect that all witnesses answered in the affirmative.

In order to allow time for this large panel, I would ask that you all observe strictly the five minute clock. Your entire opening statements are in the record, so your comments may be completely in addition to that, if you would like.

With that, we first recognize the gentlelady, OPM Director Katherine Archuleta.

WITNESS STATEMENTS

STATEMENT OF THE HONORABLE KATHERINE ARCHULETA

Ms. ARCHULETA. Chairman Issa, Ranking Member Cummings, and members of the committee, thank you for inviting me to testify today regarding the role of U.S. Office of Personnel Management in the Federal security clearance process. I appreciate the committee's oversight of this matter and I want you to know how deeply committed I am to ensuring the integrity and the efficacy of our programs and our products.

Understandably, this issue has come under greater scrutiny since the tragedy at the Washington Navy Yard, which took the lives of 12 people and injured 8 more. I want to express my deepest sympathies and condolences to those who lost loved ones in the Navy Yard tragedy. I can only imagine the anguish felt by the families of those affected by this senseless attack, and those individuals are in my thoughts and in my prayers as they move forward in light of this awful event.

OPM plays a critical role in protecting our national security. We conduct more than 2 million investigative actions each year for over 100 Federal agencies. This represents 95 percent of all background investigations. Each agency is responsible for determining whether an individual requires clearance and adjudicating eligibility for access to classified information. OPM provides the background information for many agencies to make an informed decision about security clearances.

Since arriving at OPM three months ago, I have made this issue a top priority. Of central importance to me are addressing legitimate questions about the background investigation process and working with DOJ and OPM's Office of Inspector General to investigate the outrageous allegations of fraud by one of our contractors.

Let me be clear: OPM does not tolerate and has never tolerated fraud in any form. It is wholly inconsistent with OPM's core values and does not reflect the integrity and the dedication of hard-working OPM employees. When any allegation of fraud is brought to OPM's attention, OPM works closely with DOJ and OPM's OIG to bring those involved to justice.

The case against USIS outlined in the complaint filed by DOJ raises grave concerns of an egregious violation of the public trust. Since we learned about these issues, OPM has taken steps to improve the oversight of our contracts, remove contractor employees from the contract, and strengthen our overall operations. It is imperative that we have a process in place that meets the highest standards of quality, efficiency, timeliness, and integrity; the American public expects no less and so do I.

At the President's direction, and under the leadership of the director of OMB, OPM has been working with its colleagues on the Sustainability and Security Performance Accountability Council to review the Federal security clearance and suitability processes. The background investigation program is a complex undertaking and OPM is vigilant in ensuring the highest standards of quality.

Mr. Chairman, I have made this issue one of my top priorities. Starting last week, I directed that the quality review process conducted by OPM be fully federalized. We no longer have contractors participating in our ongoing final federally controlled quality process. Having Federal employees now perform this function acts as an internal quality control, preventing any contractor from performing the final quality of review of its own work.

OPM remains committed to developing effective, long-term policies and processes for ensuring high quality review standards. As the largest provider of investigative products, OPM recognizes that, in a rapidly changing world, the background investigation program, and the security clearance process in particular, must keep up with the times while continuing to meet existing demands.

We continue to work with ODNI as the security executive agent and our other reform partners to ensure that we have processes in place that meet the high expectations set by Congress, our interagency partners and, most importantly, the American public. As the new director of OPM, I look forward to working with this committee to ensure the highest quality of background investigations through strong leadership, accountability, and forward thinking.

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

[Prepared statement of Ms. Archuleta follows:]

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

STATEMENT OF
THE HONORABLE KATHERINE ARCHULETA
DIRECTOR
U.S. OFFICE OF PERSONNEL MANAGEMENT

before the

UNITED STATES HOUSE OF REPRESENTATIVES COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

on

"DC NAVY YARD SHOOTING: FIXING THE SECURITY CLEARANCE PROCESS"

February 11, 2014

Introduction

Chairman Issa, Ranking Member Cummings, and members of the Committee, thank you for inviting me to testify today regarding the role of the U.S. Office of Personnel Management (OPM) in the Federal security clearance process. I appreciate the Committee's oversight of this matter, and I want you to know how deeply committed I am to ensuring the integrity and efficacy of our program and products.

OPM plays a critical role in protecting our national security. We conduct more than two million investigative actions each year for over 100 Federal agencies representing 95 percent of all background investigations. Each agency is responsible for adjudicating eligibility for access to classified information at that agency, but OPM provides the background information for many agencies to make

an informed decision about security clearances. OPM background investigations also support a host of other determinations or adjudications, including eligibility for national security sensitive positions and logical or physical access to Federal information, systems, and facilities; suitability for Federal employment in the competitive service (pursuant to a suitability program that OPM itself administers); fitness requirements for excepted service positions; military accessions; and fitness requirements imposed on individuals working under Government contracts.

Since arriving at OPM three months ago, I have made a priority of addressing legitimate questions that have been raised regarding the background investigation process. Of central importance to me is OPM's work with the Department of Justice (DOJ) and OPM's Office of the Inspector General (OIG) to investigate the outrageous allegations of fraud by one of our contractors.

Let me be clear, OPM does not tolerate and has never tolerated fraud in any form. It is wholly inconsistent with OPM's core values and does not reflect the integrity and dedication of hard working OPM employees. When any allegation of fraud is brought to OPM's attention, OPM works closely with DOJ and OPM's OIG to bring those involved swiftly to justice. The case against USIS outlined in the complaint filed by DOJ raises grave concerns of an egregious violation of the public trust. Since we learned about these issues, OPM has taken steps to improve the oversight of our contracts, remove contractor employees from the contract, and strengthen our overall operations.

It is imperative that we have a process in place that meets the highest standards of quality, efficiency, timeliness, and integrity. The American public expects no less, and so do I.

In the short time I have been at OPM, the agency has demonstrated its commitment to ongoing improvement through the continuous review and evaluation of its processes and operations. This has included collaborating with our colleagues from other agencies to review the sufficiency of the investigative standards, the frequency of reinvestigations, and what should be done when issues arise after a clearance is granted. While we are confident that our work meets all investigative standards, including those related to national security investigations, we are serious

about addressing any and all issues raised about the completeness of our work and the quality of our products.

Review of the Security Clearance Process

At the President's direction, and under the leadership of the Director of the Office of Management and Budget (OMB), OPM has been working with its colleagues on the Suitability and Security Performance Accountability Council (PAC) to review the Federal security clearance and suitability processes. This review is focused on steps that can be taken to strengthen current processes and to implement identified solutions. Participating in this review is a valuable opportunity for OPM and our partners to work together to ensure the integrity and efficacy of the background investigations we perform and the determinations they support, including adjudications of eligibility for access to classified decisions, suitability determinations, and credentialing decisions.

The background investigation program is a complex undertaking, and OPM is vigilant in ensuring the highest standards of quality. OPM continues to be responsive to concerns expressed by members and Committees of Congress, the Government Accountability Office (GAO), OPM's OIG, our customer agencies, and others. We are employing new quality assessment tools in our quality review processes to ensure that our background investigations meet investigation standards.

In addition, OPM is engaged in an interagency Quality Assessment Working Group that we co-chair with the Department of Defense and the Office of the Director of National Intelligence (ODNI). The working group brings together over 20 Federal agencies involved in investigations and adjudications who are devising better and more standardized means to measure the quality of background investigations across the Federal government.

OPM and ODNI, through the PAC, are also leading the way with training standards for investigators and adjudicators, which also help to ensure that investigations are conducted to consistent standards across all investigating agencies. The training standards for investigators are modeled after our own

Federal Background Investigator Training Program. OPM has been, and will continue to be, a leader in developing and implementing investigation training standards.

As is true in every area, OPM's background investigations program is only as strong as its people. In this regard, OPM has many qualified individuals leading the background investigation program, particularly when it comes to quality review. Moreover, members of this program's team are held to the highest standards of conduct and have the skills to review background investigations for completeness and accuracy.

Conclusion

Mr. Chairman, I have made this issue one of my top priorities. I am meeting with my staff regularly for updates related to the ongoing reviews and operational improvements, and I am making changes where appropriate.

Starting last week, I directed that the quality review process conducted by OPM be fully federalized. Only Federal employees will be conducting the second layer of quality review before the final product is sent to the agency for review and adjudication. We no longer will have contractors participating in our ongoing final federally controlled quality review process. Having Federal employees now perform this function responds to concerns, including the mere perception, that our review has been or ever will be anything less than rigorous. We believe this is the best immediate response. We remain committed to developing effective, long-term policies and processes for ensuring high quality review standards, and executing those standards.

As the largest provider of investigative products, OPM recognizes that, in a rapidly changing world, the background investigation program, and the security clearance process in particular, must keep up with the times while continuing to meet existing demands. We are continuing to work with the Director of National Intelligence, as Security Executive Agent, and our other reform partners to ensure that we have processes in place that meet the high expectations set by Congress, our interagency partners, and most importantly, the American public. I am

committed to continuing to work closely with our interagency partners, OPM's OIG, GAO, and members of this Committee and other members of Congress, to determine the best ways to improve the current system. Lastly, I want to ensure that our staffing and operations reflect the highest levels of quality review, integrity assurance, and ethical conduct.

Once again, thank you for the opportunity to testify today, and I welcome any questions you may have.

Chairman ISSA. Thank you. At this time I ask unanimous consent that the cases filed in the Alabama court, entitled Blake Percival v. U.S. Investigation Services, Inc., and the second one entitled United States of America ex rel Blake Percival v. U.S. Services be placed in the record. Without objection, so ordered.

Chairman ISSA. We now go to Mr. Stephen Lewis.

STATEMENT OF STEPHEN LEWIS

Mr. LEWIS. Chairman Issa, Ranking Member Cummings, and distinguished members of the committee, I appreciate the opportunity to appear before you today to address the practices and the procedures in the Department of Defense regarding the personnel security clearance process. I am here today on behalf of Under Secretary of Defense for Intelligence Michael Vickers, who serves as the principal staff assistant to the secretary and deputy secretary for security matters.

In addition, the USDI is the senior official for DOD's personnel security program and has the primary responsibility for providing oversight, guidance, and development for policy and procedures governing civilian, military, and industrial-based personnel security programs within the DOD.

In order to address the Department's personnel security policies and practices, I believe it is important to first identify the national level policy framework. Executive Order 13467 designates the Director of National Intelligence as the Security Executive Agent with the responsibility to develop uniform policies and procedures to ensure effective completion of investigations and determinations of eligibility for access to classified information or to hold National Security Positions, as well as reciprocal acceptance of those determinations.

In addition, E.O. 13467 designates the Director of the Office of Personnel Management as the Suitability Executive Agent with similar responsibilities for those who have positions that require eligibility for logical and physical access to Federal Government installations and information systems.

Finally, 13467 creates a Performance Accountability Council, chaired by the Deputy Director for Management in the Office of Management and Budget, and includes the DNI and the Director of OPM with the responsibility to ensure alignment of suitability security and, as appropriate, contractor employee fitness investigative and adjudicative processes.

With regard to the oversight roles and responsibilities within DOD, the heads of DOD Components are responsible for establishing and overseeing implementation of procedures to ensure prompt reporting of significant derogatory information, unfavorable administrative actions, and adverse information related to its personnel; and this information goes to appropriate officials within their component and, as applicable, to the DOD Consolidated Adjudication Facility. This responsibility applies to military service members, DOD civilians, and embedded contractor personnel.

Under the National Industrial Security Program, cleared contractors are required to report adverse information coming to their attention regarding their cleared employees. In addition, the Defense Security Service is responsible for conducting oversight of compa-

nies cleared to perform on classified contracts for DOD and 26 other Federal departments and agencies that use DOD industrial security services.

The Department has worked very hard to create improvements that produced greater efficiencies and effectiveness in the phases of initiating and adjudicating background investigations. In 2011, the Government Accountability Office removed DOD's personnel security clearance program from its high risk list.

We have used multiple initiatives to review and confirm the quality of the investigative products we receive, the quality of our adjudications, and the accuracy and completeness of the documentation of adjudicative rationales in support of oversight and reciprocity. In addition, we have implemented a certification process for DOD personnel security adjudicators.

I thank you for your time and look forward to answering your questions.

[Prepared statement of Mr. Lewis follows:]

Statement of

Mr. Stephen Lewis
Deputy Director for Personnel, Industrial and Physical Security Policy
Counterintelligence & Security Directorate
Office of Under Secretary of Defense for Intelligence

before the
House Committee on Oversight and Government Reform
on

February 11, 2014

Good Afternoon

Chairman Issa, Ranking Member Cummings, and distinguished Members of the Committee – I appreciate the opportunity to appear before you today to address the practices and procedures in the Department of Defense regarding the security clearance process. I am Steve Lewis, Deputy Director for Personnel, Industrial and Physical Security Policy in the Office of the Under Secretary of Defense for Intelligence, and I am here today on behalf of Under Secretary, Michael Vickers.

The Under Secretary of Defense for Intelligence (USDI) is the Principal Staff Assistant to the Secretary and Deputy Secretary for security matters. In addition, the USDI is the senior official for DoD's personnel security program and has the primary responsibility for providing and approving guidance, oversight,

and development for policy and procedures governing civilian, military, and industrial base personnel security programs within DoD.

In order to address the Department's personnel security policies and practices, I believe it is important to first identify the national level policy framework. Executive Order (E.O.) 13467 designates the Director of National Intelligence (DNI) as the Security Executive Agent with the responsibility to develop uniform policies and procedures to ensure effective completion of investigations and determinations of eligibility, for access to classified information or to hold National Security Positions, as well as reciprocal acceptance of those determinations. In addition, E.O. 13467 designates the Director of the Office of Personnel Management (OPM), as the Suitability Executive Agent, with responsibility for developing and implementing uniform and consistent policies and procedures regarding investigations and adjudications, relating to determinations of suitability and eligibility for logical and physical access to Federal Government installations and information systems. Finally, E.O. 13467 creates a Performance Accountability Council, chaired by the Deputy Director for Management, Office of Management and Budget, and including the DNI and the Director OPM, with the responsibility to ensure alignment of suitability, security, and, as appropriate, contractor employee fitness investigative and adjudicative processes.

With regard to the oversight roles and responsibilities within the DoD, the heads of DoD Components are responsible for establishing and overseeing implementation of procedures to ensure prompt reporting of significant derogatory information, unfavorable administrative actions, and adverse actions related to its personnel, to appropriate officials within their component and, as applicable, to the DoD Consolidated Adjudication Facility. This responsibility applies to military service members, DoD civilians, and embedded contractor personnel.

Under the National Industrial Security Program (NISP), cleared contractors are required to report adverse information coming to their attention regarding their cleared employees. In addition, the Defense Security Service (DSS) is responsible for conducting oversight of companies cleared to perform on classified contracts for DoD and 26 other federal departments and agencies that use DoD industrial security services.

The Department has worked very hard to create improvements that produced greater efficiencies and effectiveness in the phases of initiating and adjudicating background investigations. As a result, in 2011, the Government Accountability Office removed the DoD's personnel security clearance program from the high risk list.

We have used multiple initiatives to review and confirm (1) the quality of the investigative products we receive, (2) the quality of our adjudications, and (3)

the accuracy and completeness of the documentation of adjudicative rationale in support of appropriate oversight and reciprocity. In addition, we have implemented a certification process for DoD personnel security adjudicators.

In May, 2012, the Deputy Secretary of Defense directed the consolidation of all adjudicative functions and resources (except for DoD Intelligence Agencies) at Fort Meade, Maryland, under the direction, command, and control of the Director of Administration and Management (DA&M). This decision was made in order to maximize the efficiencies realized by the collocation of the various Centralized Adjudications Facilities (CAFs) under the 2005 round of Base Realignment and Closure (BRAC). Effective October 1st, the DoD CAF has also been tasked to adjudicate background investigations which serve as the basis for the issuance of Common Access Cards (CACs) used for physical access to DoD installations and access to DoD information systems.

I thank you for your time, and look forward to answering your questions.

Chairman ISSA. Thank you.

Mr. McFarland, you are recognized for five minutes.

STATEMENT OF THE HONORABLE PATRICK MCFARLAND

Mr. MCFARLAND. Good morning, Chairman Issa, Ranking Member Cummings, and distinguished members.

Recent events, including the horrific actions of Aaron Alexis and the unauthorized disclosure of classified information by Edward Snowden show how critical it is to continuously improve and strengthen the background investigations process. I am grateful that the committee is holding this hearing and taking steps to address this issue.

The U.S. Office of Personnel Management carries an immense responsibility regarding its critical role in safeguarding our Country's national security. There is no other entity of the Federal Government that serves in the capacity of a first responder to such a vast linkage of current Federal employees and the constant flow of applicants for Government positions.

The background investigations OPM performs are the very first step in determining whether a person deserves the trust of the United States and should be permitted access to restricted areas and sensitive information. Director Archuleta has requested several briefings from us on the issue and we are very appreciative of her strongly stated support for our work.

We performed an in-depth examination of Mr. Alexis's background investigation, which was conducted by USIS in its role as a contractor for OPM's Federal Investigative Services. During this review, we found that although the OPM procedures in place at that time were followed, other steps, such as directly contacting the King County District Court, could have provided critical additional information.

The committee's recently released report entitled Slipping Through the Cracks contains a straightforward analysis that shows several weaknesses in the background investigation process and contains multiple recommendations that I believe will greatly strengthen OPM's program. The Office of the Inspector General is ready and willing to offer any assistance we can as the committee pursues its reform efforts.

It has been well publicized that the OIG is the lead investigating entity in a civil suit against USIS. My written testimony more fully describes the allegations contained in the complaint filed by the Department of Justice. In short, the complaint alleges that USIS failed to perform quality reviews related to at least 665,000 cases as required under its contract with OPM. This permitted USIS to release more background investigation cases to OPM, which in turn allowed it to increase the company's bottom line.

The exact damages suffered by OPM will be determined by the court at trial. The penalties imposed under the False Claim Act range from $5,500 to $11,000 per false claim or statement. If each of these 665,000 cases were considered a false claim or statement, penalties could range from approximately $3.7 billion to $7.3 billion.

In closing, I would like to offer a very sincere thank you to this committee and to their staff for crafting the recent legislation enti-

tled The OPM IG Act. Subcommittee Chairman Blake Farenthold and Ranking Member Steven Lynch provided the much needed forum for us to explain the dilemma facing our Office of Inspector General as a result of an agency funding decision. As you know, an unconscionable denial of funding greatly thwarted our efforts to properly audit and investigate an OPM program of paramount national security concern, the Federal Investigative Services. Regardless, we utilized as best we could our office's general appropriation funding to accomplish as much oversight as was feasible.

Chairman Issa and Ranking Member Cummings, you have our organization's pledge, now with access to the OPM Revolving Fund, that we will fully engage our audit and investigative resources to protect the national security. Thank you.

[Prepared statement of Mr. McFarland follows:]

Office of the Inspector General
United States Office of Personnel Management

Statement of the Honorable
Patrick E. McFarland
Inspector General

before the

Committee on Oversight and Government Reform

United States House of Representatives

on

"D.C. Navy Yard Shooting: Fixing the Security Clearance Process"

February 11, 2014

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

Good morning. My name is Patrick E. McFarland. I am the Inspector General of the U.S. Office of Personnel Management (OPM). Thank you for inviting me to testify at today's hearing on policy issues related to background investigations conducted by OPM that are used to grant security clearances, as well as our recent investigative and audit work in that area.

Aaron Alexis

In response to a letter from Senators Claire McCaskill, Ron Johnson, Jon Tester, and Rob Portman, my office performed a review of the background investigation of Aaron Alexis. We reported the results of our review to the Senators, as well as to the distinguished Members of this Committee, in a letter dated November 5, 2013.

OPM conducted only one background investigation of Mr. Alexis: his initial background investigation in 2007. Therefore, OPM was not aware of any actions or incidents that occurred after 2007. This is because OPM conducts reinvestigations of individuals only at the request of their employing agencies.

Further, it is important to note that OPM is not involved in the decision to grant security clearances. Rather, OPM's background investigation reports are provided to customer agencies, which are then responsible for reviewing the available information and determining whether a clearance should be granted.

Based on the background investigation report provided by OPM, the U.S. Department of the Navy had these two critical pieces of information *before it granted Mr. Alexis a SECRET clearance in 2007*: (1) that he had been arrested for "malicious mischief" in 2004 and that the charge was dismissed and (2) that Mr. Alexis had falsely stated on his personnel security questionnaire that he had never been arrested. Thus, although the Navy did not know the details of the arrest, they did know of the arrest and that Mr. Alexis failed to disclose the arrest.

During our review of Mr. Alexis's background investigation, we determined that the background investigators complied with OPM's established procedures in force at the time. However, at issue is a particular OPM procedure, which permitted background investigators to rely exclusively on databases if they could not obtain information directly from local law enforcement organizations, which continues to be the current procedure.

Mr. Alexis's Arrest

The arrest for "malicious mischief" in 2004 involved a situation where Mr. Alexis shot the tires of a car with a firearm. Mr. Alexis confessed to this action to the investigating detectives from the Seattle Police Department and was booked into the King County jail.

The Office of the Inspector General's (OIG) investigators confirmed that in 2007, the Seattle Police Department released only conviction information to OPM background investigators. Incident reports concerning arrests that did not result in a conviction were not released. As a result, the background investigator did not obtain any records from the Seattle Police Department.

OPM Background Investigation Procedures

The type of background investigation requested by the Navy includes conducting checks of law enforcement and financial records. Because records checks revealed an arrest and financial issues, a background investigator was also tasked with conducting a subject interview of Mr. Alexis.

OPM's Federal Investigative Services' (FIS) Investigator's Handbook states that law enforcement records are typically obtained by computer link or inquiry. A background investigator is expected to obtain the law enforcement record and disposition of the case in any locations of known arrests. *If the law enforcement arrest records do not contain the disposition of the case, background investigators are expected to obtain court records as well.*

However, FIS informed the OIG that it "sometimes provides standard workarounds to investigators, such as using an automated database that captures local court records where prior history with a locality establishes that it is unwilling or unable to provide historical arrest records."

Because the Seattle Police Department at that time did not release the required information, the background investigator accessed court records by computer link to the Washington Statewide District and Municipal Courts Database and the King County Superior Court's Database. Based upon a review of these database records, the background investigator reported the 2004 incident as a charge for "malicious mischief," with no mention of a firearm.

The OIG, however, contacted the King County District Court directly and obtained a document (referred to as a "Superform") that *did* make reference to use of a firearm. The OIG learned that in 2007, the Superform would have been available in paper format if a background investigator had come to the courthouse in person or submitted a telephonic or written request, but it would *not* have been available electronically through a database. A representative of the King County District Court informed us that there was no record that a background investigator directly contacted the court regarding Mr. Alexis.

Thus, the background investigation report relied only on electronic databases for information pertaining to the 2004 arrest of Mr. Alexis. If the King County District Court had been contacted directly in 2007, the background investigator would have obtained the Superform and thus been aware of – and presumably reported – the fact that the 2004 arrest involved a firearm. This incident proves that overreliance on automated records and databases may result in missing critical information.

Based on our review, the OIG made the following recommendations in the November 5, 2013 letter:

1. Review of whether national policy concerning the adjudication of security clearances should specifically address whether individuals who provide material false statements on personnel security questionnaires be deemed ineligible for SECRET security clearances.

2. Revision of national policy to require reinvestigation for SECRET security clearances more often than once every ten years, as is the current policy.

3. Continued focus on efforts to improve background investigators' access to State and local law enforcement records.

4. Revision of OPM policy to require direct contact with courts and review of the complete court record when relevant court records have been identified in a database and are substituted for unavailable law enforcement records.

Qui Tam Lawsuit Against USIS

In August 2011, the OIG was notified by the Department of Justice (DOJ) that a *qui tam* complaint had been filed against U.S. Investigative Services, LLC (USIS) which included allegations that USIS had violated the False Claims Act by not performing contractually-required quality reviews of Reports of Investigation (ROIs).

The OIG immediately began investigating the allegations and has been working closely with OPM's FIS and DOJ on this matter. DOJ filed its notice to intervene in the *qui tam* lawsuit on October 30, 2013, and filed its official complaint on January 22, 2014.

Because our investigation is still ongoing and the case is currently being litigated in Federal Court, I must stress that I may discuss only that information that is in the public domain. To do otherwise would compromise the Government's ability to ensure that those who violate the law are held accountable.

I would also like to note that after OPM and the OIG were informed of the *qui tam* lawsuit, OPM began taking steps to address the issue and prevent dumping from occurring. The most recent of these steps was announced last week, when OPM Director Katherine Archuleta determined that USIS would no longer have any role in the final closing review function, and that this function would be performed only by Federal employees. OPM is in a better position to describe its other reforms.

Background

As background, USIS holds two contracts with OPM: (1) a Fieldwork Contract to perform investigative fieldwork and (2) a Support Contract to perform support services. Multiple companies hold Fieldwork Contracts with OPM, but USIS is the only contractor that holds a Support Contract.

In performing a background investigation under a Fieldwork Contract, the contractor's employees conduct assigned interviews and/or review records, and then write "Reports of Investigation" or "ROIs." A single background investigation case may contain multiple ROIs written by different background investigators if, for example, the subject of the background investigation lived in multiple cities.

The Fieldwork Contracts required each contractor, including USIS, to perform a quality review of all its ROIs prior to releasing a case to OPM. The contractor was paid the majority of its fee when these cases were released to OPM.

Once a contractor completed a background investigation and released the case to OPM, OPM's procedures required the background investigation to receive a final closing review before it was sent to the customer agency. Prior to the aforementioned reform, many final closing reviews were performed by USIS employees under the Support Contract. Consequently, in many cases closed during the time period of the alleged dumping, both the fieldwork and final closing review were performed by USIS employees, albeit under separate contracts.

Allegations

Please note that this is a summary of the allegations made in the civil complaint filed by DOJ, pursuant to the investigation conducted by the OIG and FIS. These are only *allegations* and have yet to be ruled upon by a court.

According to the civil complaint,

> [b]eginning in at least March 2008 and continuing through at least September 2012, USIS management devised and executed a scheme to deliberately circumvent contractually required quality reviews of completed background investigations in order to increase the company's revenues and profits. Specifically, USIS devised a practice referred to internally as "dumping" or "flushing," which involved releasing cases to OPM and representing them as complete when, in fact, not all ROIs comprising those cases had received a quality review as required by the Fieldwork Contract.
>
> USIS engaged in the practice of dumping in order to meet budgeted goals and, therefore increase its revenues and profits. Given that USIS was paid by OPM for each completed case, the more cases USIS completed each month the more money it received from OPM. USIS's dumping practices also enabled the company to receive annual performance incentive payments that it would not otherwise have been entitled to receive absent the dumping.

As described in the complaint, initially, USIS dumped cases manually. Eventually, however, USIS used a software program called Blue Zone that enabled USIS to mark a large number of ROIs as "Review Completed," even if they had not in fact been reviewed. These cases were then automatically released to OPM with the notation "Review Completed" attached.

According to the allegations, each morning, USIS employees, including some in supervisory positions, identified all of the ROIs that needed to be reviewed that day in order to meet USIS's internal goals. At the end of the day, designated USIS staff determined how many assigned ROIs had not been reviewed that day. Using Blue Zone, these employees dumped some or all of those un-reviewed ROIs. Some ROIs were dumped even if they had not yet been assigned to a reviewer.

The allegations also state that soon dumping began to occur at various times during the day, not only at the end of the day, which increased the number of cases that were dumped. Although dumping occurred on a daily basis, the number of cases dumped tended to increase significantly at the end of the month, quarter, and year.

DOJ's complaint alleges that senior management at USIS were not only aware of but directed the dumping practices. Beginning in at least March 2008, USIS's President/Chief Executive Officer established the internal revenue goals for USIS. USIS's Chief Financial Officer determined how many cases needed to be reviewed or dumped to meet these goals. This information was passed down the corporate ladder.

As detailed in the civil complaint, during the time period March 2008 through September 2012, USIS released at least 665,000 background investigations to OPM and represented them as complete when, in fact, one or more of the ROIs comprising those background investigations had not received a quality review as required by the Fieldwork Contract. This represented approximately 40 percent of the total background investigations conducted by USIS during that time frame.

The civil complaint also describes various steps that USIS allegedly took to conceal its dumping practices from OPM. For example, in April 2011, OPM conducted a data analysis that showed that a small group of USIS employees were identified as having released a substantial number of cases when compared with the workload of other reviewers. In addition, the data analysis showed that some ROIs marked as "Review Complete" had not even been opened by a USIS reviewer. OPM wrote to USIS about these concerns. USIS failed to disclose its dumping practices and instead informed OPM that these issues were due to a variety of software problems and glitches. USIS also ceased dumping practices when OPM was onsite conducting audits.

Further, as alleged by DOJ, USIS personnel working on the Fieldwork Contract also improperly used information received by USIS pursuant to its responsibilities under the Support Contract in order to prevent OPM from discovering its dumping scheme. Those USIS employees reviewing cases under the Fieldwork Contract would determine which categories or types of cases that OPM was likely to target for review and closing by the FIS Federal staff after the case was transmitted to OPM, as opposed to those cases more likely to be directed to USIS employees under the Support Contract. As the civil complaint noted, this was done to minimize the risk that cases would be returned to USIS by FIS for further rework, and raise concerns at OPM about the quality of the review process.

USIS received performance awards for meeting OPM's established goals in the areas of timeliness, quality, and program management for the years 2008, 2009, and 2010 totaling approximately $11.8 million that it would not have received had OPM known of its fraudulent actions.

Effect of USIS's Fraud

Recently, OPM has publicly stated that all background investigation cases dumped by USIS underwent subsequent quality reviews, thus implying that the quality of the background investigations provided by OPM to customer agencies is not in doubt. We feel that this statement is premature and overly confident. OPM is assuming that the final closing reviews conducted at the time were sufficient despite the fact that, as OPM's support contractor, USIS personnel were performing many of the final closing reviews. As described earlier, the civil complaint alleges that USIS personnel working on the Fieldwork Contract improperly used information received by USIS pursuant to its responsibilities under its Support Contract to identify the case types that OPM intended to have FIS Federal staff review. USIS thereby avoided dumping those case types, choosing instead to dump cases that they expected to be reviewed by USIS support personnel. As mentioned earlier, the civil complaint stated that USIS did this to avoid raising concerns at OPM about the quality of the review process.

In addition, a final audit report issued by the OIG in 2010 observed that USIS, in its role as OPM's support contractor, was frequently closing deficient cases. For example, an internal audit conducted by OPM in March 2009 found that 28.24 percent of cases closed by the support contractor were unacceptable during the second quarter of fiscal year 2009.

Consequently, the OIG is very concerned about the potential quality implications of USIS's alleged fraudulent actions. Indeed, the civil complaint alleges that USIS dumped ROIs *knowing* there could be potential quality issues associated with those ROIs. We have informed OPM of our concerns both in writing and orally during meetings. Although OPM disagrees, I would like to note for the record that the OIG continues to believe that USIS's fraud may have caused serious damage to national security.

OIG Audits of OPM's Background Investigations Program

The OIG is currently conducting an audit examining the operations of both FIS and its contractors. Specifically, the audit is examining whether:

1. FIS has adequate oversight controls in place to ensure that contractors are meeting their contract requirements.
2. The contractors' background review processes meet their contract requirements.
3. FIS has controls in place to ensure the Federally-conducted background investigations are reviewed.
4. FIS and its contractors have controls in place to ensure that their review personnel are trained to perform their duties.

Prior to this current audit, the OIG issued an audit report of the quality assurance process over background investigations on June 22, 2010 (2010 Audit). At that time, the OIG was particularly concerned about falsification of background investigations by both Federal and contractor background investigators. The primary objective of the 2010 Audit was to determine whether FIS had effectively implemented controls for the related quality assurance process. Our auditors were looking at the controls in place to prevent falsification and not the controls over the review of ROIs.

Conclusion

The issues addressed at today's hearing emphasize the critical need for greater oversight of the background investigations process. I offer my sincere thanks to Subcommittee Chairman Blake Farenthold, Ranking Member Stephen Lynch, and the other distinguished Members of this Committee for championing the OPM IG Act, which, as of February 7, 2014, is awaiting signature by the President. This Act will give the OIG the funding and resources necessary to increase oversight of the operations of FIS and the other Revolving Fund programs and hopefully help OPM improve its work in those areas. I assure you that I am determined and committed to

taking any and all steps available to work with OPM to strengthen the background investigations program, which has such a significant impact upon national security.

I am happy to answer any questions you may have.

Chairman ISSA. Thank you.
Ms. Ordakowski.

STATEMENT OF SUSAN A. ORDAKOWSKI

Ms. ORDAKOWSKI. Good morning, Chairman Issa, Ranking Member Cummings, and members of the committee. Thank you for the opportunity to be here today to discuss the Federal security clearance process. My name is Sue Ordakowski. I am the Chief Contracts and Compliance Office of KeyPoint Government Solutions, and I am also the Acting Program Executive for the KeyPoint OPM Background Investigation Program. I joined KeyPoint shortly after the company won its first Government contract in 2004, and my role is to make sure the company does things the right way.

The committee initially invited KeyPoint's President, Jeff Schlanger, to testify, and he is here today, but, as we discussed with your staff, he recently availed himself of an opportunity to return to public service as the chief of staff to the Manhattan district attorney. He remains on KeyPoint's board, however, and is a key advisor to the company.

Fourteen years ago, KeyPoint was founded as Kroll Government Services. In 2004, OPM expanded its contractor pool from just USIS and KeyPoint was awarded a position on the IDIQ contract for background investigations. In May 2009, the company was spun off from Kroll and renamed KeyPoint.

Over time, KeyPoint has built a high-quality, well-trained network of experienced investigators and a culture of zero tolerance for any lapses of integrity. In large part, KeyPoint's success can be attributed to the fact that our company's focus was and is providing high-quality, fairly priced background investigations to OPM and other Government agencies. Today, KeyPoint performs approximately 25 percent of the fieldwork conducted by contractors for OPM's background investigations and we are working hard to achieve parity with our major competitor on the contract.

As this committee assesses the security clearance process, it will compare the performance of private enterprises and the Government. We believe this is an important comparison that will help to achieve our collective goal of protecting our Nation's secrets to the greatest extent possible. Although this hearing is highlighting problems with one contractor, and not the Government, both have experienced their share of problems with a process that requires constant vigilance, integrity, and improvement.

KeyPoint has collaborated with various Government agencies, including OPM, to improve the background investigation process. An example of this is our Investigator of the Future initiative through which we are working collaboratively with OPM to develop a tablet-based tool for collecting field data and providing reference resources directly to investigators in the field. We believe the tool will increase quality and efficiency, and protect the large amounts of personally identifiable information that we collect and utilize.

OPM contract requirements are rigorous and complex, and we commit significant resources to ensure that we meet or exceed OPM standards. Because of our solid performance on the OPM contract, OPM has encouraged KeyPoint to grow its capacity, and we have done so. Throughout the years, our primary focus has always

been on the quality of our case work. We have implemented a comprehensive quality review system to ensure independent review of each case before submission to OPM. We have never wavered from this focus on quality and never intend to do so.

It is our understanding that the primary purpose of this hearing is to explore ideas for improving the background investigation process. A few key areas where improvements could be made include, one, consistency between the requirements set by OPM versus those set by agencies with delegated authority; two, the use of technology; three, the use of new sources of information; four, continuous evaluations; five, the contracting process; and, six, increased cooperation from State and local authorities. I have provided more details on these points in my written testimony.

In conclusion, I am very proud of the service that KeyPoint has provided to the United States Government over the past 14 years and look forward to continued growth. KeyPoint will continue its work to constantly improve the security clearance investigation process and will continue our tradition of providing the highest quality investigations at fair prices to our client agencies and to the taxpayer.

I appreciate the opportunity to testify before you and welcome your questions.

[Prepared statement of Ms. Ordakowski follows:]

Statement of Susan A. Ordakowski
KeyPoint Government Solutions
Vice President, Contracts and Compliance
Acting Program Executive for OPM Program
February 11, 2014
House Committee on Oversight and Government Affairs

Good morning, Chairman Issa, Ranking Member Cummings, and Members of the Committee. Thank you for the opportunity to be here today to discuss the federal security clearance process. My name is Sue Ordakowski. I am the Chief Contracts and Compliance Officer of KeyPoint Government Solutions ("KeyPoint"), and I am also the Acting Program Executive for the KeyPoint OPM Background Investigation Program. I have been a Vice President of the company since March 2004, and have been involved with our Office of Personnel Management ("OPM") contract from the beginning. I joined KeyPoint shortly after the company won its first government contract, and my role is to make sure the company does things the right way. I have worked for government contractors for over 30 years, and I have served as a contracts executive for the past 20 years for both large and small government contractors.

The Committee initially invited KeyPoint's President, Jeff Schlanger, to testify, and he is here today, but, as we discussed with your staff, he recently availed himself of an opportunity to return to public service as the Chief of Staff to the Manhattan District Attorney. Although Jeff stepped down from his role as President on January 30, 2014, he remains on KeyPoint's board and is a key advisor to the company.

KeyPoint History

Fourteen years ago, Kroll Government Services, a wholly-owned subsidiary of Kroll, Inc., was started to provide consulting and independent investigation services to local, state and federal agencies. The company's goal was to bring some of the best practices of the private sector to government contracts. KeyPoint quickly captured various types of federal background investigation contracts, including contracts for the Transportation Security Agency, Customs and Border Protection, and Immigration and Customs Enforcement . In 2004, OPM expanded its contractor pool from just USIS, and KeyPoint competed for and was awarded a position on the IDIQ contract for background investigations. In May 2009, Kroll Government Services was spun off from Kroll and became a stand-alone company, renamed KeyPoint Government Solutions.

Over time, KeyPoint has built a high-quality, well-trained network of experienced investigators and a culture of zero tolerance for any lapses of integrity. In large part, KeyPoint's success can be attributed to the fact that our company's focus was and is providing high-quality, fairly priced background investigations to OPM and other government agencies. Today, KeyPoint performs approximately 25 percent of the fieldwork conducted by contractors for OPM's background investigations, and we are working very hard to achieve parity with our major competitor on the contract.

As this Committee assesses the security clearance process, from data collection to final adjudication, it undoubtedly will compare and contrast the responsibilities and results of both private enterprises and the government. That comparison is important and, we believe, will be helpful in achieving our collective goal of protecting our nation's secrets to the greatest extent

possible. Contractors and government employees bring strong capabilities to the overall background investigations process but, while this hearing is highlighting problems with a certain contractor, both have experienced their share of problems with a process that requires consistent vigilance, integrity and improvement.

KeyPoint prides itself on providing high-quality products, including background investigations, at a competitive price to the U.S. government. We are constantly striving to improve our processes and procedures and to provide better and more cost-effective service to our customers.

To that end, we have collaborated with various government agencies, including OPM, to improve the background investigation process through initiatives focused on increasing the use of technology. An example of this is our "Investigator of the Future" initiative through which we are working collaboratively with OPM to develop a tablet-based tool for collecting field data and providing reference resources directly to investigators in the field. We believe the tool will increase quality and efficiency and protect the large amounts of Personally Identifiable Information that we collect and utilize.

OPM contract requirements are rigorous and complex. We invest extensively in training and mentoring in order to ensure that we meet or exceed OPM standards. Because of our solid performance on the OPM contract, KeyPoint has been encouraged by OPM to grow its capacity and we have done so. Throughout the years, our primary focus always has been on the quality of our case work. We have implemented a comprehensive quality review system to ensure independent review of each case before submission to OPM. We have never wavered from this focus on quality and never intend to do so.

Improving the Security Clearance Investigation Process

It is our understanding that the primary purpose of this hearing is to explore ideas for improving the background investigation process. A few key areas where improvements could be made include: (1) consistency between the requirements set by OPM versus those set by agencies with delegated authority; (2) the use of technology; (3) the use of new sources of information; (4) continuous evaluations; (5) the contracting process; and (6) increased cooperation from state and local authorities.

Consistent Standards: KeyPoint believes that OPM's qualifications for and required training of investigators are wholly appropriate. That said, there are some significant discrepancies between requirements set by OPM and those set by agencies with delegated authority. The system would benefit from a common standard for investigator qualifications and training, which we understand is currently under consideration by government working groups. Similarly, the standards for investigations themselves, as well as report formats and content specifications, differ between OPM and the agencies with delegated authority. Reconciliation of those standards will facilitate consistent adjudication and reciprocity.

Use of Technology: We also believe that the investigative process could be improved through expanded use of technology that could promote quality, timeliness and efficiency, and we are working with OPM on facilitating such improvements. For instance, there are automated systems that would allow us to compare various identity checks and data with the answers subjects provide in the SF86 Security Clearance Questionnaire, which could help identify false or omitted information.

Sources of Information: Currently, investigators do not review subjects' social media or traditional media records. Those sources of information should be reviewed in appropriate circumstances to conduct more thorough investigations. It is important, however, that the utilization of such sources be balanced against a person's right to privacy.

Continuous Evaluation: KeyPoint believes that implementing a continuous evaluation process of security clearance holders would improve the process tremendously, provided that OPM and agencies with delegated authority develop consistent standards for such evaluations. We are mindful that cost, also, must be factored into this equation.

Contracting Process: Some delegated authority agencies use "Low Cost, Technically Qualified" as the evaluation for awards for their fieldwork contractors. These contracts should be "Best Value" procurements. Currently, bidders who understand that ensuring quality comes with significant costs cannot prevail. Of course price should be a factor, but it should not be the only factor for such a critical function, even after technical qualification is determined.

State and Local Authorities: Federal mandates that require law enforcement agencies, both state and local, to cooperate with security clearance investigations by providing full details of arrests and investigations would greatly improve the ability to evaluate whether a particular incident should be disqualifying.

Conclusion

In conclusion, I am very proud of the service that KeyPoint has provided to the United States Government over the past fourteen years and look forward to continued growth. KeyPoint will continue its work to constantly improve the security clearance investigation process and will

continue our tradition of providing the highest quality clearance investigations at fair prices to our client agencies and to taxpayers. I appreciate the opportunity to testify before you today. I am glad to answer your questions.

Chairman ISSA. Thank you.
Mr. Rhodes.

STATEMENT OF MICHAEL RHODES

Mr. RHODES. Good morning, Chairman Issa, Ranking Member Cummings, and members of the committee. Thank you for the opportunity to appear before you today. My name is Michael Rhodes and I an Executive Vice President with CACI and Manager of the Mission Systems and Services Business Group, the business unit within CACI responsible for our work with the Office of Personnel Management, or OPM.

I would like to provide you with a brief introduction to our company and the work we do to assist OPM in the security clearance process.

CACI is an organization of nearly 16,000 professionals working in more than 120 offices worldwide, with a very diverse information solutions and services customer base. CACI is one of the three contractors currently assisting OPM by conducting fieldwork for security clearance investigations. We perform approximately 11 percent of OPM's fieldwork assignments, which equates to slightly more than 1 percent of our company's overall annual business base.

Having provided mission support services to the Government for the past 50 years, we understand that the process of conducting background investigations is fundamental to our national security. On a daily basis, CACI employees work side-by-side with those people whose lives depend upon us getting the security clearance process right. Like them, our primary commitment is to protecting our national security. Quality, accuracy, and thoroughness must come first.

Our business practices and model under the OPM contract demonstrate the emphasis we place on quality. CACI investigators are expected to conduct their fieldwork in accordance with OPM guidelines, and we conduct an robust internal review of investigations for quality, accuracy, and thoroughness prior to submission to OPM for final review and approval.

Now, our business model is based upon four key principles: first, our corporate culture, the character of the company and its employees, and the importance we place on ethics and integrity; second, having the right policies and procedures for oversight; third, effective and continual training; and, fourth, a constant auditing and monitoring.

Now, to be clear, we do not grant clearances or make recommendations as to who should receive a security clearance. Our primary role in the investigation process is fact-finding, ensuring that we conduct background investigations in accordance with OPM guidelines and contract requirements. We provide the results of our investigation to the Government for their approval and use in making their final clearance determinations.

We know firsthand about the importance of an effective security clearance process, as more than half of our employees hold clearances that are critical to the work they perform for our Country. Even though we were not the investigators for Snowden or Alexis, we were deeply impacted, most notably by the incident at the Navy

Yard, where we have a substantial number of CACI employees. We collectively mourn with our Nation when these tragedies happen.

We at CACI are committed to best practices and continuous improvements in the security clearance process. In this regard, we have suggestions in three areas: first, making background investigations more efficient; second, more effectively capturing information; and, third, strengthening contractor oversight.

On behalf of my company, and as a former active duty Army officer and a security clearance holder for over 30 years supporting the intelligence community, I thank you for the opportunity to present CACI's input on these matters, and I appreciate the courtesies extended to us by you and your staff during the course of this inquiry. Thank you for inviting me to testify today, and I look forward to your questions.

[Prepared statement of Mr. Rhodes follows:]

Michael P. Rhodes, Executive Vice President
Mission Systems and Services Business Group
CACI International Inc

Written Testimony for the House Oversight and Government Reform Committee
February 11, 2014

Good morning Chairman Issa, Ranking Member Cummings, and Members of the Committee. Thank you for the opportunity to appear before you today. My name is Michael Rhodes, and I'm an Executive Vice President with a wholly owned subsidiary of CACI International Inc ("CACI") and Manager of the Mission Systems and Services Business Group, the business unit within CACI responsible for our work with the Office of Personnel Management ("OPM").

CACI is an organization of nearly 16,000 professionals working in more than 120 offices worldwide, with a very diverse information solutions and services customer base. CACI is one of three contractors that currently assist OPM by conducting fieldwork for security clearance investigations. We perform about 11% of OPM's fieldwork assignments, which comprises about 1% of our overall business.

Having provided mission support services to the government for the past fifty years, we understand that the process of conducting background investigations is fundamental to our national security. We know first-hand about the importance of an effective security clearance process, as more than half of our employees hold clearances that are critical to the work they perform for our country. On a daily basis, CACI employees work side by side with those people

whose lives depend upon us getting the security clearance process right. Like them, our primary commitment is to protecting our national security.

Our business model under the OPM contract is based on four key principles:

- First, our corporate culture – the character of the company and its employees, and the importance we place on ethics and integrity.
- Second, having the right policies and procedures.
- Third, effective and continual training.
- Fourth, constant auditing and monitoring.

Quality, accuracy, and thoroughness must come first.

CACI's Role in the Security Clearance Process

Our investigators are expected to conduct their fieldwork in accordance with federal guidelines. We perform internal reviews of all investigative reports to ensure that no background investigation is submitted to the government as complete without first undergoing a thorough internal assessment.

Our role in the overall security clearance process is a limited one. We are assigned an investigation, or a "case," through the Personnel Investigations Processing System ("PIPS"), which also designates a case type (*e.g.*, initial investigation or five-year reinvestigation). The type of case determines the scope of our review, both in terms of depth of investigation and time span covered. Our investigators then conduct their fieldwork in accordance with the OPM Investigators' Handbook for conducting background investigations. After an investigation is

complete, one of our case reviewers evaluates the investigative report for quality, completeness, and to ensure the investigation has been conducted according to federal guidelines. Once the case reviewer determines the investigative report meets all quality standards and federal requirements, the report is submitted to OPM as complete.

To be clear, we do not grant clearances or make recommendations as to who should receive a security clearance. Our primary role in the investigation process is fact finding, ensuring that we conduct background investigations in accordance with OPM guidelines and contract requirements. We provide the results of our investigation to the government for its use in making final clearance determinations.

As indicated earlier, we believe our quality control model is robust. We have internal controls to ensure our case reviewers are conducting exhaustive reviews of the cases assigned to them. We require reviewers to log each step of the review process, and maintain an internal case management system that allows us to more effectively monitor their work. In addition to real time controls, we monitor reviewer statistics on a daily, weekly, monthly, quarterly, and annual basis. We encourage employees to be as thorough as necessary in conducting a case review, and we regularly provide employee training and counseling.

We at CACI are committed to best practices and continuous improvement in the security clearance process. In this regard, we have suggestions related to three areas: one, making the background investigation process more efficient; two, more effectively capturing information; and three, enhancing contractor oversight.

On behalf of my company and as a former active duty Army officer and a security clearance holder for over 30 years supporting the Intelligence Community, I thank you for the opportunity to present CACI's input on these matters and I appreciate the courtesies extended to us by you and your staff during the course of this inquiry. I look forward to answering your questions.

Chairman ISSA. Mr. Phillips.

STATEMENT OF STERLING PHILLIPS

Mr. PHILLIPS. Chairman Issa, Ranking Member Cummings, and members of the committee, my name is Sterling Phillips, and since January of 2013 I have served as CEO of USIS, a Federal contractor headquartered in Falls Church, Virginia. As part of a wholesale leadership change at the company, I joined USIS after more than 30 years in senior management positions with Federal contractors.

I am here today representing more than 6,000 USIS employees dedicated to excellence in supporting the missions of our Government customers. That number includes 2,000 field investigators across the Country who conduct background investigations, as well as nearly 400 of their colleagues involved in assuring the quality of our work.

Over the past nine months, the disclosure of classified material by Edward Snowden and the Navy Yard tragedy caused by Aaron Alexis have caused a great deal to be written and said about the security clearance process in general and USIS specifically. Much of this public commentary has been factually inaccurate. Today I hope to correct these inaccuracies and clarify the role contractors like USIS play in the Nation's security clearance process so as to provide you with better insight as to how this process might be improved.

In order to understand the process, it is critical to recognize that USIS and OPM's other contractors have no role in deciding whether an individual actually receives or retains a security clearance. We only collect and report information, and we do not even make a recommendation. The decision-making process is known as adjudication, and that authority lies solely with the agency requesting the clearance.

All OPM background investigations, whether conducted by contractors or Federal employees, follow specific procedures and protocols established by OPM. Contractors like USIS rigorously adhere to the established investigative process and have no flexibility in terms of how an investigation is conducted.

Once an investigation is complete and accepted by the Government, our work is done and we have no further role in the oversight or monitoring of cleared personnel. In fact, contractors are not allowed to maintain any of the case materials or information, all of which are returned to OPM.

Our performance goals for all cases, including Snowden and Alexis, are to strictly follow the OPM process and to meet all OPM standards for quality in our work. If we ever fail to do so, we are promptly notified by OPM with a detailed description of any defects. All indications to USIS are that we met all standards on each of these two cases.

Mr. Chairman, in my 13 months at USIS, I have been impressed with the dedication and professionalism of our investigators and other employees. They understand that they are performing a sensitive and vital national security function. Many of our investigators came to us from the military or law enforcement. They understand their responsibilities and take them seriously.

It is important to note that all investigations are fixed-price products. USIS has an extensive and costly quality review system, and all of our work is subsequently reviewed by OPM and the adjudicating agency. At any time, the USIS National Quality Team, OPM, or the requesting agency can send the case back for additional work at no extra cost to the Government. The cost to USIS of quality defects and re-work is high. Both short-and long-term, it is in the best financial interest of the company to do the job right the first time.

In any enterprise of this size, however, from time to time there are individuals who fail to meet our high standards, but I submit to you that in USIS those individuals are an aberration, and not the norm.

When USIS suspects that an individual investigator has misrepresented or falsified his or her work product, we immediately suspend that investigator and launch an internal investigation. If our investigation determines that work has been falsified or misrepresented, we proactively report and refer those cases to OPM and cooperate with the U.S. Attorney's Office for subsequent prosecution.

As you know, the U.S. Department of Justice has intervened in a civil false claims suit against USIS. That matter is ongoing and has not been resolved.

I was not at USIS when the alleged conduct in that case occurred, but I can tell you that the allegations in the complaint relate to a small group of individuals over a specific time period and are inconsistent with our values and strong record of customer service. Since learning of these allegations nearly two years ago, the company has acted decisively to ensure the quality of USIS work and compliance with OPM requirements. New leadership has been installed, oversight has been enhanced, and internal controls strengthened. From the outset, the company has fully cooperated with the Government's investigation and will continue to do so.

Finally, I hope this hearing is helpful to you as you assess possible policy changes in America's security clearance process. USIS and our 6,000 employees are prepared to assist you in any way that we can. Thank you.

[Prepared statement of Mr. Phillips follows:]

Testimony of Sterling Phillips
Chief Executive Officer
USIS

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

My name is Sterling Phillips, and since January 2013, I have served as CEO of USIS, a federal contractor headquartered in Falls Church, Virginia. As part of a wholesale leadership change at the company, I joined USIS after more than 30 years in senior management positions with Federal contractors.

I'm here today representing more than 6,000 USIS employees dedicated to excellence in supporting the missions of our government customers. That number includes 2,000 field investigators across the country who conduct background investigations, as well as nearly 400 of their colleagues involved in assuring the quality of our work.

Over the past nine months, the disclosure of classified material by Edward Snowden and the Navy Yard tragedy caused by Aaron Alexis have caused a great deal to be written and said about the security clearance process in general, and USIS specifically, in the media. Much of this public commentary has been factually inaccurate.

Today I hope to correct these inaccuracies and clarify the role contractors like USIS play in the nation's security clearance process so as to provide you with better insight as to how this process might be improved.

In order to understand the process, it is critical to recognize that USIS and OPM's other contractors have *no* role in deciding whether an individual actually receives or retains a security clearance. We only collect and report information and we do not even make a recommendation. The decision-making process is known as "adjudication" and that authority lies solely with the agency requesting the clearance.

All OPM background investigations, whether conducted by contractors or Federal employees, follow specific procedures and protocols established by OPM. Contractors like USIS rigorously adhere to the established investigative process and have no flexibility in terms of how an investigation is conducted.

Once an investigation is complete and accepted by the government, our work is done and we have no further role in the oversight or monitoring of cleared personnel. In fact, contractors are not allowed to maintain any of the case materials or information, all of which are returned to OPM.

Our performance goals for all cases, including Snowden and Alexis, are to strictly follow the OPM process and to meet all OPM standards for quality in our work. If we ever fail to do so, we are promptly notified by OPM with a detailed description of any defects. All indications to USIS are that we met all standards on each of these cases.

Mr. Chairman, in my 13 months at USIS, I have been impressed with the dedication and professionalism of our investigators and other employees. They understand that they are performing a sensitive and vital national security function. Many of our investigators came to us from the military or law enforcement. They understand their responsibilities and take them very seriously.

It is important to note that all investigations are fixed-price products. USIS has an extensive and costly quality review system and all of our work is subsequently reviewed by OPM and the adjudicating agency. At any time, the USIS National Quality Team, OPM or the requesting agency can send the case back for additional work at no extra cost to the government. The cost to USIS of quality defects and re-work is high. Both short- and long-term, it is in the best financial interest of the company to do the job right the first time.

In any enterprise of this size, however, from time to time there are individuals who fail to meet our high standards. But I submit to you that in USIS those individuals are an aberration, not the norm.

When USIS suspects that an investigator has misrepresented or falsified his or her work product, we immediately suspend that investigator and launch an internal investigation. If our investigation determines that work has been falsified or misrepresented, we pro-actively report and refer those cases to OPM and cooperate with the U.S. Attorney's Office for subsequent prosecution.

As you know, the U.S. Department of Justice has intervened in a civil false claims suit against USIS. That matter is ongoing and has not been resolved. .

I was not at USIS when the alleged conduct in that case occurred, but I can tell you that the allegations in the complaint relate to a small group of individuals over a specific time period and are inconsistent with our values and strong record of customer service. Since first learning of these allegations two years ago, the company has acted decisively to ensure the quality of USIS's work and compliance with OPM requirements. New leadership has been installed, oversight has been enhanced and internal controls strengthened. From the outset, the company has fully cooperated with the government's investigation and will continue to do so.

Finally, I hope this hearing is helpful to you as you assess possible policy changes in America's security clearance process.

USIS and our 6,000 employees are prepared to assist you in any way that we can.

Thank you.

Chairman ISSA. Thank you.

I will recognize myself.

Director, we received a list of 450 cities that do not cooperate fully, it is part of an OPM list of cities that simply will not answer questions, in all or in part, as to criminal backgrounds and so on of individuals. We were also given a redacted version, which basically takes out all the names and is useless. Would you agree that the 450 cities not willing to cooperate should be, in the public interest, made available?

Ms. ARCHULETA. Mr. Chairman, there are about 18,000 jurisdictions that exist across the United States that are——

Chairman ISSA. Right, there are 18,000, many of which are not on this list. You have 450 jurisdictions, including, at the time of Aaron Alexis, Seattle, Baltimore, New York, Los Angeles, and Washington, D.C. that were not cooperating. Aaron Alexis was, in fact, somebody for whom OPM had on the list, to our understanding at the time, that Seattle was not going to give you that information that ultimately we didn't have as to the shooting that Aaron Alexis had already done. My question to you is can you give this committee any reason that the names of those municipalities should be withheld from the public.

Ms. ARCHULETA. Those 450 names have been discussed and mentioned, and we would work with you to provide those names of the cities that are not in——

Chairman ISSA. Okay, well, we have a list. We would like to make it public. We believe that it says—and I am respecting the status that was on it—it says "Sensitive Law Enforcement Information for House Use Only" that was stamped on our copy. It is this chairman's opinion that this is information the public has a right to know, that their city is not providing criminal information when somebody is receiving a security clearance, such as Aaron Alexis.

Ms. ARCHULETA. Mr. Issa, we would be glad to work with you to release those names.

Chairman ISSA. Thank you. I appreciate that. As I previously said, obviously, at the time that Aaron Alexis was being checked, Seattle wasn't compliant or participating. Is it possible that, in fact, the inspector—and I am not trying to defend anybody here—the inspector that was doing the sheet looked and said this is on the list of cities that are already not compliant, it is not reasonable for us to go and ask for that record?

Ms. ARCHULETA. I couldn't speculate to the mind-set of the investigator at that time.

Chairman ISSA. Do you believe this committee should empower OPM and the Department of Justice—this question is for Mr. Lewis—to have leverage over cities to ensure that if they are not going to comply, that Federal funds that help them build those very databases be withheld or in some other way use Federal clout to ensure that we do get full information when trying to clear individuals for sensitive information? Mr. Lewis.

Mr. LEWIS. I can't comment on——

Chairman ISSA. Would you like to have tools to see that that happens?

Mr. LEWIS. We would like to have access to that information, yes, sir.

Chairman ISSA. Okay. Well, it is the committee's intention to provide tools to the Executive Branch to encourage that compliance.

For the director, Ms. Archuleta, what have you done in order to reduce the amount of that list. Have you taken, in those three months, any material actions that might cause cities, other than being on a list that we might publicly disclose, to want to cooperate more fully?

Ms. ARCHULETA. Most recently, the District of Columbia has agreed to provide that information and Mr. Miller, as the director of FIS, has been working within the compact to continue discussions with some of those major cities who have not been providing the information. We will continue to pursue that; it is an important relationship and information that would be most helpful in our background investigations.

Chairman ISSA. Thank you.

I have one question that perplexes me a little bit, and it is kind of a billion dollar question here. My understanding, and, Mr. McFarland, you probably know the case history on it, OPM discovered and was working with Department of Justice prior to January of 2011, was aware of the dumping that went on at Mr. Phillips's company, is that correct?

Mr. MCFARLAND. I believe that is.

Chairman ISSA. So the United States Government discovered dumping prior to the filing in Alabama by Blake Perceval of a qui tam case, is that correct?

Mr. MCFARLAND. Yes, that is correct.

Chairman ISSA. And yet when—I put this in the record already, but when the Director of Personnel Manager, OPM Director, said that Department of Justice had filed, that wasn't true. Department of Justice joined the case in which the recipient will be a private individual that will receive large amounts of money if, in fact, there is a payment from Mr. Phillips's company, is that correct?

My question to anyone on the panel is is there any good reason for the Government to discover that they had been wronged by a company and then allow an insider to become a qui tam recipient of millions of dollars because the Government doesn't act, and then have the Government join the case much later with righteous indignation, when in fact, in my review of this case filed by Department of Justice against USIS, all they have really done is asserted the same things previously asserted in the qui tam case. Anyone want to comment on that? Because there are a lot of U.S. dollars that are going to go to outside lawyers and an individual who, in fact, doesn't appear to be the first to discover or have some rights in this case?

Ms. ARCHULETA. Mr. Issa, in April of 2011, Mr. Miller and his staff noticed an anomaly in the cases that were being sent forth from USIS and began a dialogue with USIS to discover why that was happening. They had introduced some new automation that was indicating to them that the number of cases being reviewed were much higher than——

Chairman ISSA. Okay, my time has expired. I just want to very quickly say was that discovery based on Blake Perceval's information?

Ms. ARCHULETA. No, it was not.

Chairman ISSA. So the Government discovered that, in fact, it had been wronged, potentially, and yet we have an individual with a billion dollar qui tam case that the Government is in second position on, is that correct? If I am wrong in any way, I would like to understand that.

Ms. ARCHULETA. Again, I would reiterate that in April we began to uncover that anomaly.

Chairman ISSA. Okay. Well, I am going to take the privilege of referring this over to the committee next door, to Judiciary, because I am deeply concerned that the Government is not, in this case, potentially protecting its own right to get a recovery in its entirety and not share it with a third party.

Mr. Cummings.

Mr. CUMMINGS. Thank you very much. I want to join with the chairman with regard to this whole issue of law enforcement officers cooperating with your agency, Ms. Archuleta. I learned that there were some in my own district, and I am going to be urging them to cooperate. I think this is so very, very important.

I want to go to you, Mr. Phillips. You said something in your written statement and I think you said it in your oral statement, you said, but I can tell you that the allegations in the complaint relate to a small group of individuals over a specific time period and are inconsistent with our values and strong record of customer service. I can understand that; it makes sense. But would you agree that the top people are gone? I mean, they have either been fired or they left, right? They were the ones who were orchestrating this. Hello?

Mr. PHILLIPS. The people associated with the allegations are gone from the company.

Mr. CUMMINGS. Yes, they are gone; they have been either fired or they left.

Mr. PHILLIPS. And they were at multiple levels in the company.

Mr. CUMMINGS. Multiple levels. So, you know, when you say just a few bad apples, I mean, this is a little bit more than that, and we would not have that many people having left. And I don't think the Justice Department would be doing what it is doing if it were just a few bad apples. Now, I am not talking about probably 95 percent of the employees, but when you have key people—and from what we have learned they were key—doing certain things, making certain decisions, you wonder about statements like the one you just made. But we will come back to you.

Director Archuleta, records produced by OPM to this committee show that during the period of the alleged fraud OPM was paying bonuses to USIS for what you thought was very rapid progress in clearing cases. Between 2008 and 2012, OPM paid about $16 million to USIS just for bonuses under these contracts. Director, if USIS was defrauding OPM to meet its revenue targets, and if it met timeliness goals only by not, not doing quality reviews 40 percent of the time, what is OPM doing to recover those ill-gotten bonuses?

Ms. ARCHULETA. The bonuses that were paid to USIS, which were last provided in 2010, were bonuses that were provided to them under the performance-based standards within the contract.

The Government attempting to recover those bonuses is part of the civil action that has been filed, and no bonuses have been awarded to USIS under the current leadership.

Mr. CUMMINGS. So you are saying Justice is trying to get those bonuses back, is that what you are telling me?

Ms. ARCHULETA. Yes, as part of the civil action charging fraud, that is part of the recovery.

Mr. CUMMINGS. Would the staff put up the chart for the USIS bonuses?

[Chart.]

Mr. CUMMINGS. Director Archuleta, we asked the committee to provide us with the bonuses that were paid to employees who were involved in the alleged fraud. Now, here is some of what they told us. You have the chart there. The CEO received almost $500,000 in the first year of the alleged fraud. Director Archuleta, OPM does not approve these bonuses to individual people at USIS, is that correct?

Ms. ARCHULETA. They are performance-based within the contract, and not to individuals, but to the company.

Mr. CUMMINGS. So OPM doesn't decide who gets the check; you just basically make sure that they get money, the company gets money and then they——

Ms. ARCHULETA. Based on its performance.

Mr. CUMMINGS. All right, so let's ask the company.

Mr. Phillips, I know you are relatively new at USIS and I know you have a tough job. You were brought in to clean up this mess. But as the CEO of USIS, you have a boss, do you not?

Mr. PHILLIPS. Yes, sir.

Mr. CUMMINGS. And that boss is Altegrity, the privately held holding company that owns USIS, is that right?

Mr. PHILLIPS. Yes, sir.

Mr. CUMMINGS. Altegrity is a big company, is it not?

Mr. PHILLIPS. The holding company is a relatively small organization.

Mr. CUMMINGS. Well, but through its subsidiaries it has received over $2 billion from contracts from a dozen Federal agencies. That is pretty big to me, $2 billion. Would you agree that is pretty big for the Federal Government?

Mr. PHILLIPS. Yes.

Mr. CUMMINGS. And that is what we have tallied. Altegrity was also the boss of your predecessor, the president and CEO who is alleged to have directed the fraud. Now, he got some big bonuses. My staff asked USIS for the company's bonus policies during the years of the alleged fraud, and what we got back were documents marked "Altegrity." So the bonuses awarded to the top officials at USIS during the alleged fraud were made according to a formula devised by the parent company, Altegrity, is that right?

Mr. PHILLIPS. Yes, sir.

Mr. CUMMINGS. According to Altegrity, bonus formula, between 20 percent and 25 percent of an executive bonus, was dependent upon whether he met his objectives and whether he performed well. So if you are the CEO of USIS, Altegrity determines your bonus, is that right? They determine yours.

Mr. PHILLIPS. Yes, they do.

Mr. CUMMINGS. Who evaluates your performance as the CEO?

Mr. PHILLIPS. Altegrity and the board of directors.

Mr. CUMMINGS. And so do we have any names?

Mr. PHILLIPS. We are in the process of reorganizing Altegrity. The board of directors is comprised of principals with Providence Equity, the owners of the company. So I report directly to the board, today.

Mr. CUMMINGS. So somebody doesn't call you and check on you, the whole board calls you? I mean, how does that work? I mean, somebody is going to make sure you get a bonus, and if you deserve a bonus, I know you are going to insist that you get a bonus. Does that mean you go to the board to ask for the bonus or do you answer to someone?

Mr. PHILLIPS. The board of directors would determine my bonus. We have monthly board meetings, so there is currently—there is no CEO of Altegrity, as there was in the past.

Mr. CUMMINGS. Okay.

Mr. PHILLIPS. So the board does, in fact, to your question, the board does, in fact, evaluate my performance and determine whether I will get a bonus.

Mr. CUMMINGS. Well, who specifically at Altegrity approved the more than $1 million in bonuses for your predecessor, former CEO Bill Mixon, who has been accused of directing this fraud?

Mr. PHILLIPS. Specifically, I do not know who was CEO at the time these bonuses were paid. I would have to look at the timing. There have been a series of CEOs over the last 10 years at Altegrity.

Mr. CUMMINGS. Well, as I close, let me say this. Mr. Chairman, I think that Mr. Phillips's testimony today raises the question about whether or not officials at Altegrity knew about the alleged fraud and when did they know it, and what, if anything, did they do about it. Altegrity is a big Federal contractor through its subsidiaries, and the American people have a right to know just what kind of people are managing those subsidiaries to which the Government gave over $2 billion in recent years.

Now, Mr. Chairman, I would like to put the bonus chart and the list of Altegrity contracts in the record. The bonus chart is right here.

Mr. MICA. [Presiding.] Without objection, the bonus chart will be part of the record.

Mr. CUMMINGS. And the contracts of Altegrity.

Mr. MICA. And the contracts of Altegrity referenced to it.

Mr. CUMMINGS. Thank you very much

Mr. MICA. Thank you. Without objection, so ordered.

Mr. MICA. Okay, let me recognize myself.

Well, we are here because one of the most horrible and failure of some of the systems that we have in place to protect us failed and a lot of people died. Just an incredible tragedy. Some of it is the result of the failure of adequate contract management. We have heard some issues raised about some other failures in contract management. We also have a failure of the security clearance process, obvious in some way. And then if you look at the final action of the depraved individual in this case, a failure of our mental

health system; someone who was troubled obtained a weapon and destroyed the lives of a number of people.

First of all, Mr. Phillips, you said you collect data and you give it to OPM, so you are a data collection agent basically?

Mr. PHILLIPS. Yes, sir.

Mr. MICA. Ms. Archuleta, you have about what, 2.3 million people you do clearance on? Is that annually or is that just——

Ms. ARCHULETA. That is annually, sir.

Mr. MICA. Annually. So that is a huge amount. Just for the record, I was in Congress, actually chaired civil service when we created the initial ESOP. We gave the Federal employees the right to run that initial company, which evolved into Mr. Phillips's company. We now have three companies, private companies, that do 70 percent of the work, is that correct?

Ms. ARCHULETA. Yes, the——

Mr. MICA. It would be almost impossible for OPM to do it all itself, given 2.3 million, so we rely on contractors and contract management to execute those clearances, is that right?

Ms. ARCHULETA. That is correct, sir.

Mr. MICA. Okay, so they are collecting the data. The problem is it is sort of garbage in, garbage out, and we have flaws in the system. We see Mr. Alexis—and I went back and read the report. The 2004 incident he was, really, even if Seattle reported, he was never adjudicated with a felony or even a misdemeanor; the charges were dropped, is that correct, Mr. Phillips?

Mr. PHILLIPS. That is correct.

Mr. MICA. Okay, so then the question is the failure of the system to periodically review folks. Now, he was in the Navy, but he went on to a private contractor, is that correct, too? Are you aware of that, Mr. Phillips?

Mr. PHILLIPS. That is my understanding.

Mr. MICA. Okay. And I see there is a 5 to maybe 15 year review. Do you think that is adequate for these clearances, Ms. Archuleta?

Ms. ARCHULETA. I am very supportive of a continuous evaluation——

Mr. MICA. We should do that. The problem I have is Ms. Ordakowski here, she gave us some recommendations. Technology, we could easily compare the data coming in. We probably should look at some stages, because, again, the ultimate decision, Mr. Lewis, is given by the agency for the clearance, is that correct?

Mr. LEWIS. That——

Mr. MICA. And you gave that. This individual was a Navy person, first got it as a Navy, then he shifted to a contract person, where he committed the deed. Is that correct, Mr. Lewis?

Mr. LEWIS. That is correct.

Mr. MICA. Okay. So I think we ought to look at some point at which there is a re-review. Certainly what the chairman brought up in entities not reporting, again, garbage in, garbage out, we won't know, but I think for improvement we need to look at if they shift positions, the contractor should do a review. It could easily be run through technology, although, dear God, I have the greatest reservation about OPM and technology now chairing the Government Operations Subcommittee, seen $271 million, almost a third of a billion dollar fiasco in trying to just keep the records of Federal

employees for retirement, etcetera. Are now still doing that by hand, ma'am? Do you know?

Ms. ORDAKOWSKI. I do not know.

Mr. MICA. Do you know, Ms. Archuleta? Do you know the failure of trying to institute technology for records for retirement?

Ms. ARCHULETA. That is why I have instituted an IT modernization plan.

Mr. MICA. Okay, well, we spent hundreds of millions and it is a fiasco. This is also back to contract management, the top person at OPM in managing contracts. We have three contracts for these folks; we have contracts for IT. Certainly, technology could give us a better handle on reviewing. You know, people are normal today. Look at this panel, they all look pretty normal, don't they? But they could flip out on you in a few years, particularly some. So we do need some mechanism to review people periodically as they take on new roles. Wouldn't you say that would be good, Ms. Archuleta?

Ms. ARCHULETA. Yes, sir, I would say that.

Mr. MICA. Mr. Phillips, what do you think?

Mr. PHILLIPS. I agree.

Mr. MICA. Don't tie your shoelaces now. What?

Mr. PHILLIPS. No, I agree.

Mr. MICA. Okay.

Mr. Lewis?

Mr. LEWIS. Very much agree.

Mr. MICA. Okay.

Mr. McFarland?

Mr. MCFARLAND. Yes, I agree.

Mr. MICA. Okay. And then we haven't even talked about the failure of mental health. Government employees, be they military, private contractors, do not go out and shoot multiple people. There is something wrong. Again, this individual had incidents of severe mental health problems, and yet obtained a weapon. And we have to look at also how you get a sawed-off shotgun into a Government facility and then kill people.

I would like, also, if you could please provide a copy of the IT modernization plan to the committee. I guess we will ask Ms. Archuleta for that. Can you do that?

Ms. ARCHULETA. It is my intent to discuss the IT modernization plan with the committee, yes.

Mr. MICA. I am over slightly, but not as much as Mr. Cummings.

Let me yield next to Ms. Norton, with trepidation. Thank you. And joy. Good to see you.

Ms. NORTON. All right. Now that that has been corrected, thank you, Mr. Chairman.

You know, this city was somehow spared in 9/11, and there are theories as to how that occurred, yet we were hit very hard at the Navy Yard, and we were hit by a deranged man who, as I understand it, had the second highest security clearance.

Mr. Lewis, is that the second highest security clearance you can get?

Mr. LEWIS. There is secret and top secret, so, yes.

Ms. NORTON. So he was pretty much up there. As we look back over his history, it had some arrests, they weren't reported from Seattle. He was arrested in Georgia for disorderly conduct the

same year that he got his security clearance, apparently; and then in 2010 in Texas for firing a gun through the ceiling of his downstairs neighbor. And then just a month—and here is where the tragedy that we are still feeling in this city is—just a month before the Navy Yard incident, the Rhode Island police were cognizant enough, intelligent enough—I am not sure they knew, in fact, I believe they did not know, because they were called to the hotel, and here is the hotel who had the consciousness, because Alexis had apparently called down saying he was hearing voices. So here we have people without security clearances that understand there was something wrong with this man.

Now, first, let me ask about Alexis's run-ins with the law in Georgia and Texas. Did any part of the Federal Government, Mr. Lewis, did you know, did the Government know about either of these run-ins with the law in Texas and Georgia?

Mr. LEWIS. Well, because there is a 10-year interval between investigations, that information, unless it became known to the commander or supervisor of Mr. Alexis, would not have been reported to the Department of Defense.

Ms. NORTON. Are you saying it was not reported, then?

Mr. LEWIS. That is correct.

Ms. NORTON. Had it been reported, would those incidents have been investigated?

Mr. LEWIS. Upon the receipt of derogatory information, the DOD consolidated adjudications facility would have made a determination does this clearance need to be suspended or revoked; is additional investigation required. So additional action would have been taken.

Ms. NORTON. Well, first of all, as you indicated, this man had a security clearance that enabled him to go for 10 years without review. I can't understand the original set of the 10-year notion. Even the most stable person has incidents in his life in a decade. Where did the 10-year period come from?

Mr. LEWIS. The 10-year period is part of the current Federal investigative standards that are in place today. These standards are under review, most prominently with the suitability and security processes review that is ongoing as we speak.

Ms. NORTON. You are not telling me where it came from. Again, here we have a series of people who have no expertise, who understood that this man probably needed help, and yet the Government sets a 10-year period during which it doesn't have to—I will get to the report in a moment, but it doesn't have to investigate to see if there has been any deterioration in the person. You don't know where this came from. Would you find the paperwork that indicated the rationale for the 10-year period and write that within a 30-day period to the chairman of this committee?

The Rhode Island incident is the most troubling because Alexis was working as a contractor for a company called Experts. Was Experts aware of this erratic behavior?

Mr. LEWIS. Experts did become aware of this information. They were required to report it; they failed to do so.

Ms. NORTON. What has happened to Experts in the meantime? Is Experts still a contractor with the Federal Government?

Mr. LEWIS. I don't know if they are still a contractor, but their security clearance has been adversely impacted. They were invalidated——

Ms. NORTON. Ms. Archuleta, do you know if Experts is still—excuse me?

Ms. ARCHULETA. I apologize. I would rely on Mr. Lewis's assessment of that. It seems that their contract has been suspended. Is that what I heard, Mr. Lewis?

Mr. LEWIS. Their security clearance has been suspended.

Ms. ARCHULETA. Their clearance has been suspended.

Ms. NORTON. So that means they can't do this work any longer. I thank you, Mr. Chairman.

Mr. MICA. Thank you.

Ms. NORTON. It seems clear that—and that is why I asked the report to the chairman—we have to know the basis for the 10 years and we have to assure that there is continuous monitoring of anybody who has a security or a top security clearance.

Mr. MICA. I thank the gentlelady for an excellent line of questioning.

Let me yield to the distinguished gentleman from Ohio, Mr. Turner.

Mr. TURNER. I would like to echo what the chair said. I think Ms. Norton gave us a great description of what we see as the disintegration of the individual and raised two very important issues, on the 10-year evaluation process and also the issue of failure of reporting requirements or failure to report when the requirement existed.

But I would like to do the follow-on, then, to Ms. Norton's line of questioning. I understand that even when you get to the 10-year period and when you get to the review of someone to reaffirm their classified status that there is difficulty with the cooperation with State and local government officials. Now, I served as a mayor for the City of Dayton. I am also on the Armed Services Committee here, in addition to this committee, so the issue of clearances, as we look to Snowden and the other things that are going on, obviously the issue of the Navy Yard is one that gives us a picture of our continuous vulnerability, not just this incident.

But I am concerned that it is my understanding that there are also issues of State and local law enforcement sharing information with the Federal Government in the security process; that although there is a requirement for disclosure and for full cooperation, that, in fact, there may be some impediments.

Ms. Archuleta, if you could please speak on that issue. Do you have State and local agencies, governments that do not take this issue as seriously and that particular at varying levels, and is that an impediment for you?

Ms. ARCHULETA. I wouldn't classify it in just one category; I would say that there are some that have not provided the information, choose not to provide. Others are smaller jurisdictions that, in fact, may not have the capability of providing that information; others, because of just the small size of their jurisdiction, may not have the records that are complete records going several years or many years back. So there are many reasons why local law enforcement agencies are not providing the information, but the most im-

portant part here is that we must take every step, and I would be supportive of looking at how we can work with local law enforcement agencies and the courts to provide this information. This is part of the President's 120-day PAC review and of the Quality Assessment Working Group that is ongoing right now.

Mr. TURNER. Okay, well, even though you sort of side-stepped it there for a moment, I think your answer is still very troubling, so let's back up for a moment and review your answer. You said there are jurisdictions that choose not to share the information.

Ms. ARCHULETA. Yes.

Mr. TURNER. Although you indicated that there are jurisdictions that perhaps don't have the resources, that there are those who just are not sharing the information with you. And I think you would acknowledge to this committee that the information is critical, is it not?

Ms. ARCHULETA. Yes, that is correct, sir.

Mr. TURNER. And then the issue of resources. Although there are communities that would indicate that the period of time of the review may be difficult for them for their record-keeping, we are talking only—we are in present day; we are talking 10-year periods, we are not going to the 1800s, correct? I mean, these are present records that we are asking for information on.

Ms. ARCHULETA. I can't comment as to why they believe their resources aren't there, sir.

Mr. TURNER. I see. It is troubling for you, though, correct?

Ms. ARCHULETA. Yes, it is.

Mr. TURNER. Are you concerned at all that the amount of classified material post-9/11 may be resulting in a proliferation of individuals having clearance; the fact that the data that we now consider to be classified is so voluminous that, in fact, it is pushing the system in providing increased classified status to individuals?

Ms. ARCHULETA. I know that the director of national intelligence is looking at this very serious issue as to the standards for granting clearances and also who should receive those clearances; it is an ongoing review that he takes very seriously and we are working with him in every way.

Mr. TURNER. But you do consider that the amount of classified material certainly is a factor that is pushing, a driver of the issue of the number of classified status——

Ms. ARCHULETA. Who is eligible to receive a clearance is a decision of the DNI.

Mr. TURNER. Ms. Archuleta, is there a difference between the manner in which contractors and Government employees go through the clearance process?

Ms. ARCHULETA. No. The same standards for Federal investigations or background investigations is the same for both contractors and Federal employees.

Mr. TURNER. Going back to the issue of communities that do not participate or choose not to participate, what actions do you take to try to encourage their participation?

Ms. ARCHULETA. We work directly with those jurisdictions and also with our counsels and with other Federal agencies to persuade and encourage their cooperation with our investigations.

Mr. TURNER. Sorry, Mr. Chairman, if I could just one more.

It does inhibit, though, the process, does it not?

Ms. ARCHULETA. We attempt to get as much information as we can, and the records from local law enforcement is very important to us, so, as I said before, I am very supportive of ways that we can encourage these entities to provide us the information.

Mr. MICA. I thank the gentleman and the witness.

We will go to Mr. Lynch, the gentleman from Massachusetts.

Mr. LYNCH. Thank you, Mr. Chairman.

I want to thank the witnesses, as well, for your attendance.

This was a terrible tragedy and I just want to get at the depth of this tragedy. I am going to mention the 12 individuals who were killed during this attack.

Michael Arnold, age 59, had been a pilot with the Navy for many years. He had a wife and two grown sons.

Martin Bodrog, age 54, graduate of the United States Naval Academy at Annapolis. He was a surface warfare officer in the Navy. He left a wife and three daughters.

Arthur Daniels, age 51, left a wife and five children.

Sylvia Frasier, age 53, she had five sisters and a brother. She worked at the Naval Sea Systems Command. She also served as a deaconess and altar counselor at the Rhema Christian Center Church in Washington, D.C. Loved by many.

Kathleen Gaarde, age 62, she worked as a financial analyst at the Navy Yard. She and her husband had an adult son and daughter.

J.J. Johnson, age 73, he was father to four adult daughters and had 11 grandchildren.

Mary Francis DeLorenzo Knight, age 51, she and her husband had two daughters.

Frank Kohler was only 50 years old, left behind his wife and two daughters. He was a big time Rotary Club participant.

Vishnu Pandit, age 61. Mr. Pandit and his wife, Anjali, had become grandparents recently, when one of their two sons had a daughter.

Kenneth Proctor, age 46, left behind a wife and two teenage sons.

Gerald Read, 58, he and his wife, Kathy, have a grown daughter, Jessica, and she has three granddaughters. Well, they have three granddaughters.

And Richard Michael Riggell, age 52. Mr. Riggell was working as a security officer at the Navy Yard, after having worked several years in Iraq on behalf of our Country. His wife and his three daughters remember him as a brave man and a great father.

So this process, this current security clearance process allowed this to happen. It allowed Mr. Alexis to get in there and do what he did.

I have some legislation that I drew up last night, H.R. 4022. It is the Security Clearance Reform Act of 2014. It will introduce a continuous review of security clearances, rather than these period events that we are seeing. It also withholds some Federal funding, a penalty, if you will, for jurisdictions that do not cooperate with us when somebody from their jurisdiction applies for a security clearance from the Federal Government. It also gets at a problem that we had with USIS, which is there was a conflict there. USIS had two contracts, one was an investigative contract and one was

a review, another contract, a support services contract that allowed USIS to review their own work. That is how this was allowed to remain hidden for a long period of time, because the USIS reviewers that were reviewing USIS investigations basically sandbagged the reviews and allowed the dumping to occur. That is a real problem. So the legislation that I have, among many other things, also gets at that issue, that conflict issue.

Mr. McFarland, you are a frequent-flyer to this committee. Sorry to see you here today, but do you think that this dual contract situation, where you have a contractor reviewing its own work, does that contribute to the reduced quality of those reviews and does it introduce a conflict into the system?

Mr. MCFARLAND. It is an absolute conflict, no question about it.

Mr. LYNCH. Okay.

Mr. MCFARLAND. It did quite a job on the quality.

Mr. LYNCH. Okay, thank you. I just want to say that I know we have a lot of partisan issues before this committee sometimes. This is not one of those cases. We have had great cooperation from majority staff and minority staff; we have had great cooperation between the members on both sides of the aisle. This is the way it is supposed to work. We are honestly, I think, embarked on an effort to fix this situation and, like I say, I have some legislation here, H.R. 4022. I would welcome cosponsors from both sides of the aisle and any changes or improvements to that bill would be welcome, and I yield back.

Mr. BENTIVOLIO. [Presiding.] Thank you.

At this time I will recognize myself.

I would like to thank the witnesses for appearing today.

I believe one of the primary tasks of the Federal Government is to maintain our national security. As the tragic shooting at the Navy Yard clearly shows, the clearance process is deeply flawed and the American people have suffered as a result. It is essential that we now determine the best way to fix the loopholes in this process and prevent a tragedy such as this shooting from ever happening again.

Clearance holders must self-report derogatory information that could impact their clearance. In practice, such self-reporting is rare.

Mr. Lewis, are security clearance holders required to report any derogatory information once they have obtained a clearance?

Mr. LEWIS. Yes, they are required to do such self-reporting, as well as their supervisors.

Mr. BENTIVOLIO. What types of information should be reported?

Mr. LEWIS. An example would be bankruptcy, if they are arrested, things of that nature.

Mr. BENTIVOLIO. Do a clearance holder's commanding officers or employers have an obligation to report any derogatory information?

Mr. LEWIS. Yes, they do.

Mr. BENTIVOLIO. How often is such derogatory information actually reported? And I want to emphasize actually reported.

Mr. LEWIS. Sir, we have looked at data that is reported into the DOD system of record for security clearances, and it is in the 50,000 reports a year range. There are many reports of derogatory information.

Mr. BENTIVOLIO. You said 50,000?

Mr. LEWIS. YES.

Mr. BENTIVOLIO. What is the Department of Defense doing to incentivize reporting of derogatory information? You said 50,000 actually reported, but how do we determine what wasn't reported?

Mr. LEWIS. You speak to a fundamental issue, which is partially educating commanders and supervisors as to their responsibilities; and then the second half of that equation would be holding individuals accountable for failure to execute their responsibility.

Mr. BENTIVOLIO. Okay, let's see if I understand this right now. Somebody is hired, they have a security clearance. And it is reviewed how often?

Mr. LEWIS. Currently, at the top secret level it is a 5-year reinvestigation process. At the secret and below level it is 10 years. That is going to be transitioning to a 5-year recurring review. And we do believe that continuous evaluation, ongoing reviews of available records should occur as well.

Mr. BENTIVOLIO. Okay, in the review process are you permitted to check the social media, like Facebook, a person's Facebook, if they have one? What else? Like what is on them on Wikipedia or something?

Mr. LEWIS. Social media is not a tool that is currently being used; however, it is being studied. And one of the challenges of using social media is validating the information that is available on the Web.

Mr. BENTIVOLIO. Okay. And what do you do with the information of a previous investigation that is maybe 10 years old?

Mr. LEWIS. Well, as part of the reinvestigation process, the previous investigation is looked at for any derogatory information there, looking for trends, looking for ongoing concerns; and it is all part of a whole person concept where you look at what has happened in the person's life, what challenges they have faced, whether or not they have had issues with credit or alcohol, and that is part of the adjudicative process.

Mr. BENTIVOLIO. Thank you very much.

The chair now recognizes Mr. Connolly from Virginia.

Mr. CONNOLLY. I thank the chair.

Mr. BENTIVOLIO. Oh, I am sorry. I apologize. Ms. Duckworth.

Ms. DUCKWORTH. Thank you, Mr. Chairman.

The Justice Department's complaint against USIS alleges that between March 2008 and September the company dumped the background investigations by submitting them to OPM as complete for payment, but without ever completing the quality review. We have discussed this, but I am really struck by how massive the scale of this fraud is. Approximately 665,000 cases were dumped over the four and a half year period.

The fact that the Justice Department alleges that USIS dumped cases knowing that there could potentially be quality issues associated with those dumped, we have seen from the Aaron Alexis case the damage that one person can inflict.

Inspector General McFarland, in your prepared remarks you express concern about the overall effect of USIS's alleged fraud. You stated that you believe that USIS's fraud may have caused serious

damage to national security. Can you elaborate that on and why are you concerned?

Mr. MCFARLAND. Yes, I would be happy to. The overall concern that national security is damaged is sometimes hard to find a specific example. I guess a good example that we are dealing with today, though, would be the Aaron Alexis case, because so often you will see the plaque that says if you see something, say something. Well, I think this case is a perfect example of people that saw something, but didn't say anything. And going back to the police department that refused to give a record, even that is awfully hard to understand. I did hear at one time that part of their reason was that they felt it was a liability to give out something if there was not a conviction. Well, I applaud the committee for thinking in the big terms of doing something about it, because it is going to take a big operation to change all of this.

The Navy, as an example, they were told that there was an arrest, and they were also told that he was not truthful on his clearance papers. I would think that that probably should have been enough not to give him a secret clearance; at least to look into it further.

There is a lot of wrongdoing going on; nothing more stunning, of course, than what USIS did. It is just kind of unbelievable to me that somebody can come to work one day and basically call in some supervisor that says, well, we are really going to put the screws to the people now; let's not do this or that, let's just feather our nest. That is just an absolute shame today to have to witness something like that.

Anyway, the bottom line is I hope that the committee can go forward. The draft report that they just finished writing, I think that pretty much says it all about the conditions of things.

Ms. DUCKWORTH. Can you speak to the fact that USIS also performed the quality review for those very same cases that they dumped? So basically you have the single contractor both performing the investigations and then another branch of the same company verifying that they had reviewed. Do you think it is a conflict of interest to have the same company conduct a background investigation and a final quality review?

Mr. MCFARLAND. I absolutely do.

Ms. DUCKWORTH. This is really a very serious concern.

I would like to provide Director Archuleta the opportunity to respond to this. Director Archuleta, do you know whether the 665,000 that were alleged dumped by USIS underwent sufficient quality reviews?

Ms. ARCHULETA. Yes. There is a three-stage, there is a multilayered process for reviewing a background investigation. The contract requires that USIS would conduct its own quality review before sending it on for a final quality review either conducted by the contractor in the support services or by the Federal employee.

With regard to the Alexis case, I might add that both our internal review and the IG's review stated that USIS followed the standards that were in place for the background investigation. However, this does not negate the outrageous behavior that the previous management engaged in during 2008 through 2012 of the dumping of the cases.

Let me just add that last week I took steps to federalize that process so that now only Federal employees are reviewing in that last stage those background investigations.

Ms. DUCKWORTH. Let's hope you get the resources to do that as well.

I am over time. Mr. Chairman, thank you.

Mr. BENTIVOLIO. Thank you.

The chair now recognizes the gentleman from Texas, Mr. Farenthold.

Mr. FARENTHOLD. Thank you very much, Mr. Chairman. I have two areas I want to hit on.

Ms. Archuleta, we have heard a lot of questions and testimony with respect to local authorities not providing the level of information that you guys are needing. Could you tell the reasons for that? I understand some may be financial. Are there other reasons they are not giving that information?

Ms. ARCHULETA. Yes, sir. Sometimes they choose not to; other times resources are unavailable for them to do so.

Mr. FARENTHOLD. As a former member of the Homeland Security Committee, we do a lot of grants to local police departments. It seems like if they don't want to help us, we might be a little bit more reluctant to help them. Would you have a problem with us withholding all or some funds to police departments that don't cooperate?

Ms. ARCHULETA. I am supportive of making sure that we can get these records; it is a very important part of our background investigations and I know that the work of this committee, as well as the President's PAC, is looking at this very serious issue.

Mr. FARENTHOLD. As far as the overall guidelines—and I don't mean to rush; I have a limited amount of time. With respect to overall guidelines, do you know the date of the guidelines for what is done in a background check? When were those last reviewed, the procedure and what is checked?

Ms. ARCHULETA. I don't know, sir, but I would be glad to get that for you.

Mr. FARENTHOLD. As part of the background check, do you all Google the person?

Ms. ARCHULETA. The use of social media is a technique that is being reviewed right now and recommendations have been provided by the DNI and supported by OPM.

Mr. FARENTHOLD. But currently you don't check——

Ms. ARCHULETA. They are under review right now.

Mr. FARENTHOLD. Or news stories on Google or anything like that?

Ms. ARCHULETA. I think just making sure that the quality and the validation of that information is secure.

Mr. FARENTHOLD. All right, let's talk a little about the ongoing investigations. We have heard several people list some of Mr. Alexis's very questionable behavior; shooting out his ceiling and an arrest and some other issues there. There is nothing in place now, right, to do that? The only way you were to find out about it is if he self-reported?

Ms. ARCHULETA. That is exactly right, sir.

Mr. FARENTHOLD. Now, doesn't the FBI get information about arrests and convictions, and things like that, automatically? Are you aware of that?

Ms. ARCHULETA. I am not aware of that, sir. I would be glad to find out for you.

Mr. FARENTHOLD. All right. You know, there is no routine ongoing checking somebody's credit score. You get in trouble, you are susceptible to corruption by a foreign government or whatever. So there is no ongoing as easy as a credit score.

Ms. ARCHULETA. There are credit scores, but there is not continuous evaluation. So once the first background investigation is conducted, in Mr. Alexis's case it would be 10 years later. But the issue of continuous evaluation is one that is very important to me and to the President's PAC, as well as the ODNI.

Mr. FARENTHOLD. It seems like that is something that could, at a very simple level, be automated. You have their name, you have their date of birth, you have their social security number. Okay, after Healthcare.gov, I am questionable about the Government's ability to automate anything or compute its way out of a paper bag, but that seems like a relatively trivial——

Mr. Phillips, your company does background checks, albeit we had some issues there. But is that something you all could easily automate, you think?

Mr. PHILLIPS. Are you asking about the——

Mr. FARENTHOLD. Just checking somebody's credit score on a regular basis or polling databases to see if somebody's name pops up.

Mr. PHILLIPS. In my view, that would be a fairly straightforward application of technology to continuous monitoring.

Mr. FARENTHOLD. Mr. McFarland, you are the IG there, you have your hands in the water. You have some other things that can really easily and inexpensively be done to do ongoing checks?

Mr. MCFARLAND. Well, the point that you just made about isn't there someway you can reach out, I think the FBI, they collect a tremendous amount of arrest records throughout the Country——

Mr. FARENTHOLD. Mr. Lewis, you are with the DOD. The holding of a security clearance isn't a right, it is a privilege. We don't have to wait until something is finally adjudicated, whether you are convicted or not. Shouldn't an arrest be enough to just raise a red flag?

Mr. LEWIS. Certainly there is information in arrest records that is worthy of consideration for whether or not someone should continue to have a clearance.

Mr. FARENTHOLD. And sometimes between arrest and conviction could potentially be years. Meanwhile, that person still has access to sensitive information, is that not correct?

Mr. LEWIS. That is a concern, very much so.

Mr. FARENTHOLD. All right, I see my time has expired, but I do want to join with the other side of the aisle and the rest of this committee in coming up with a solution to give you guys the tools that you need to help keep our Country safe and make this process much more streamlined, much more automated, and much more responsive to the needs so we avoid another tragedy like Navy Yard.

I yield back.

Mr. BENTIVOLIO. Thank you.

The chair now recognizes the gentleman from Virginia, Mr. Connolly.

Mr. CONNOLLY. Thank you, Mr. Chairman, and welcome to our panel.

Mr. McFarland, we had a colloquy earlier between Ms. Archuleta and the chairman of 450 municipalities or jurisdictions that do not exchange information, background information with us when we are doing a security check-in. One wonders what could go wrong with that. So, for example, if they are not exchanging information with the Federal Government on a background check, could that mean that arrest records are not known at all?

Mr. MCFARLAND. Yes, that is right.

Mr. CONNOLLY. Could it mean that somebody is a child predator and we don't know that at all?

Mr. MCFARLAND. That is correct.

Mr. CONNOLLY. There could be some kind of recorded deviant behavior and we wouldn't know that at all.

Mr. MCFARLAND. That is correct.

Mr. CONNOLLY. Well, that is an extraordinary hole in the system, is it not?

Mr. MCFARLAND. It truly is.

Mr. CONNOLLY. I would remind my Republican friends who raised the question of maybe we should make certain kinds of Federal assistance contingent on their full cooperation, a desirable goal, but in light of the Supreme Court ruling in the Affordable Care Act on Medicaid, that tactic of encouraging cooperation may, in fact, be unconstitutional. So we may have to look for other ways to do that.

Ms. Archuleta, I assume you share Mr. McFarland's concern that this is a big hole in the system.

Ms. ARCHULETA. Yes. And that discussion, sir, as I mentioned before, is happening right now within the President's PAC, as well as within the Quality Assessment Working Group that includes OPM and the DNI.

Mr. CONNOLLY. The Democratic staff have done a report I have just seen, and I haven't had a chance to go through it all, but I guess the question that this raises for me is where was OPM, though? It seems to me that one of the things we focused on, an admirable goal, was the backlog problem. Do you want to remind us what the backlog was?

Ms. ARCHULETA. Oh, I am sorry, sir. I wasn't here at the time and I don't remember the number.

Mr. CONNOLLY. Mr. McFarland, do you remember?

Mr. MCFARLAND. I assume you are speaking of the retirement backlog?

Mr. CONNOLLY. Well, also just the backlog on security clearances. One of the goals of OPM was try to reduce the backlog.

Mr. MCFARLAND. Yes.

Mr. CONNOLLY. It was quite considerable.

Mr. MCFARLAND. I think it was.

Mr. CONNOLLY. And so maybe we focused so heavily on that metric. The ranking member put up the bonus chart for former executives of this organization that we had outsourced to, but they were

getting bonuses because that was the metric they were being measured by, was it not? Ms. Archuleta?

Ms. ARCHULETA. I am sorry, sir. The metric was timeliness and quality.

Mr. CONNOLLY. But weren't we also pressing heat into that backlog?

Ms. ARCHULETA. I am told that it was about half a million in the backlog.

Mr. CONNOLLY. Right.

Ms. ARCHULETA. The result of which we were trying to reduce that backlog so that Government could continue with employees that were seeking that clearance.

Mr. CONNOLLY. When Ronald Reagan was going to Iceland, he invoked a Russian expression, dovre noprovre; trust, but verify. It looks to me, in this case, that OPM fell down on the job of the verify piece. I mean, if you are going to be looking at sort of rapid delivery of security clearances, where is the random auditing to make sure they are what they say they are supposed to be?

Ms. ARCHULETA. I would just mention, sir, that during the process, it is a multilayered process, and all of those cases that were dumped went through another review; they didn't go directly from the contractor to the adjudicator, but there was a third and final review, or second and final review was taken.

Mr. CONNOLLY. But for years we weren't catching the fact that people were dumping.

Ms. ARCHULETA. The egregious behavior of USIS in hiding this is is part of the justification for the civil suit that is being conducted right now.

Mr. CONNOLLY. But irrespective of a civil suit, how are we going to correct it, moving forward? What are the measures you are putting in place to safeguard the fact that nobody can do that again, at least not easily.

Ms. ARCHULETA. Well, once we learned that there, in fact, had been this behavior, we took immediate steps for strengthening our oversight. We now conduct oversight on——

Mr. CONNOLLY. Ms. Archuleta, my question, though, was what was the oversight at the time. It seems like it was pretty thin.

Ms. ARCHULETA. I wasn't here at the time, sir, but I can comment, going forward, that I am doing everything I can——

Mr. CONNOLLY. No, Ms. Archuleta. My question is about what went wrong. How are we going to correct it moving forward if we don't understand what went wrong, from the Federal Government's point of view, from OPM's point of view, or from our point of view about OPM? We were relying on OPM to manage this. It is not good enough to say I wasn't there, so I can't answer any of that.

Ms. ARCHULETA. No, I agree with you, sir. But I have to take a look at what I can learn from what happened, as you mentioned, and, going forward, how I can prevent that from happening again.

Mr. CONNOLLY. Forgive me, Mr. Chairman, just pressing this one more time.

Is it your view, Ms. Archuleta, and I know you are new on the job, that something went terribly wrong and that we do need to put corrective measures in based on what went wrong——

Ms. ARCHULETA. Absolutely, sir, I agree with you.

Mr. CONNOLLY. Okay. I thank you and I thank the chair.

Mr. BENTIVOLIO. Thank you.

The chair now recognizes the gentleman from Georgia, Mr. Woodall. No questions?

Mr. Lankford?

The chair now recognizes the gentlelady, Ms. Kelly.

Ms. KELLY. Thank you, Mr. Chair.

Good morning. The most frequent question that has been asked about the Aaron Alexis incident is how this young man could have received a security clearance in 2008, given his 2004 gun-related arrest in Seattle.

Mr. McFarland, I understand that your office reviewed the background investigation conducted on Alexis by USIS and found that a copy of the police report was not included in the investigation. Can you explain for us why the police report was not included in the investigation report?

Mr. MCFARLAND. Well, my assumption is that the history of the Seattle police department to provide that type of information was that they would not get it, so OPM or the Federal investigative service had created what they referred to as a workaround, allowing the investigator to take other avenues of approach, such as databank information; and that is the reason that they didn't come up with the information on the gun. But I also understand that the police department was hesitant to give any information out because of liability concerns if there wasn't already a conviction attached to it, and in this case there was not a conviction at that point.

Ms. KELLY. And, Mr. Lewis, is it possible that if details of the 2004 gun-related arrest had been included in his background investigation report, he may not have received a secret level clearance?

Mr. LEWIS. That sort of information could have led to the denial of his clearance.

Ms. KELLY. Director Archuleta, is the Seattle police department one of a number of State and local jurisdictions that does not cooperate with investigative requests for criminal history information?

Ms. ARCHULETA. Seattle is now cooperating.

Ms. KELLY. Oh, they are now cooperating?

Ms. ARCHULETA. They are now cooperating, since 2011.

Ms. KELLY. Since 2011. And how many are on that list, what was that number?

Ms. ARCHULETA. It is about 450.

Ms. KELLY. And do you see any of the others changing like Seattle?

Ms. ARCHULETA. As I mentioned, the District of Columbia has recently come on board as a cooperating law enforcement district.

Ms. KELLY. That is just one out of many.

Ms. ARCHULETA. We are working very closely with others to persuade them to participate.

Ms. KELLY. Okay. How do we address situations like the Alexis case, where the workaround apparently did not capture some of the very critical information?

Ms. ARCHULETA. I think there are two issues that you raise here. The first one is with the continuous evaluation, so that we are getting this information not once every 10 years, but we are contin-

ually provided information about anyone who holds a secret or top secret clearance. Secondly, I think it is the relationships that we have with the local law enforcement agencies, and that needs to be strengthened, and I look forward to working with this committee in support of that.

Ms. KELLY. And, panel members in general, there is existing Federal law that requires State and local law enforcement agencies to comply with a request for criminal history information, but there is no enforcement mechanism under that law. Ranking Members Lynch and Cummings have introduced legislation that would strengthen compliance, or at least disincentivize noncompliance. Do you agree that there is need for such legislation? Any of you.

Mr. RHODES. Yes, we absolutely concur with that.

Ms. ORDAKOWSKI. We do as well.

Mr. MCFARLAND. Also agree.

Mr. LEWIS. We need to get the information, that is true.

Ms. ARCHULETA. I think the Administration, working with this committee, would be very interested in reviewing such legislation.

Mr. PHILLIPS. And we would welcome anything that would increase the cooperation with local law enforcement.

Ms. KELLY. I know we are here today talking about secret level clearance and how this person got it and we didn't know his background, but I also feel, not to do with you guys, but that also speaks to the importance of background checks, period. So thank you.

I yield back.

Chairman ISSA. [Presiding.] I thank the gentlelady.

We now go to the gentleman from Oklahoma, Mr. Lankford.

Mr. LANKFORD. Thank you, Mr. Chairman, and thank you all for being here for the long day. You have gone through a lot of questioning already.

I have a couple questions just on insourcing once we get to the OPM process. Obviously a lot of this was taken out of OPM and moved to private contractors, 70 percent of it back in the 1990s. Now there is some thought about does it need to move back into it. I would like to ask the director what your thoughts are about that. Do you believe the Federal security clearance background investigations performed by OPM employees, do you think they should be performed solely or mostly, I would even say, by OPM employees, or do you think the current model of outsourcing is a good model still?

Ms. ARCHULETA. As I mentioned earlier, sir, the enormity or the large numbers of clearances requested and background investigations that are conducted by OPM is a very large number, and I don't think that right now there is the numbers with Federal employees within FIS to conduct those, that is why we rely on contractors to assist us.

Mr. LANKFORD. So it should continue, in your perspective; not what it is now, but that should continue?

Ms. ARCHULETA. I believe that with strong quality performance standards that we could rely on contractors to help us.

Mr. LANKFORD. Okay. Have a question as well, again. Before OPM sends the background investigation files out to the client

agencies, there is a final quality review to ensure the file is complete, is that correct? I am tracking with that correctly?

Ms. ARCHULETA. Yes, that is correct.

Mr. LANKFORD. What percentage of those files are returned back to OPM by the client agencies because the file is incomplete?

Ms. ARCHULETA. About one percent.

Mr. LANKFORD. Okay. Can you explain just that quality review process, how that works, mechanically?

Ms. ARCHULETA. Yes. After a background investigation is completed, the contractor is required to perform a quality review. Once that quality review is completed, it is sent to OPM or FIS, and another quality review is conducted. It is sent then to the adjudicator, who then reviews all of the information, determines whether a clearance will be given.

Mr. LANKFORD. Thank you.

Mr. Lewis, can I ask you that same question? What percentage of cases do you estimate that you get from OPM that are incomplete?

Mr. LEWIS. There are two layers to that. The cases that get rejected back to OPM are about a one percent rate. There are cases that come through that are missing information, but they are not missing information because OPM failed to carry out a complete investigation; they are instances where employers refused to talk to the OPM investigator and give information. So it is greater than the one percent, but——

Mr. LANKFORD. Give me a guess on a percentage there.

Mr. LEWIS. The last number I heard was in the 30 percent rate. But, again, these are instances where the failure of a source to provide information was adequately documented and we were able to continue with——

Mr. LANKFORD. So what do you do with that? How do you finish that out? Obviously, you have an incomplete file. Can you give me an example of something that might be missing from that? And then what do you do with it?

Mr. LEWIS. Well, for example, at the top secret level there is a requirement for neighborhood checks, and particularly in this area people move and there may not be anybody who knew the subject of the investigation who is available, so we have given guidance to the DOD consolidated adjudication facility, which identifies the types of information which may not be available and which would still allow the DOD CAF to do their adjudication.

Mr. LANKFORD. But you are saying right now, once you get it over, you are still able to navigate that.

Mr. LEWIS. Yes.

Mr. LANKFORD. Okay.

Mr. Rhodes, can I ask you just a question about OPM investigations for a contract investigator if there is a misconduct issue? Sometimes that investigation occurs and it is my understanding that sometimes you don't even know that a person is being investigated that you have contract responsibility for. Is that correct or not correct?

Mr. RHODES. That is correct.

Mr. LANKFORD. Then my understanding is that at some point you get a bill, when you find this has occurred; they have done an in-

vestigation, you get billed for the investigation, there is misconduct that has occurred with someone that is under your purview as well. I would like to know just how you handle that, how you process that as a contractor that is trying to oversee people. How would it improve your workflow to be able to be in the loop on that?

Mr. RHODES. Thank you, sir, for that question. If there is a—and typically it will be identified by us, that there may be a falsification of data through the rigorous quality processes that we have in place within CACI; a series of re-contacts, re-checks, re-record checks. So if that is suspected, by contract terms, we report that to OPM immediately within 24 hours. OPM makes the decision what to do with that person. If, in fact, there is further investigation that is required, essentially at that point, and you are correct, sir, that we basically get the bill for the amount of re-work that is required, yet we don't have insight into that. We have requested additional details to allow us to have insight into what the support data is on that. We welcome additional detail on that when we do get those bills.

Mr. LANKFORD. Just the detail of what the cost is, you are saying? So not just being in the loop in it, but actually getting a detailed here is what I am paying for?

Mr. RHODES. Absolutely, yes, sir.

Mr. LANKFORD. Okay. Thank you.

I yield back.

Chairman ISSA. I thank the gentleman.

We now go to the gentlelady from California, Ms. Speier.

Ms. SPEIER. Mr. Chairman, thank you, and thank you to all of the witnesses for your participation today.

Let me start off by asking Mr. McFarland if you would like to clarify a statement you made earlier. Did OPM know about the fraud before the whistleblower filed their lawsuit?

Mr. MCFARLAND. Actually, the Government was not aware of the extent of the fraud until the qui tam was filed in July of 2011; and then our office came into that information August of 2011.

Ms. SPEIER. So what is really clear to me in general is that we have a contractor that had two contracts that created a conflict of interest, they knew it created a conflict of interest, they used it to their advantage, and the penalty imposed upon them is to continue to have a contract with the U.S. Government.

Let me start with you, Director Archuleta. My understanding is that they circumvented OPM's oversight of their performance in quality review. This is a statement made during the audit: I am not splitting hairs, but they knew how we were auditing; they knew what kind of reports we generated to oversee that we were actually performing the activity, so they circumvented our oversight process and they falsified records to help do that.

Why did OPM allow USIS to hold both contracts?

Ms. ARCHULETA. The first contract on the background investigations was split between USIS, CACI, and KeyPoint, and then the support contract was only bid by USIS.

I might just mention as well that as soon as we found out about the egregious behavior, we took immediate action.

Ms. SPEIER. So USIS no longer has the support contract, is that correct?

Ms. ARCHULETA. I took action last week to federalize that, the support contract.

Ms. SPEIER. All right. But why would we initially have done it in the first place? It is just a fundamental conflict of interest. Whether it is acted upon or not, it creates an environment so that the kind of activity and the dumping of 40 percent of these reviews was able to take place for over four years. So why would we ever do that?

Ms. ARCHULETA. I don't disagree with you and, as I stated, I took action to change that.

Ms. SPEIER. So can we agree that you will never have a support contract being provided to an entity that also has a function?

Ms. ARCHULETA. I believe that the review of quality has to be done by FIS, and I would agree with you on that.

Ms. SPEIER. By that you mean by the Federal Government or by a third party?

Ms. ARCHULETA. By the Federal Government, the Federal Investigative Services of OPM.

Ms. SPEIER. All right. Has anyone done an analysis—I think Mr. Lankford was pursuing a set of questions about continuing to privatize some of this function. He and I may disagree a little bit, but has anyone done an analysis to see how much we spend with private contractors that the market seems ready, willing, and able to invest in—private equity is all over USIS and others—versus doing it internally? I don't think we pay bonuses of $375,000. And this is bonuses the taxpayers of this Country paid to these contractors. Let's be really clear about it. This isn't money coming out of their pockets, it is money coming out of the taxpayers.

So have you done an analysis to see whether or not it is actually cost-effective to continue to privatize some of the reviews?

Ms. ARCHULETA. To my knowledge, there hasn't been such an analysis.

Ms. SPEIER. So why wouldn't we do that?

Ms. ARCHULETA. I would certainly like to discuss that with you further.

Ms. SPEIER. Mr. Chairman, I think before we continue to privatize the function—I think if we ask the American people do you think that private contractors should be determining whether or not top secret clearances are given to various contractors and various Federal employees, they would probably be alarmed to know that we privatize that function. But, more importantly, at the very least we should determine whether or not it is cost-effective.

Chairman ISSA. I agree. If the gentlelady would yield. I agree with the gentlelady that we should do a thorough review of the history that began, quite frankly, in the Clinton Administration, when this was originally outsourced, and I would look forwards to working with the lady both on the effectiveness and the cost. USIS, as you know, was spun off, effectively, from an in-house service, and the idea that we should periodically look at a program.

I also share with the gentlelady that although I do not object to a potential contractor doing the review, there needs to be real separation between those doing something and those auditing something. And the same should be true, as you know, in my opinion,

when Government entities audit themselves. We need to have a level of independence of those auditors.

Ms. SPEIER. Thank you, Mr. Chairman. Reclaiming my time.

I am also concerned that we are wimps in the Federal Government, that even when we are taken to the cleaners by contractors, we go back for more, and that there aren't any penalties that are imposed of any significance.

So my question to you, director, is has USIS or Experts been penalized at all?

Ms. ARCHULETA. The civil case against USIS is requesting treble damages, up to treble damages.

Ms. SPEIER. Are there no administrative actions you can take, fines that you can impose?

Ms. ARCHULETA. We have withheld all of the bonuses since 2010 and, as we move forward with this case, we will be working closely with DOJ.

Chairman ISSA. The gentlelady's time has expired. I thank the gentlelady.

We now go to the gentleman from Georgia, Mr. Woodall.

Mr. WOODALL. Thank you, Mr. Chairman. I would like to yield my time to you, if I may.

Chairman ISSA. I am deeply pleased to accept that.

Following up on a couple of questions for the director. One question is can you fire a Federal employee at will, any time, if they did similar failures to perform to what Mr. Phillips's employees did?

Ms. ARCHULETA. The merit system protects Federal employees and there is a process where there is——

Chairman ISSA. Just shortcut it for this committee that is familiar with it. Mr. Phillips's 20 people have been fired. They could be fired or forced to resign at a moment's notice. Isn't it true that every one of his employees, each of these contractor's employees you could individually disqualify without any lengthy administrative process, thus that, if you see wrongdoing by any of these contractor's individual employees, you can terminate their ability to work on these contracts?

Ms. ARCHULETA. Each of the contractors that were accused of this egregious behavior were immediately suspended from the contract.

Chairman ISSA. I think that is an important thing for Ms. Speier, is that the flexibility of your quickly taking somebody out who even slightly loses your confidence is something you have within the contractor industry where, quite frankly, people would be on administrative leave with pay for a long period of time, at best, and you would be denied their services but still paying, isn't that true?

Ms. ARCHULETA. The merit system protects Federal employees, as you know, sir.

Chairman ISSA. Okay. I will take that as a yes.

Mr. McFarland, I want to make sure the record is clear, and I think it isn't clear. Ms. Speier asked you a question about the investigation in which your answer implied to me that Mr. Blake Perceval brought the case before you understood the magnitude. Is that correct?

Mr. MCFARLAND. Yes, before we understood the magnitude, yes.

Chairman ISSA. Okay. I would like to bring your attention to an April 4, 2011 document, and I would ask unanimous consent it be placed in the record. It is to the USIS VP Field Operations, Mr. Robert Calamia, and it bears Steven Anderson's signature, the Branch Manager, Federal Investigation Oversight Branch. Are you familiar with that letter?

Mr. MCFARLAND. No, I am not.

Chairman ISSA. Well, we will have a copy given to you. In a nutshell, on April 4, 2011, the United States Office of Personnel Management lays out a serious complaint, not necessarily all the 650,000 or four years, a serious complaint, and you are talking about thousands of these dumpings. And the reason that I am so concerned that the Government is getting a bad wrap on this qui tam case is one of the cc's is Mr. Blake Perceval. So he is cc'd about a major investigation, a deep area of concern that OPM has discovered on April 4. Three months later he files a billion dollar lawsuit.

I will give you a copy of that, and I would like to follow up after you have had a chance to look at it. But from what I can tell, OPM notified the complainant of their deep concern and an open investigation. He seized on the magnitude of it ahead of time, but not on the basic discovery. Since Abraham Lincoln, qui tam cases were intended to discover that which would otherwise not be discovered, not simply to amplify, prosecute, and benefit financially by it. It is a deep area of concern. I have to tell you if Mr. Phillips's company owes us $1 billion, I want the billion dollars. But, quite frankly, I don't want to share it with somebody who was cc'd on a letter three months before they filed the case. At least on the surface this kind of thing should be a deep concern to all of us.

Chairman ISSA. With that, I have probably only one other question.

Mr. Rhodes, there have been a lot of questions. Mr. Phillips's company is in the spotlight, but isn't it true that, in fact, the level of flexibility and cost, and the ability to up—also for Ms. Ordakowski—your companies can scale up to meet demand quicker than the Federal workforce, isn't that true?

Mr. RHODES. Yes, sir.

Ms. ORDAKOWSKI. Yes, sir.

Chairman ISSA. And if, tomorrow, we were to have a reduction in the level of need, you would also lay people off immediately, isn't that true?

Ms. ORDAKOWSKI. Yes.

Mr. RHODES. Yes, sir, and we have.

Chairman ISSA. During the shutdown, the so-called shutdown of the Government, were your people paid?

Mr. RHODES. Sir, we typically have a backlog of cases that range about two months, so we were pressing down on that and coming close to actually having no backlog.

Chairman ISSA. So you continued to work without an assurance of being paid, is that correct?

Mr. RHODES. Yes, sir, to meet the mission.

Chairman ISSA. And you only got paid for work done. Had we not authorized it when we opened back up, you wouldn't have been paid.

Mr. RHODES. That is correct, sir.

Chairman ISSA. Okay. Did either of your companies, any of the three companies lay anyone off?

Mr. RHODES. We were close at that time; we were working down our backlog. But I do not believe specifically because of the shutdown we laid anyone off.

Chairman ISSA. Okay. So I just want to make it clear, if you had furloughed anybody, they wouldn't have been paid even when we turned back on, because they wouldn't have accomplished work. You are only paid for work you do, not for days in which people are employees, but laid off.

Mr. RHODES. Yes, sir.

Chairman ISSA. True of all your companies?

Ms. ORDAKOWSKI. Yes.

Mr. PHILLIPS. Yes.

Chairman ISSA. Okay. I want to make that clear because it is very, very clear that Federal workers are not an easily raised or lower level, and I share with the director the desire to make sure that the stable force, the long-term force of people auditing and reviewing are inherently governmental. I want to be a little careful not to rush to bring everything in-house when, in fact, we are not very good in the Federal Government at increasing or reducing workloads the way your companies can be asked to do.

For the director, is that pretty consistent with your view of best case for OPM? You mentioned earlier that you were not in a position to take on all the workforce if you were to eliminate these contractors.

Ms. ARCHULETA. I think there is a critical balance the work that the Federal employee can perform, as well as in partnership with private contractors.

Chairman ISSA. I thank the gentlelady.

We now go to the gentlelady from New York.

Mrs. MALONEY. Thank you.

There are allegations of fraud. This is serious allegations. I am wondering are we looking at a case of too big to suspend? You have suspended workers, but you haven't suspended the company. And I understand that grounds to suspend is that the contracting officer could suspend the contract due to fraud, and by all indications it appears that fraud is there. Would anyone like to answer that? Ms. Archuleta?

Ms. ARCHULETA. USIS has taken the steps to remove all those individuals who were——

Mrs. MALONEY. I said that, they removed people.

Ms. ARCHULETA. They removed them and we——

Mrs. MALONEY. But it was the company and the atmosphere in the company that allowed this to happen. May I just read one internal email from April 2010? It stated, "Shelves are as clean as they could get. Flushed everything out like a dead goldfish." Were you aware of this email?

Ms. ARCHULETA. No.

Mrs. MALONEY. Was anyone aware of this email?

Mr. MCFARLAND. I was aware of it.

Mrs. MALONEY. You were aware of it. And seeing that evidence today, do you believe that USIS was honest with OPM, Mr. McFarland?

Mr. MCFARLAND. No, I don't believe they were honest at all.

Mrs. MALONEY. Do you think they were honest, Ms. Archuleta?

Ms. ARCHULETA. USIS, at that time, was not honest and had worked and engaged in fraud.

Mrs. MALONEY. So why in the world are we continuing this contract with this company? Is it too big to suspend? Who could suspend this, the contracting officer, Mr. McFarland?

Mr. MCFARLAND. Yes, the contracting officer could do that.

Mrs. MALONEY. Is the contracting officer on the panel?

Mr. MCFARLAND. No.

Mrs. MALONEY. Well, is there a concrete standard that we have that would point out when something could be suspended?

Ms. ARCHULETA. The procurement officer and the design of the contract holds the contractor accountable, and that is why we were able to remove the individuals who conducted this egregious behavior and why we have been able to take immediate steps to——

Mrs. MALONEY. Well, I would say the contracting law, as I remember it, says contracts can go to responsible bidders. Does anyone think that USIS has been a responsible bidder in this? Does anyone think they have been a responsible bidder in any way, shape, or form?

Mr. PHILLIPS. May I respond to that?

Mrs. MALONEY. Sounds like they were defrauding the Government.

I just have another question. I want to make sure I get my questions in before yielding to you, Mr. Phillips.

There is a system, actually, I wrote the law, called VENDEX, where you have to check the performance of contractors before you award a contract; and in that is whether or not they meet the contract criteria, whether or not they get the contracts done on time, whether they have cost overruns repeatedly, if they have a track record. I wrote this after a $25 million contract was given to a company that didn't exist when I was on the city council in New York. I am not kidding. So it just basically looks at the performance.

And at the very least, Mr. Chairman, we should have part of the VENDEX file whether or not they defrauded the Government. I would say that this is a grounds of not being a responsible contractor.

Now, I understand that this is a big company; you spun off from the Government. So my basic question is do you think that they are too big to be suspended, Mr. McFarland.

Mr. MCFARLAND. No, I don't think that they are too big to be suspended; I think they could be suspended and others would take over. But there would be an interim of a problem area, for sure. But I don't know that that would be enough to suggest that they shouldn't be suspended.

Mrs. MALONEY. Well, they created a national security threat.

Mr. MCFARLAND. Yes, I agree.

Mrs. MALONEY. Absolutely created a national—I would call that very serious.

Mr. MCFARLAND. It is very serious.

Mrs. MALONEY. Extremely serious. And I think at the very least this performance should be tagged on their VENDEX review and that anybody who gives them a contract has to expressly say why

in the world are they giving it to someone who defrauded the Government and created a national security threat to our Country.

Anyone else like to comment on this?

Mr. Phillips?

Mr. PHILLIPS. Thank you. When these allegations—and, by the way, they are just allegations at this point, we have not had our day in court. When these allegations first came to the company's attention in January of 2012, the company moved aggressively to cooperate with the investigation, which was initially led by the OPM IG, subsequently joined by DOJ. Any employees who were found to have any responsibility related to those allegations were quickly separated from the company. Over the past two years the company has taken aggressive and effective action to increase controls, enhance procedures, place new leadership in place, and today USIS is a strong, responsible contractor providing a cost-effective and high-quality service for OPM; and that is after two years of hard work, including separating of anybody who had any responsibility for the behavior alleged in the complaint.

Chairman ISSA. I just want to make sure, before I go to Ms. Grisham, the director, you said something I think you want to correct the record. You said they committed fraud. Do you want to correct that to——

Ms. ARCHULETA. Yes. I actually did say afterwards, but I didn't say it loud enough, an allegation of fraud. Thank you, sir.

Chairman ISSA. Okay. Thank you.

The gentlelady from New Mexico.

Ms. LUJAN GRISHAM. Thank you, Mr. Chairman.

Director Archuleta, welcome. Point of personal privilege, Director Archuleta is from my district, sort of, and definitely from my home State.

Chairman ISSA. She very proudly told me that in our one-on-one meeting, so she does not make it a secret one bit that she is in a much colder and less hospitable climate here.

Ms. LUJAN GRISHAM. Sometimes. In any event, Mr. Chairman, thank you for that.

And congratulations on your job. By virtue of the content and the discussion in this hearing, it is an important role with many, many challenges that do not go unaddressed; we continue to have these significant and serious threats and issues to our security, so I appreciate very much your high level attention and your willingness to tackle the issues that have been presented today, and others.

I want to take a different tact, and I don't want anyone to assume that I don't agree with many of the statements by my colleagues on both sides of the aisle about focusing in on improving practices and minimizing all of our security breaches and threats, and getting our criminal background checks and related issues on track, and safeguarding that information and making sure that we have actors on behalf of the Federal Government that are able to do that job, and that we feel safeguarded by virtue of having that information vetted and dealt with appropriately.

But in the context of mental health, there is an interesting and I think a very difficult balance, and I want to talk about it for a minute, and that is that we want folks to disclose, we want folks to disclose prior to a criminal background screening, and we want

them to disclose after. Some emotional illnesses or emotional problems are not a specific diagnosis and have something to do with what happens in your environment, in your life later, after a security clearance; and I would guess that most people aren't going to disclose that because you lose your security clearance for reasons that I think aren't easy to talk about. But if people get the right kind of help, they may not be a security threat and might get the kind of help that they need. So it is a very delicate balance.

We don't want to create any more problems where people fall through the cracks and we create these problems and security threats and loss of life. They are absolutely unacceptable. But I am interested in where we draw some of these balances and how we can do a much better job screening and getting folks to want to participate in that screening.

Are you wrestling with these issues currently?

Ms. ARCHULETA. Yes. These very serious issues are being discussed right now, and I appreciate your comments and would seek to have further discussions with you. Issues of balancing privacy and national security are very difficult, but the issues of mental health are also and play an important role in our background investigations and the granting of security clearances. So I would appreciate the opportunity to have further discussions with you as these ongoing issues are being reviewed by both OPM and ODNI through the Quality Assessment Working Group.

Ms. LUJAN GRISHAM. Thank you. Maybe in that Quality Assessment Working Group how do we today, notwithstanding that I hope that these processes get greatly improved, how do you ensure that employees who reach out now about mental health or mental health-related issues, that they are actually getting the assistance that they need? And it is really a two-part issue, because, one, you want to make sure that you are responding correctly in balancing those privacy issues, but then if there is a treatment course, you want to make sure that that employee is, to the highest degree possible, notwithstanding their own legal protections, that they are adhering to those, because if not then you have to minimize, potentially, any of those threats internally or externally that you are required to eliminate or mitigate to the highest degree?

Ms. ARCHULETA. Certainly the support of OPM for any employee around mental health issues is there, and offering not only whatever support we can as employers, but also helping to refer those individuals to doctors or other practitioners who can help.

Ms. LUJAN GRISHAM. And I am assuming also that with your agency's involvement, that the inspector general, that all related players would be weighing in on trying to strike that very delicate balance.

Ms. ARCHULETA. I know they already are, and I appreciate your support for this issue and would look forward to further discussions with you.

Ms. LUJAN GRISHAM. Thank you.

I am out of time, so I do hope, Mr. Chairman, that we can continue to have these kinds of discussions, because the best possible practice isn't going to get at all of these issues, and even in law enforcement—I know I am taking up time I don't have, so I appreciate your patience with me—there are the screening tools that are

prepared by mental health professionals, and it depends on the jurisdiction about how effective those tools are at screening people in or out appropriately, or inappropriately, and I don't think it is an area that we have been all that effective at. And given what has tragically occurred, we have to do something about it immediately.

Chairman ISSA. Well, for the gentlelady, one advantage of going last is you are unlikely to see a heavy, quick gavel on your time. But I join with the gentlelady in recognizing that mental health after somebody is an employee is critical. Part of what we are concerned about here today, of course, is Aaron Alexis was somebody whose mental health should have made them not an employee, as it turns out. But I share with you that sort of screening desire and treatment as appropriate.

Ms. LUJAN GRISHAM. Thank you, Mr. Chairman.

Chairman ISSA. Thank you.

The gentlelady from the District of Columbia has one final question.

Ms. NORTON. Mr. Chairman, I just want to clear up what seems to be a circular process here, but I do want to say I think this may be the first hearing, I may be wrong, in the House on the Navy Yard shooting, and I want to thank you very much for this hearing. I am certain I speak not only for my own district. There were people from—they have had to rename the building, this was such a tragic occurrence.

But I was puzzled, really, that apparently OPM barred the president of USIS investigative division from working on contracts. You can understand OPM is doing that, though. But then USIS protests, essentially implicating OPM in the fact that the man was promoted in the first place. I have no idea whether or not, perhaps Ms. Archuleta, OPM reconsidered its decision. All we know is that the committee was informed that this man has resigned.

Perhaps I should go to Mr. McFarland. Do you think he should have been suspended? Should OPM have been implicated in his promotion, as apparently USIS says and was shocked that the implication was so deep that OPM would then bar him from working on the contract?

Mr. MCFARLAND. I am not familiar with that aspect that you are talking about right now.

Ms. NORTON. Ms. Archuleta, you are aware that this man has resigned now. Was OPM involved, as USIS says, in promoting him to president?

Ms. ARCHULETA. No, we weren't. I think he may be talking about the process of uncovering who was involved in the alleged fraud, and the individuals were removed over a sequence of time, and as we learned of——

Ms. NORTON. All I am trying to find out is do you have any say on who gets promoted or not promoted.

Ms. ARCHULETA. No.

Ms. NORTON. So you didn't have anything to do with that, with the resignation. How did the resignation come about? Now he is gone. You tried to make him gone, now he is gone. Did you request his resignation?

Ms. ARCHULETA. We suspended him from the contract. What he did afterwards was up to the company itself.

Ms. NORTON. I just want to suggest that this—if you have such a close relationship, Mr. McFarland, maybe this is inherently a governmental matter. It looks like they are in bed, virtually, with USIS, and if they are in bed with them, it may be that it involves secure matters, and that they can't really separate themselves from the company. So one wonders whether this is appropriately given to a contractor.

Mr. MCFARLAND. Are you saying that the suggestion is that that person was in bed with OPM hierarchy?

Ms. NORTON. I am suggesting that the company may be in bed with OPM, because it worked so closely and apparently has to work so closely because it is inherently governmental work because it involves secure matters, and despite the mistakes that have been made here, it looks like they are going to be working even more closely with the company. One wonders whether there is a distinction between the Government and the company sometimes.

Thank you, Mr. Chairman.

Chairman ISSA. I thank the gentlelady.

We now will go to the ranking member for his closing.

Mr. CUMMINGS. Mr. Chairman, I again want to thank you for this hearing. To the panel, I want to thank you too.

Just a few years ago I chaired a subcommittee in the Transportation Committee, and that committee was called Coast Guard and Maritime Matters, and we had a situation there where literally the Government was purchasing boats that didn't float, literally. You know, when I listen to the testimony here and I hear things like 665,000 dumped files, Mr. McFarland, it is shocking to the conscience, it really is. You know, sometimes I think that when people do these things, they need to understand that there are consequences. They may not live long enough to see the consequences, they may not ever hear about them, they may never be brought to justice, but there are consequences. And when we, as entities and individuals, create a—and doing our individual jobs that we are supposed to do—move to a culture of mediocrity or negligence or pure fraud and greed, it causes all kinds of problems. And we have to put in, unfortunately, we have to put in the mechanisms to protect ourselves from ourselves. And I am hoping that there are a lot of lessons learned here.

We cannot bring back those individuals who were killed, but hopefully we can put things in place, and I know we are continuing to do it, Ms. Archuleta and others, I know we are trying to do that, but we need to kind of make sure it happens fast. And nobody, and I know the chairman will agree with me, nobody is trying to put a negative light on all the folks who work for these various companies. No. It only takes a few, but the few can do mighty damage.

Mr. Phillips, as I said to you a little bit earlier, you have a tough job. You really do. And maybe it has been made easier by a lot of people taking the exit ramp and getting out of the company for one reason or another. But surely many of them will be brought to justice. And as I sat here, I could not think that the chairman and I were just talking about our various districts and I think about the people on my block. I live not too far from the Ravens Stadium in Baltimore, and I have said this many times, if somebody in my block, and there are people there who, if they stole a bike, they get

a record for a lifetime. If they steal a bike, $150 bike. Record, lifetime, where they may won't be able to get jobs, won't be able to live in certain places, won't be able to get certain education opportunities like scholarships and whatever.

And then when I look at stuff like this, where people are not doing their jobs and I am sure the investigation will reveal what it will reveal, but I am sure there are some criminal activity here. You know, I want to make sure that we get to that, and I am sure the Justice Department will, because I think not only must we do it to make sure that these incidents don't happen again, but one of the things that the chairman talks about in his statement when he gives the purpose of the committee, he talks about trust in Government and making sure that tax dollars are spent properly and making sure that people feel good, feel that we are making sure that their tax dollars are spent effectively and efficiently. So this is a bipartisan effort because this is about making sure that those people who are given clearances deserve them. After all, we don't come up with this concept of clearances just to be doing it; there is a purpose for this.

So, again, I want to thank all of you for what you have contributed.

I know I went a little longer than I expected to, Mr. Chairman, but I think this is just so very, very important because there are consequences. Thank you very much.

Chairman ISSA. I thank the gentleman.

In closing, a couple of things. First of all, Mr. Phillips, Mr. Rhodes, and Ms. Ordakowski, we are going to be looking at your companies on an ongoing basis. This committee has the primary jurisdiction for the Federal workforce and their contractors, and it is an area of interest that we are going to do on an ongoing basis. We certainly want to make sure that what Mr. Phillips says has been straightened out at his organization has been. We also are going to want to make sure that best practices continue to evolve at both of yours.

I am of the opinion that Government does best what it checks somebody else doing, and does worse what it does in-house and then tries to hold itself accountable. That has been a problem of Government for a long time, is are we an honest broker of what works and what doesn't.

Director, you are the honest broker, and it is extremely important that, in fact, first, we see if the systems that failed us, including the software that wasn't in place for many years, that ultimately discovered that case files were being opened and quickly closed, now dubbed dumping, that kind of work, that kind of IT forward-leaning, something that the ranking member and I have been working on trying to modernize Federal IT procurement so that you can have those systems, we need to work with you to make sure you have it, those management tools, because we think it is important.

I think here, on both sides of the aisle today, we became very aware that there are two problems we are dealing with. One has to do with how security clearances occur, and for which there are some legal changes that this committee is going to have to work on. But, director, there is something that I am more concerned

about, and that is that it is a policy not to look at the Internet as an investigative tool. This is an area within your jurisdiction that I strongly encourage you make your best effort, recognizing that there are some questions of whether you will be sued for doing it and so on, that both in the case of security clearances you free up your in-house people and these contractors to at least begin looking at this tool for what could be important information that would then lead to further investigation that would not necessarily be on the Internet.

And, secondly, that you ask the question from a standpoint of the entire Federal workforce, is it wise in this day and age not to at least look at the Internet before each and every person is hired; that some sort of a pro forma that is done objectively not occur, because I think that it is important that we say we have done due diligence on every person that comes to work for the Federal Government so that if they have an anger management problem, like shooting tires out, that we don't wait and ask did they get a clearance wrong, but we ask should this individual, Aaron Alexis, ever been hired to work for any Federal work organization or contractor. And we could have gotten into Snowden and had a similar discussion about that.

Lastly, Mr. Lynch dropped a bill the other day. The committee has been working on a completely bipartisan basis. Most of what is in his bill and some other items are items that we have brought to the attention both of OPM and Department of Defense, and we have gotten unofficial answers and some comments. At this point, based on your discussion today, we would ask that you work with committee staff, both majority and minority, on all aspects to give us, if you will, final answers on the proposals we are making so that we can draw up a comprehensive bipartisan bill. The majority did not offer a bill, figuring that it was much better to have this hearing and then get your final comments, but I think it is now appropriate to do so.

Lastly, I meant it deadly seriously, I believe in qui tam. I believe that whistleblowers bringing us new information where the Government is being wronged is critical. I also believe that, whenever possible, the Federal Government should find its own problems, correct them, and any amount owed to the Federal Government flows to us, without an outside piece of litigation. For that reason, I am deeply concerned that the evidence in the case of this particular lawsuit appears on its face to be an individual filing a case months after he was cc'd on what I would have considered to be the smoking gun; and I would ask that you be aware of that. We will be making an additional referral to Judiciary Committee and to Department of Justice, asking them to at least give us a legal evaluation of whether or not this qui tam may, in fact, be inappropriate, not the suit, but the qui tam.

If you have any final questions or statements, I would be happy to take them now; otherwise, we are concluded. Seeing none, I thank you all for your presence. We are adjourned.

[Whereupon, at 12:51 p.m., the committee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Opening Statement
Rep. Elijah E. Cummings, Ranking Member

Hearing on "DC Navy Yard Shooting: Fixing the Security Clearance Process"

February 11, 2014

There is no doubt that we need to conduct a thorough investigation to determine how Aaron Alexis was able to obtain and keep a security clearance given his troubling background. We owe this to the families of the twelve people he killed and the others he injured, as well as all Americans who rely on the background check system to protect our national security.

Mr. Chairman, I want to thank you and your staff for your bipartisan approach on this investigation to date. Our work has the potential to stand as an important part of this Committee's legacy if we follow through on these efforts. Here is what we know so far.

First, Alexis obtained a security clearance from the Navy in 2008, and his background investigation was conducted by U.S. Investigations Services (USIS). USIS is the single biggest contractor that performs background investigations for the Office of Personnel Management (OPM), completing more than the government or any other contractor.

Four years before Alexis got his clearance, he was arrested in Seattle for shooting out the tires of someone's car. USIS did not obtain a copy of that 2004 arrest report, and OPM did not require one because the City of Seattle refused to cooperate with similar requests in the past. Instead, USIS obtained a summary that omitted references to the weapon and said only that Alexis was charged with malicious mischief. If USIS and the government had obtained a copy of that arrest report, perhaps Alexis' clearance would have been denied.

Under its contract, USIS also was required to conduct a "quality review" of its background investigation of Alexis. However, nobody has been able to confirm that USIS did that quality review. USIS has not confirmed it, nor has OPM, nor has the Inspector General.

In 2011, a long-time USIS employee, its Director of Fieldwork Services, accused USIS of a massive conspiracy to bilk U.S. taxpayers. Although USIS was required to conduct quality reviews of all of its background investigations, this official reported that USIS was "dumping" unfinished cases and billing OPM for the work anyway.

Inexplicably, USIS also had a separate contract with OPM to conduct additional quality reviews on behalf of the agency. In other words, USIS was checking its own work.

In January, the Committee conducted a transcribed interview with Merton Miller, OPM's Associate Director of Federal Investigative Services. He accused USIS of using information obtained through this second contract to evade detection of its fraud under the first. He said:

> [T]hey circumvented OPM's oversight of their performance of their quality review. I'm not splitting hairs, but they knew how we were auditing. They knew what kind of reports we generated to oversee that they were actually performing the activities ... so they circumvented our oversight process, and they falsified records to help do that.

The Department of Justice has now determined that these allegations have merit and filed a False Claims Act suit seeking more than $1 billion from USIS, claiming that the company charged taxpayers for work it never performed on 665,000 background investigations from 2008 to 2012. The Department stated:

> USIS management devised and executed a scheme to deliberately circumvent contractually required quality reviews of completed background investigations in order to increase the company's revenues and profits.

In 2007, USIS was purchased by a private equity firm known as Providence Equity Partners. The Committee's investigation revealed that directly after this acquisition, USIS adopted aggressive new financial incentives to accelerate its work. During this period, USIS executives received huge bonuses, including more than $1 million for the company's CEO, Bill Mixon, and about $470,000 for the company's Chief Financial Officer. The Justice Department alleges that both officials were "fully aware of and, in fact, directed the dumping practices." USIS also received millions of dollars in bonus payments from OPM for its seemingly incredible progress, including $2.4 million in 2008, $3.5 million in 2009, and $5.8 million in 2010.

In the wake of this scandal, the company's CEO, CFO, and nearly two dozen other officials have resigned, been terminated, or left the company. In fact, just yesterday, USIS informed us that the President of its Investigations Services Division has also now resigned.

These revelations cry out for an investigation, but to date the Committee has not conducted a single transcribed interview of any USIS employee. Mr. Chairman, I know you wanted to focus first on OPM's oversight, but given what we have uncovered, these serious allegations must be investigated. While I have no objection to Mr. Phillips being here today, he was hired only last year and has no firsthand knowledge of these allegations. We should investigate how bonuses and incentives were paid to USIS executives, as well as the roles played by Providence Equity Partners and Altegrity, the holding company formed to house USIS.

Finally, Mr. Chairman, I appreciate that your staff provided us with a draft of your report last week, but I regret that you issued it yesterday without including most of this information about USIS that we asked you to include. For these reasons, I am issuing my own staff report today that provides this information, and I ask that it be made part of the record.

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

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
DARRELL ISSA, CHAIRMAN

SLIPPING THROUGH THE CRACKS: HOW THE D.C. NAVY YARD SHOOTING EXPOSES FLAWS IN THE FEDERAL SECURITY CLEARANCE PROCESS

STAFF REPORT
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES
113TH CONGRESS
FEBRUARY 11, 2014

Table of Contents

I. Executive Summary

On September 16, 2013, Aaron Alexis walked into Building 197 of the Washington Navy Yard and murdered twelve people. Four more were injured. Alexis was granted access to the Navy Yard that morning because he worked for a small private company that held a subcontract with the Navy to update computer hardware at Navy facilities around the world. At the time, Alexis had worked for the company for a total of seven months. He was hired in large part because he held a Secret level security clearance.

Before being killed by police during his murderous rampage, Alexis was one of roughly 4.9 million Americans—over 1.5 percent of our country's population—that hold security clearances, potentially granting them access to some of our nation's most confidential secrets and most secure facilities. The Office of Personnel Management (OPM) is the federal government's clearinghouse for background investigations for security clearances for non-intelligence community personnel. When an agency wants to sponsor an individual for a security clearance, it relies primarily on OPM to conduct the background check on the individual. OPM then transmits its findings to the agency, which adjudicates the individual's clearance.

In FY 2012, OPM prepared over 2.3 million investigative products for federal agencies. Approximately 30 percent of this work was conducted by OPM employees, with the other 70 percent being outsourced to three companies who hold contracts with OPM. The Federal Investigative Services (FIS) branch of OPM, responsible for conducting these background investigations, has defined processes in place that are largely automated, which allows for faster investigations at the expense of thoroughness. Key information sometimes does not reach the agency adjudicators, which means that individuals—such as Aaron Alexis—are occasionally granted clearances that, had the adjudicator been aware of all the pertinent information, should have received more scrutiny and could have been denied.

Section II of this report discusses the story of how Aaron Alexis was able to receive, and maintain, his security clearance, despite a string of questionable conduct over several years. In 2004, Alexis was arrested for malicious mischief in Seattle for shooting the tires out of a car, claiming that he had a "black-out" fueled by anger. Three years later, when Alexis applied for a security clearance, OPM did not include this information in the background investigative file that went to the Navy. The Navy ultimately granted Alexis his clearance. After receiving his clearance, Alexis continued to engage in behavior that should have raised red flags. He broke his foot jumping off stairs while intoxicated, he fired a gun into his ceiling and through the apartment above, he fired a bullet through the wall of his room, he quit his job, and he complained that individuals were using a microwave machine to send vibrations into his body. None of this information was ever given to an adjudicator who had the ability to pull Alexis' Secret level clearance, which he maintained until September 16, 2013.

Section III of this report describes OPM's tightly-controlled federal security clearance process, as well as some of the challenges this process faces. This part of the report discusses how a background investigation is initiated, the type of field work conducted during an investigation, and the fact that up to three or four people can work on a single background investigation yet never communicate with each other about the investigation. Before an

investigation is sent to the client agency for adjudication, OPM performs quality review over the file. Despite this quality review, however, GAO has found that 87 percent of OPM's background investigation files are "incomplete." That number is completely unacceptable.

The Committee on Oversight & Government Reform plans to consider legislation to improve problems identified in the security clearance process during this investigation. Section IV of the report discusses potential legislative fixes that the Committee is considering. The notion of a continuous evaluation is something that has been heavily discussed over the past decade, but has yet to become a reality. OPM must implement a continuous evaluation system to ensure that questionable conduct, such as Aaron Alexis', will be reported to adjudicating authorities in near real-time. Congress should force OPM's investigative practices into the twenty-first century by allowing investigators to use the internet and social media sources in particular for the first time. Legislation could also finally allow agency adjudicators to directly speak with OPM investigators, giving adjudicators additional information on an applicant when deciding whether or not to grant a clearance. Congress must take steps to address OPM's need to capture information on the mental health of those holding security clearances. Finally, Congress should consider measures that will require local law enforcement offices across the country to cooperate with OPM investigators by providing specific information to security clearance investigators when they seek legal information on applicants. Though these offices are required under current federal law to cooperate with OPM, over 450 of these offices do not, and OPM has not taken the necessary steps to obtain better cooperation.

Major security clearance reform was last pushed through Congress ten years ago with the passage of the Intelligence Reform and Terrorism Prevent Action of 2004. While the backlog of clearance investigations has dramatically subsided since then, recent technologies and the rise of social media now allow for these investigations to encompass even more information about applicants while still allowing the investigations to be completed in a timely manner. This ability to capture relevant, detailed information, and to do it in near real-time, however, is not being properly utilized by OPM. Updated legislation is necessary to ensure that this relevant information is sent to the proper authorities in a timely manner.

No legislation or congressional action can repair the damage that Aaron Alexis inflicted on both the families of his victims as well as the Nation as a whole. Nonetheless, Congress has a responsibility to investigate the process that permitted Aaron Alexis to receive and maintain a security clearance, and Congress must take steps to improve that process to prevent dangerous people from gaining access to secure federal facilities and information. Congress, OPM, the Department of Defense (DOD) and other federal agencies must work together to tighten this process and ensure that fewer individuals like Aaron Alexis slip through the cracks in the future.

II. Aaron Alexis: A Case Study for Reform

Just before 8:00 a.m. on September 16, 2013, Aaron Alexis arrived at the Washington Navy Yard.[1] After parking his rented vehicle, he used a valid Common Access Card to enter Building 197.[2] Though he carried a backpack, Alexis was indistinguishable from other contractors and federal employees reporting for work at the Navy Yard that Monday morning. In his backpack, however, Alexis had a Remington 870 shotgun that he had purchased just two days earlier. The condition of the shotgun—Alexis had sawed the stock and barrel of the shotgun to shorten its length[3]. Alexis also carved "Better off this way" and "My ELF weapon" into the stock,[4] which gave an indication of his mental state in the days preceding the shooting.

At 8:16 a.m., less than 15 minutes after entering the building, Alexis began shooting.[5] At 9:25 a.m., law enforcement officers shot Alexis in the head, fatally wounding him.[6] During the intervening 69 minutes, Alexis killed twelve people and wounded several others.

In the following days, the world learned about Aaron Alexis and speculated about what prompted his horrible rampage. A particularly bewildering question emerged: how did Aaron Alexis obtain and maintain a security clearance which allowed him access to Building 197? After months of investigation by the Committee on Oversight & Government Reform the answer is clear, but unfortunate—the federal security clearance process in place at the time allowed Aaron Alexis to slip through the cracks.

A. 2004: Alexis' Malicious Mischief Arrest

Nearly a decade before the shooting at the Navy Yard, Aaron Alexis showed signs of dangerous instability. In 2004, Alexis was arrested in Seattle for "malicious mischief." The initial police incident report described Alexis' actions on May 6, 2004. It stated:

> [Witness] saw the suspect remove what appeared to be a gun from his waistband, chamber a round and shoot [Witness'] rear left tire. The suspect then walked to the right side of [Witness'] car and shot the right rear tire. The suspect returned to the left side of the car and shot one round into the air.[7]

---

[1] Staff Reports, *What Happened Inside Building 197?*, WASH. POST, Sept. 25, 2013, at http://www.washingtonpost.com/wp-srv/special/local/navy-yard-shooting/scene-at-building-197/ [hereinafter *Building 197 Staff Reports*].
[2] *Id.*
[3] Ashley Halsey III, Clarence Williams, & Sari Horowitz, *Officials Probing Whether Workplace Dispute Drove Navy Yard Shooting*, WASH. POST, Sept. 20, 2013, http://www.washingtonpost.com/local/navy-yard-reopens-but-scene-of-mass-shooting-remains-closed/2013/09/19/387ba03a-2120-11e3-a358-1144dee636dd_story.html.
[4] Sari Horowitz, Steve Vogel, & Michael Laris, *Officials: Navy Yard Shooter Carved Odd Messages Into His Gun Before Carnage*, WASH. POST, Sept. 18, 2013, http://www.washingtonpost.com/local/officials-navy-yard-shooter-carved-odd-messages-into-his-gun-before-carnage/2013/09/18/edaae792-2065-11e3-8459-657e0c72fec8_story.html.
[5] Building 197 Staff Reports, *supra* note 1.
[6] *Id.*
[7] Seattle Police Department Incident Report and Related Documents (June 15, 2004), at 1-2 [hereinafter *Seattle Police Report*].

In a subsequent interview, one of the witnesses told the Seattle police that Alexis had "stared at the construction workers every morning for about 30 days prior to the shooting."[8]

On June 3, 2004, Alexis was arrested and confessed to shooting out the tires. Alexis told the police that he perceived one of the witnesses to have "disrespected him" and led to a "'black-out' fueled by anger."[9] Alexis told police that he did not remember firing the gun until an hour later.[10] Alexis was booked for malicious mischief.[11]

Alexis told the police that he had been in New York on September 11, 2001, and that the events had disturbed him. Alexis' father further told the police that "his son had experienced anger management problems that the family believed associated with PTSD" and that "his son was an active participant in rescue attempts [on] September 11, 2001."[12]

According to press reports, although the case was referred to the Seattle Municipal Court on June 15, 2004, for charges related to property damage (over $50) and unlawful discharge of a firearm,[13] Alexis was never prosecuted. Despite the reference in the arrest record to the referral, a court spokesperson for the Seattle Municipal Court said the court never received the case.[14] Spokespeople for both the Municipal Court and the Seattle City Attorney's office said that the case should have been referred to the City Attorney's Office, which handles misdemeanor charging decisions.[15] The City Attorney's Office, however, never received a referral for Alexis' case.[16] Accordingly, when Alexis appeared in court the next month, the charges were dropped.[17]

B. 2008 – 2011: Alexis's Time in the Navy Reserve

Alexis enlisted in the Navy Reserve at the New York Military Entrance Processing Station in Brooklyn, New York, on May 5, 2007.[18] Upon completion of Recruit Training in July

---

[8] *Id.* at 4.
[9] *Id.*
[10] *Id.* at 5.
[11] *Id.*
[12] *Id.* During its investigation, the Committee was unable to confirm if Alexis was in New York, New York on September 11, 2001, or what, if any, role he played in rescue attempts after the attack. On his SF-86, Alexis listed that he lived at an address in Brooklyn, New York, from January 10, 2001 to March 11, 2001, and in Seattle, Washington, from March 12, 2001, to August 31, 2005. However, Alexis claimed to work for a company in Brooklyn, New York from January 3, 2001, to February 4, 2004. He also claimed to attend the Borough of Manhattan Community College from February 5, 2001, to February 8, 2003. Form SF-86, completed by Aaron Alexis (Mar. 22, 2007).
[13] *Id.* at 3, 6.
[14] *Why Wasn't Aaron Alexis Prosecuted for Previous Shooting Incidents?*, CBS NEWS, Sept. 19, 2013, http://www.cbsnews.com/news/why-wasnt-aaron-alexis-prosecuted-for-previous-shooting-incidents/.
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] Memorandum from Juan M. Garcia, Asst. Sec'y of the Navy to Sec'y of the Navy, *Review of Service Record and Performance of Former Sailor Aaron Alexis* (Sept. 20, 2013) *available at* http://www.nytimes.com/interactive/2013/09/24/us/24shooting-document1.html [hereinafter *Navy Review of Service Record*].

2007 and Aviation Electrician's Mate "A" School in December 2007, Alexis was assigned to the Fleet Logistics Support Squadron 46.[19] In March 2008, despite his failure to disclose the 2004 arrest and several outstanding debts amounting to several thousand dollars, the Navy granted Alexis a Secret level clearance. Upon granting the clearance, the Navy sent a single warning letter to the squadron where Alexis was stationed concerning his negative credit history.[20]

After receiving his clearance, Alexis was cited at least eight times for misconduct over the three years he spent in the Navy Reserve. This misconduct ranged from a traffic ticket and showing up late for work, to an insubordination charge in 2008, a disorderly conduct charge in 2009, and extended unauthorized absences from work several times between 2008 and 2010.[21]

Alexis received several administrative punishments during his time in the Navy Reserve. On August 10, 2008, Alexis was arrested on a disorderly conduct charge in DeKalb County, Georgia.[22] He spent two nights in jail after destroying furnishings in a nightclub.[23] On September 23, 2008, Alexis' commander imposed a non-judicial punishment for his unauthorized absence from work due to his time in jail. This punishment was later suspended, though a record of non-judicial punishment appeared in Alexis' service record going forward.[24]

In July 2009, Alexis broke his foot after allegedly jumping off stairs in a tavern while intoxicated. Alexis' commander sought to impose a non-judicial punishment with a reduction in pay. Alexis appealed, and the punishment was suspended due to a lack of evidence that Alexis was intoxicated at the time of the incident. The report of non-judicial punishment was removed from Alexis' record.[25]

On September 16, 2010, Alexis fired a gun into the ceiling of his apartment which proceeded through the apartment above.[26] The occupant of that apartment told police that she was "terrified" of Alexis and thought he had intentionally fired the round into her apartment.[27] Alexis had confronted her several days earlier, complaining that she was making too much

---

[19] *Id.* Fleet Logistics Support Squadron 46, based in Atlanta, Georgia when Alexis joined, moved to Fort Worth, Texas in 2009.

[20] Letter from Dir., Dep't of the Navy Central Adjudication Facility, to Aaron Alexis via Commanding Officer, Fleet Logistics Support Squadron 46 (Mar. 11, 2007). As discussed in Part III(C) of this report, warning letters relay concerns DOD adjudicators have about an applicant to the applicant and his or her commanding officer. *See* Part III(C) at 31-32.

[21] Sari Horowitz, Craig Whitlock, & Jerry Markon, *Navy Yard Gunman Had History of Mental Illness, Checkered Military Career, Officials Say*, WASH. POST, Sept. 17, 2013, at http://www.washingtonpost.com/politics/alleged-navy-yard-gunman-had-checkered-military-career-officials-say/2013/09/17/a136ad0c-1fa1-11e3-8459-657e0c72fec8_story.html.

[22] Uniform Traffic Citation, Summons, and Accusation for Aaron Alexis, DeKalb County, GA Police Department (Aug. 10, 2008).

[23] Navy Review of Service Record, *supra* note 18, at 3; *see also Timeline: The Life of Navy Yard Shooter Aaron Alexis*, WASH. POST, Sept. 18, 2013, at http://www.washingtonpost.com/national/timeline-the-life-of-navy-yard-shooter-aaron-alexis/2013/09/17/0915a9d8-1fab-11e3-94a2-6c66b668ea55_story.html.

[24] Navy Review of Service Record, *supra* note 18, at 3. Before the non-judicial punishment was suspended, Alexis was ordered to forfeit half of his monthly pay for two months, and he was reduced one pay grade.

[25] *Id.*

[26] Incident Report for Aaron Alexis, Fort Worth Police Department (Sept. 16, 2010).

[27] *Id.*

noise.[28] When the police arrived to question Alexis about the shooting, he emerged only after firefighters arrived to force entry into his apartment. Alexis told the police that he had been cleaning his gun while cooking and that the gun accidentally discharged because his hands were greasy.[29] Alexis was arrested for improperly discharging a firearm.[30] According to the Tarrant County District Attorney's office, however, there was insufficient evidence to pursue the case.[31]

After this arrest, Alexis' commander began the process to force him out of the Navy with a general discharge. An administrative separation document was prepared to send to Navy Personnel Command. Since Alexis was not ultimately charged with unlawfully discharging a firearm, the document was not signed, dated, or sent.[32] Instead, on January 31, 2011, Alexis received an honorable discharge with a Reentry Code of RE-1, designating that he was eligible to re-enlist without restriction.[33]

C. 2013: The Newport Incident

After his discharge from the Navy, Alexis lived with Oui Suthamtewakul, the owner of the Happy Bowl Thai restaurant in White Settlement, Texas, near Fort Worth. Alexis lived with Suthamtewakul and his wife, rent-free, and occasionally worked as an unpaid waiter at Suthamtewakul's restaurant.[34] In interviews after the Navy Yard shooting, Suthamtewakul said that Alexis "had a gun at all times," and at one point fired a bullet through the wall of his room.[35] Alexis drank frequently and told Suthamtewakul he thought people were "coming to get him."[36] Alexis lived with Suthamtewakul and his wife until July 2013, when Suthamtewakul filed a police report accusing Alexis of putting sugar in the gas tank of his vehicle.[37] At that time, Alexis moved in with another friend and her husband.

In September 2012, Alexis began working for an IT consulting company called The Experts. As a precondition to Alexis starting work at The Experts, the company performed a background check of Alexis, a drug test, and confirmed his Secret level clearance through the Department of Defense.[38] Alexis worked on a sub-contract The Experts held with Hewlett Packard, updating computers at various military facilities in the United States and Japan. In

---

[28] *Id.*
[29] *Id.*
[30] *Id.*
[31] Deanna Boyd & Bill Miller, *Friends Puzzled by Navy Yard Shooter's Violence*, STAR-TELEGRAM, Sept. 17, 2013, http://www.star-telegram.com/2013/09/16/5167160/fort-worth-man-accused-in-washington.html.
[32] Navy Review of Service Record, *supra* note 18, at 4.
[33] *Id.*
[34] Horowitz *et al.*, *supra* note 21.
[35] *Id.*
[36] Rick Jervis & Carolyn Pesce, *For Navy Yard Shooter, Buddhism was a Temporary Refuge*, WASH. POST, Sept. 18, 2013, http://www.faithstreet.com/onfaith/2013/09/18/for-navy-yard-shooter-buddhism-was-a-temporary-refuge.
[37] Erica Goode, Sarah Maslin Nir, & Manny Fernandez, *Signs of Distress Multiplied on Killer's Path to Navy Yard*, N.Y. TIMES, Sept. 19, 2013, http://www.nytimes.com/2013/09/20/us/signs-of-trouble-on-navy-yard-gunmans-path-to-tragedy.html?_r=0.
[38] Letter from Counsel, The Experts, Inc., to Counsel, Naval Reactors (Oct. 11, 2013) at 1 [hereinafter *Oct. 11 Experts Letter*].

January 2013, Alexis abruptly left the company, citing a desire to go back to school, and complaining about traveling too much and not making enough money.[39]

Alexis returned to the company in June 2013. The Experts again commissioned a background check, a drug test, and confirmed his Secret level clearance through the Department of Defense.[40] Alexis continued work on the sub-contract with Hewlett Packard, continuing to update computers at various military facilities around the United States.

On August 4, 2013, Alexis traveled from a military facility in Norfolk, Virginia, to one in Newport, Rhode Island. Witnesses reported that, while at the Norfolk airport, Alexis became agitated, belligerent, and shouted obscenities until airport security officers finally calmed him down.[41] Before his flight departed, Alexis called an employee of The Experts and told her that someone at the airport was trying to pick a fight with him.[42] Alexis traveled to Newport without any other reported incidents. Several hours after checking into his hotel in Newport, however, Alexis called The Experts and asked to be moved to a different hotel, complaining of noise in other rooms.[43]

On August 5 and 6, 2013, Alexis reported for work at Naval Station Newport. During the evening of August 6-7, 2013, however, Alexis called The Experts several times and continued to report that he was hearing noises. Logs from one of the hotels where Alexis stayed reported that he knocked on doors in an attempt to locate the source of the noises, waking and frightening guests.[44] Alexis eventually contacted his supervisor at Hewlett Packard and went to her hotel, where he called the Newport Police Department.[45]

Alexis told the police that three people were following him and keeping him awake "by talking to him and sending vibrations into his body."[46] Alexis reported that the voices followed him from hotel to hotel, and that the individuals were using "some sort of microwave machine" to penetrate his body.[47] Alexis told the police that he was worried that the individuals were going to harm him, and stated that he did not have a history of mental illness in his family nor had he ever had a mental episode.[48] The Newport Police advised Alexis to stay away from the individuals and notify the police if they made contact with him.[49] The Newport Police did not arrest Alexis, as the reporting officers determined they had no cause to do so.[50]

---

[39] E-mail from Aaron Alexis to Program Manager, The Experts, Inc. (Dec. 28, 2012, 12:21 a.m.) ("I don't think I will be making the Virginia project. I think it best I just go back to school and finish my degree. Not having enough money and trying to travel [to] different sites, on top of the inconsistency in pay is too much.").
[40] Oct. 11 Experts Letter at 1.
[41] Goode *et al.*, *supra* note 37.
[42] Briefing by The Experts, Inc. to H. Comm. on Oversight & Gov't Reform Staff (Dec. 19, 2013) [hereinafter *Dec. 19 Experts Briefing*].
[43] *Id.*
[44] Goode *et al*, *supra* note 37.
[45] Oct. 11 Experts Letter at 2.
[46] Newport Police Department, Incident Report, Aug. 7, 2013.
[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] Horowitz *et al.*, *supra* note 4.

After these incidents, managers at The Experts told Alexis to take time off from work and sent him back to Fort Worth, Texas.[51] The Experts temporarily removed Alexis from a list of employees who could enter Naval Station Newport.[52] On multiple occasions, The Experts spoke with Alexis' Hewlett Packard site manager, who likely had the most contact with Alexis between August 4 and 7. The manager, who also worked with Alexis in Japan during his first period of employment at The Experts, said that she was comfortable having Alexis come back to work the following week.[53] The Experts also spoke with Alexis' mother, who said that Alexis had a history of paranoid episodes and most likely needed therapy.[54] Alexis returned to work the following week.[55]

D. Interactions with the VA

Alexis filed a disability compensation claim with the Department of Veterans Affairs shortly after being discharged from the Navy. On December 12, 2011, the VA granted Alexis a 20 percent disability rating for "orthopedic issues."[56] On December 19, 2012, the VA increased this rating to 30 percent, and awarded an additional 10 percent for tinnitus.[57] Alexis received a $395 monthly benefit for his disability.[58]

Alexis received treatment from the VA on two occasions. On August 23, 2013, two weeks after his episodes at the Newport, Rhode Island hotels, Alexis visited the emergency room at the VA Medical Center in Providence, Rhode Island, complaining of insomnia.[59] Alexis told VA medical professionals that he had not been able to sleep for more than two or three hours for about three weeks.[60] Including in the record from this visit is a note from the attending physician: "Denies drugs, cocaine, heroin, caffeine product, depression, anxiety, chest pain, sob [shortness of breath], nightmares. He denies taking nap during the day. Denies SI [suicidal ideation] or HI [homicidal ideation]. He works in the defense department, no problem there."[61] VA medical professionals gave him a prescription for a small amount of Trazodone.[62]

---

[51] E-mail from Program Manager, The Experts, Inc. (Aug. 7, 2013, 12:02 a.m.) ("I've arranged for someone to cover you at NWPT the rest of the week. I'm sending you home to get some rest and will call you in the morning.").
[52] Dec. 19 Experts Briefing.
[53] *Id.*; *see also* Oct. 11 Experts Letter at 2.
[54] Serge Kovaleski, *Supervisors of Navy Yard Gunman Were Told of Issues*, N.Y. TIMES, Oct. 4, 2013, http://www.nytimes.com/2013/10/05/us/supervisors-of-navy-yard-gunman-were-told-of-issues.html.
[55] Oct. 11 Experts Letter at 2. In the following weeks, Alexis worked in Williamsburg and Stafford, Virginia the week of August 12, 2013; in Newport, Rhode Island the week of August 19, 2013; in Carderock, Maryland the week of August 26, 2013; in Arlington, Virginia the week of September 2, 2013; and at the Washington Navy Yard the week of September 9, 2013. Alexis was scheduled to be at the Navy Yard the full week of September 16, 2013. *Id.*
[56] E-mail from Cong. Relations Officer, U.S. Dep't of Veterans Affairs, to Staff of House and Senate Veterans Affairs Comm. (Sept. 18, 2013, 3:06 p.m.).
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] Aaron Alexis Medical Progress Notes (Aug. 23, 2013, 5:37 p.m.).
[61] *Id.*
[62] *Id.*

On August 28, 2013, Alexis went to the emergency room at the VA Medical Center in Washington, D.C., again complaining of insomnia.[63] On this occasion, Alexis said that he was waking up at 4:00 a.m. "like clockwork."[64] Alexis was given a refill of the same medication and was again told to follow up with a primary care physician.[65] According to the VA, on both occasions Alexis was "alert and oriented."[66] On both emergency room visits Alexis denied struggling with anxiety or depression, and denied having thoughts about harming himself or others.[67]

E. September 16, 2013: The Navy Yard Shooting

Alexis began working in the Washington, D.C. metro area on August 26, 2013. He was scheduled to remain in the area for several weeks.[68] Alexis' daily performance evaluations varied from "Poor" to "Great," but, if his managers noticed any unusual behavior, they did not report it.[69] After the Navy Yard shooting, investigators found that Alexis left behind several documents potentially detailing his motivation for the attack. Alexis wrote that the government had been attacking him for the past three months using "extremely low frequency" electromagnetic waves.[70] He wrote: "Ultra low frequency attack is what I've been subject to for the last three months . . . . And to be perfectly honest, that is what has driven me to this."[71]

He further wrote that he was prepared to die in the attack, and that he accepted death as the inevitable consequence of his actions.[72] It is not clear whether Alexis sent these documents—a clear cry for help—to anyone. It is clear in hindsight that Alexis was severely disturbed and needed help.

---

[63] E-mail from Cong. Relations Officer, U.S. Dep't of Veterans Affairs, to Staff of House and Senate Veterans Affairs Comm. (Sept. 18, 2013, 3:06 p.m.).
[64] Aaron Alexis Medical Progress Notes (Aug. 28, 2013, 5:31 p.m.).
[65] *Id.*
[66] E-mail from Cong. Relations Officer, U.S. Dep't of Veterans Affairs, to Staff of House and Senate Veterans Affairs Comm. (Sept. 18, 2013, 3:06 p.m.).
[67] *Id.*
[68] Oct. 11 Experts Letter at 4. Alexis was scheduled to be in Carderock, Maryland the week of August 26, 2013, Arlington, Virginia the week of September 2, 2013, and at the Washington Navy Yard the weeks of September 9 and 16, 2013. *Id.*
[69] Alexis' HP supervisors evaluated him on a daily basis. These evaluations, known as "Track Reports," were sent to The Experts regularly. During the week of August 12-16, Alexis received "Average" and "Good" evaluations, with some comments that he needs more training, and other comments that he appears to be proficient. During the week of August 19-23, Alexis received evaluations of "Poor" and "Average", with comments that he "needs to be more discrete in front of the customers, "makes a lot of excuses," "doesn't follow direction," and "wastes a lot of time." Alexis' manager this week also noted that his technical ability is not very high and that he was working slowly. During the week of August 26-30, Alexis received evaluations of "Average" with one note that he worked slowly. During the week of September 3-6, Alexis received evaluations of "Great" with no additional comments. During the week of September, Alexis received evaluations of "Average" and "Great" with three additional comments indicating that he worked slowly. Aaron Alexis Track Reports (July 14, 2013, to Sept. 13, 2013).
[70] Michael Schmidt, *Gunman Said Electronic Brain Attacks Drove Him To Violence, F.B.I. Says*, N.Y. TIMES, Sept. 25, 2013, http://www.nytimes.com/2013/09/26/us/shooter-believed-mind-was-under-attack-official-says.html.
[71] *Id.*
[72] *Id.*

On many occasions in the years leading up to the September 16, 2013 shooting, Aaron Alexis could have been stopped—either by a thorough investigation of his background prior to granting him a clearance, continuous evaluation of his competency for a security clearance while he was a Naval reservist, or reports of his behavior as a government contractor.

When Aaron Alexis first applied for a security clearance in 2007, he failed to disclose his arrest in Seattle on his SF-86, despite a requirement to do so.[73] When the arrest was discovered in the course of Alexis' background investigation, Alexis simply said that he "deflated" the tires on a vehicle.[74] He did not mention the use of a deadly weapon. A police report from the Seattle Police Department detailing the incident—and countering Alexis' claims—was never obtained during Alexis' background investigation.[75] As a result, the crucial information contained in the police report was never reviewed by the adjudicators who granted Alexis his clearance.

Current law requires that holders of a Secret level clearance be re-investigated every ten years.[76] No continuous re-evaluation is necessary. The individual holding the clearance is required to self-report misconduct within that ten-year span. There is no mechanism, however, other than the ten-year periodic re-investigation, to check whether or not an individual is actually reporting any misconduct. Even though Alexis' commanders at the Navy were aware of his 2008 and 2010 arrests, the Committee uncovered no evidence that Alexis reported this information to an adjudicative authority within the Navy, or that Alexis' Navy commanders reported these arrests to such an authority. Had such a continuous re-evaluation requirement been in place while Alexis was a Navy Reservist, these arrests would have been noted in a system for potential re-review by a Department of Defense adjudicator.

No one reported Aaron Alexis' questionable conduct in Newport, Rhode Island in August 2013 to an adjudicative authority. The Experts and Hewlett Packard were aware of Alexis' bizarre behavior, but neither company appears to have reported the information to an adjudicative authority. Even if one of the companies wanted to suspend Alexis' security clearance for a period of time until his behavior normalized, they could not do so. That power rests alone with the adjudicating agency.

The police report stemming from Alexis' Newport, Rhode Island conduct was sent to Naval Station Newport, where the military police said they would follow up.[77] Shortly after the Navy Yard shooting, a spokesperson for Naval Station Newport declined to comment as to whether military police actually did follow up on the incident report.[78] Regardless, this information on Alexis' mental state did not get to Department adjudicators, who could have taken steps to suspend or terminate his security clearance.

Additionally, under a continuous re-evaluation system, Alexis' two visits to VA emergency rooms in August 2013 could have been immediately flagged for Department

[73] Form SF-86, completed by Aaron Alexis (Mar. 22, 2007).
[74] U.S. Office of Personnel Mgmt., Investigative Report on Aaron Alexis, closed Aug. 24, 2007, at 20.
[75] This police report was easily obtained by Committee investigators—some nine years after the incident took place—after only two short phone calls.
[76] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3706.
[77] Horowitz *et al., supra* note 4.
[78] *Id.*

adjudicators. These incidents were not reported to these authorities and, tragically, just a month later, Aaron Alexis killed twelve people.

III. The Federal Security Clearance Process

Over the past several months, the Committee on Oversight & Government Reform has investigated the process for granting, renewing, and monitoring security clearances. Committee staff met with representatives of all major stakeholders in the process, including the Office of Personnel Management (OPM), the three contractors performing field investigation services, adjudicators from the Department of Defense (DOD), and private and public companies that employ cleared individuals. All parties cooperated with the Committee's investigation and provided candid observations on improving the process.

Congress last reformed the security clearance process in 2004, with passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). Enacted in response to large delays in investigating and adjudicating clearances, IRTPA, in part, requires government agencies to complete 90 percent of their clearance determinations in an average of 60 days, with investigations completed in an average of 40 days, and adjudications in an average of 20 days.[79] By all accounts, IRTPA has greatly improved the timeliness of security clearance investigations.

The security clearance process involves six phases: (1) the determination of whether a position requires access to classified information;[80] (2) an applicant's submission of required materials and submission by the agency of a request for a background investigation; (3) background investigation by OPM or an OPM contractor; (4) adjudication by the requesting agency; (5) an appeal, if a clearance is not granted;[81] and (6) renewal after a federally-mandated period of time.[82]

The Committee found that investigative processes and quality control policies and procedures were lacking in numerous areas. Had more thorough processes been in place at the time of the Alexis investigation, then adjudicators would have had a better picture of his activities before granting or denying him a security clearance.

---

[79] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458. The 40 day investigative standard applies to secret clearance investigations. ODNI has established an 80-day investigative standard for top secret clearance investigations. Transcribed Interview of Merton Miller, Associate Director, Federal Investigative Services (Jan. 8, 2014) at 201 [hereinafter Miller Tr.].

[80] The Committee's investigation did not examine in detail whether certain positions require a security clearance, or whether the overall number of clearances should be reduced. The Committee supports ongoing efforts to better determine which positions require security clearances.

[81] The Committee's investigation did not examine in detail the appeals aspect of the security clearance investigation process.

[82] *See, e.g.*, S. Comm. on Homeland Security &Gov't Affairs, Subcomm. on Oversight of Gov't Mgmt, the Fed. Workforce, and the Dist. Of Columbia, *Hearing on Personnel Clearances*, 110th Cong. (May 22, 2008) (Statement of Brenda Farrell) at 9.

Legislative action, however, cannot fix all aspects of this process. In 2012, 4.9 million Americans—over 1.5 percent of our country's population—held security clearances. The Executive must study whether so many clearances are necessary, and find ways to better determine whether someone needs access to classified materials or spaces. The Executive should take steps to reduce the over-classification of information, which would reduce the number of clearances needed. Another possible solution is to create a system of temporary clearances that expire after a pre-determined amount of time. Ensuring that only those who need actually need security clearances receive clearances would go a long way to reducing the pressures on the investigation and adjudication processes.

A. Initiation of a Security Clearance Investigation

Once an agency determines that a position requires access to classified information, the individual completes Standard Form (SF) 86, Questionnaire for National Security Positions, any necessary releases and certifications, and provides a copy of his or her fingerprints. In most cases, the agency submits a request for investigation to OPM, and pays for the investigation up front—before receiving the investigative product.[83] Federal Investigative Services, a division of OPM, manages the process for the majority of all security clearance investigations.

The applicant must complete the SF-86 accurately. Failure to provide full and accurate information may not only delay the investigation and adjudication of the case, but could also raise questions about the applicant's suitability for a security clearance. Aside from delaying the investigation, however, there are few repercussions for applicants who intentionally falsify information on an SF-86.[84] The relevant criminal statutes are rarely enforced.[85]

Once the applicant sends all necessary information to OPM, OPM enters it into the Personnel Investigations Processing System (PIPS),[86] OPM's primary fieldwork scheduling and management software. OPM then officially opens the investigation and begins scheduling all necessary work to field personnel. PIPS performs some scheduling automatically; USIS contract

[83] Proceeds paid by agencies for security clearances go into a revolving fund that funds the operations of Federal Investigative Services (FIS), the division of OPM that manages the security clearance process. Through this investigation, the Committee learned that the revolving fund has never been audited. Miller Tr. at 36. The Committee supports efforts to increase oversight of FIS' revolving fund.

[84] Miller Tr. at 85-86. During the course of this investigation, the Committee learned that in addition to applicants withholding information from the SF-86, it is not uncommon for recruiters or other federal employees completing the SF-86 on behalf of an applicant to omit or otherwise falsify information. OPM not only provides information to DOD on suspected falsification by recruiters, but also refers such information to OPM's Office of the Inspector General.

[85] During its investigation, the Committee learned that it is rare for an applicant or recruiter to receive any sort of punishment for intentionally falsifying a SF-86. Federal law, however, provides that making a "materially false, fictitious, or fraudulent" statement to the U.S. government may be punished by a fine or a period of imprisonment. 18 U.S.C. § 1001. The instructions for completing the SF-86 include this warning.

[86] USIS employees working on a support services contract perform a quality review of documentation submitted by an applicant to make sure that all parts are complete. Miller Tr. at 43. The USIS support services contract is a separate contract from the fieldwork services contract.

employees working on the support services contract manually schedule other parts of the field work.[87]

Some aspects of the investigation, such as automated agency checks, described below, occur entirely online. OPM staff in the Investigations Support Group perform this work.[88] Merton Miller, Associate Director, Federal Investigative Services, testified about the way that relevant records are obtained via an automated system. He stated:

> There was a process we call consolidated leads. So when we could obtain a record in an automated way, reaching out to a statewide system or an agency system to actually obtain the information, we centralized that process. So if an investigation requires certain leads that can be done in an automated way we have folks that do the consolidated leads. They reach out, obtain it in an online fashion, update our record system, PIPS, with the results of that search, and it becomes part of the investigation.[89]

Field work is assigned internally at OPM or to contract investigators. Three companies hold contracts to perform investigative services on behalf of OPM—U.S. Investigations Services, LLC (USIS), CACI International Inc (CACI), and KeyPoint Government Solutions, Inc. (KeyPoint).[90] When scheduling work among these four entities, OPM first ensures that its own field investigators, who make up approximately 30 percent of the total investigative workforce, are at capacity. OPM then assigns investigative field work to one of the three contractors based on a combination of price, quality, capacity, and timeliness. OPM determines the capacity of contractors by tracking the amount of work currently in progress.[91] Contractors, however, described the process of assigning work as a "non-transparent formula" dictated by price.[92]

Although Contractors are currently paid a set price for each investigation, not all investigations are the same. Some Top Secret investigations take substantially more time than others. Accordingly, one contractor recommended that OPM create tiers of prices based on the complexity of the case.[93] Contractors also recommended that agencies improve their forecasting of required investigations to OPM, so that OPM can provide better forecasting to the contractors.[94] OPM similarly expressed to the Committee that it is attempting to work with agencies in an effort to improve their forecasting.[95]

---

[87] Miller Tr. at 63-64.
[88] *Id.* at 86-87.
[89] *Id.* at 17.
[90] The fieldwork contracts are indefinite delivery/indefinite-quantity firm fixed unit price contracts. Each contract has one base period and four option periods. The base period for each contract began on December 1, 2011. The total value of all three contracts over five years is $2.45 billion.
[91] Briefing by OPM FIS, to H. Comm. on Oversight & Gov't Reform Staff (Oct. 7, 2013).
[92] Contractor 1 Briefings to H. Comm. on Oversight & Gov't Reform [hereinafter Contractor 1 Briefings]; Contractor 3 briefings to H. Comm. on Oversight & Gov't Reform [hereinafter Contractor 3 Briefings].
[93] Contractor 3 briefings.
[94] Contractor 1 briefings, Contractor 3 briefings.
[95] Miller Tr. at 29-30.

Currently, either a contractor or OPM handles all field work for a single investigation.[96] It is not possible to break down an investigation and assign work to contractors or federal employees based on resources or location. As a result, on occasion OPM finds that contractors move personnel into a location because they need more capacity there while OPM moves its own investigators out of the same location because their capacity is needed elsewhere.[97] According to Merton Miller, the ability to break down aspects of an individual investigation and have multiple contractors working on the same investigation would allow OPM to manage workflow and capacity more efficiently and to lower costs.[98] While OPM's current technology does not support division of investigations, OPM explained to Committee investigators that it hopes to gain this capacity through future technology upgrades.

B. Field Investigation and Quality Review of a Security Clearance Application

i. Investigator Field Work

OPM and contract field investigators perform many tasks, from obtaining educational, legal, and employment records, to interviewing applicants and people who know them. Both OPM and contract investigators are trained to the same standards promulgated by OPM, and perform the same work.

Within a single investigation multiple employees of one contractor or OPM are assigned to work on the investigation.[99] For example, one employee might conduct a law check, another employee might conduct a credit check, and a third employee might conduct a subject interview. These employees, however, have little, if any, contact with one other during the course of the investigation.[100] Case message notes regarding the investigation, which are later destroyed, may be shared over PIPS.[101] The shared notes are the extent of the contact among the employees performing the investigation. Assigning discrete investigative tasks to employees who are isolated from one another increases the likelihood pieces of critical information could slip through the cracks.

During this investigation, Committee staff interviewed all field investigators who worked on the Alexis security clearance investigation, and had numerous meetings with OPM and contractors in order to learn the investigative process in greater detail. This section focuses on the current procedures for issues covered in the proposed legislation accompanying the report, as well as quality control procedures for both the contractors and OPM.

---

[96] *Id.* at 89-90.
[97] *Id.*
[98] *Id.* at 89-91.
[99] Contractor 1 Briefings.
[100] Interview of [Alexis Investigator 1] (Oct. 18, 213); Interview of [Alexis Investigator 2] (Oct. 22, 2013); Interview of [Alexis Investigator 3] (Oct. 25, 2013).
[101] *Id.*

a. Law Enforcement Checks

Field investigators perform a legal check on all applicants applying for a Secret or Top Secret security clearance. FBI fingerprint and name databases identify whether an applicant has been arrested in the United States.[102] In addition, field investigators obtain information from local law enforcement jurisdictions where the applicant has lived, worked, or attended school for a determined amount of time, as well as known localities where the applicant has been arrested or convicted of a crime.[103] If an applicant disclosed an arrest or conviction on the SF-86, or if investigators uncover an arrest or conviction during the course of the investigation, under current practices the investigator must verify certain information, including the disposition of the arrest.[104]

Federal law requires local law enforcement and other law enforcement agencies to provide criminal history information to security clearance investigators.[105] In relevant part, the law states:

> Upon request by the head of a covered agency, criminal justice agencies shall make available criminal history record information regarding individuals under investigation by that covered agency for the purpose of determining eligibility for any of the following:
>
> (A) Access to classified information.
> (B) Assignment to or retention in sensitive national security duties.
> (C) Acceptance or retention in the armed forces.
> (D) Appointment, retention, or assignment to a position of public trust or critical or sensitive position while either employed by the Government or performing a Government contract.[106]

An OPM pamphlet explaining to law enforcement agencies how to cooperate with federal investigations describes the information an investigator will request:

> The Investigator will want to know if the subject of the investigation has a criminal history record with your department. A criminal history record includes felonies, misdemeanors, traffic offenses or other violations of law that may or may not have resulted in a conviction. The Investigator will request pertinent information about each offense, including the date/place of the offense, statement of the actual charge, circumstances of the offense, and its disposition. In addition, the Investigator may ask for a copy of the police report. Please note that the alleged or suspected

[102] Miller Tr. at 101.
[103] *Id.*
[104] *Id.*
[105] 5 U.S.C. § 9101.
[106] 5 U.S.C. § 9101(b)(1).

> criminal activity is pertinent whether or not it led to an arrest or conviction.[107]

However, because the law does not specify what information must be provided, local law enforcement agencies may decide what criminal history information to provide despite these instructions from OPM.[108] As a result, different localities provide different information in response to investigators performing the legal checks.

Many local law enforcement agencies do not provide records to OPM investigators at all. As such, these agencies are not in compliance with federal law. In 2009, the Department of Justice, on behalf of OPM, successfully sued the State of California over its failure to disclose complete criminal history records to security clearance investigators.[109] OPM maintains a list of local law enforcement jurisdictions that do not fully cooperate with security clearance investigators. That list currently includes more than 450 jurisdictions, ranging from small counties to entire states, and including numerous areas with large populations.[110]

Internal OPM notes document reasons as to why specific law enforcement agencies do not cooperate, ranging from "does not cooperate in any way, shape or form" to "staff told agent it was 'illegal' for her to request records and threatened her with arrest if she returned."[111] Some jurisdictions require investigators to use court records to obtain information about criminal activity. This method is problematic because a court record may not exist if an individual was arrested but not charged,. In addition, court records will not necessarily include information about the factual basis for an arrest. Other jurisdictions require investigators to use databases not validated by OPM.

Even statewide databases that OPM has approved provide only cursory information, including the date of offense, charge, and disposition. These databases do not include information about the underlying facts that lead to an arrest.[112] Under current practice, investigators are considered to have successfully completed a lead when they determine the disposition of an arrest. Investigators do not appear to be under any obligation to obtain—and jurisdictions face no penalties for not providing—the specific information about the actions by the applicant that led to the arrest. As was the case with Aaron Alexis' 2004 arrest for malicious mischief, there can be a large gap between the actions leading to the arrest and the ultimate disposition of a case.

---

[107] *Law Enforcement & The U.S. Office of Personnel Management*, Federal Investigative Services (June 2013).
[108] *See* 5 U.S.C. § 9101(b)(1); *see also* Miller Tr. at 105 ("However, how they provide [the information] and the level of detail that they provide ... is not specified in the law.").
[109] U.S. v. The State of Cal., 2:06-cv-2649-GEB-GGH, 2007 U.S. Dist LEXIS 85845 (E.D. Cal. Nov. 7, 2007).
[110] OPM Master List of Uncooperative Local Law Enforcement Agencies [OPM014538-OPM014547].
[111] *Id.*
[112] Miller Tr. at 110-111. Before permitting investigators to utilize a database to obtain criminal history records, OPM compares the reliability of the information in the database to physical collection of records obtained by OPM investigators and contractors. Several thousand comparisons are performed. When reliability is in the 98th or 99th percentile, OPM will permit use of the database as a source for obtaining criminal history information. *Id.*

Though Aaron Alexis did not disclose his 2004 malicious mischief arrest on his SF-86, both the FBI database check and a local law check uncovered the arrest.[113] The investigator performing the local law check used the Washington Statewide Database to determine that the charges against Alexis had been dropped. Had the investigator taken additional steps to obtain the arrest record, it likely would have been provided to the investigator.[114] As the investigator only had access to the information in the Washington Statewide Database, only minimal information was included in Alexis' investigative file.[115]

DOCKET # 204022684 **OFFENSE DATE** 06/03/04
CHARGING AGENCY KING COUNTY JAIL
CHARGES
MALICIOUS MISCHIEF
COURT HISTORY
ON 6/4/2004 THE CASE WAS FILED IN KING COUNTY DISTRICT COURT (WEST DIVISION) WITH AARON ALEXIS CHARGED WITH MALICIOUS MISCHIEF.
ON 6/7/2004 THE CASE WAS DISMISSED DUE TO CHARGE NOT BEING FILED.
THE CASE IS CLOSED.
DISPOSITION DATE 06/07/04
DISPOSITION
THE CASE WAS DISMISSED.

ITEM: 007 COLLATERAL ITEM(S): 005 **SOURCE: 004**
NAME KING COUNTY SHERIFF, KING COUNTY SHERIFF 516 THIRD AVE, 516 THIRD AVE, SEATTLE, WA 98104
LAW ENFORCEMENT-ARREST
PROVIDER [redacted] SRS
SF RELEASE
TELEPHONE TESTIMONY
NO RECORD

KING COUNTY SHERIFF HAD NO RECORD OF THE SUBJECT'S 6/3/2004 MALICIOUS MISCHIEF OFFENSE. SEE WASHINGTON STATEWIDE DISTRICT AND MUNICIPAL COURTS (ITEM 005) FOR DISPOSITION.

ITEM: 007 INVESTIGATOR'S NOTE **SOURCE: 005**

RECORD FROM KING COUNTY SHERIFF OBTAINED VIA FAX PER STANDING ARRANGEMENT WITH AGENCY.

The 2004 arrest record, however, contained substantially more information.[116]

[113] Investigative Report on Aaron Alexis, at 17, 19, 30 (closed Aug. 24, 2007) [hereinafter Alexis Investigative Report].
[114] H. Comm. on Oversight & Gov't Reform, *DC Navy Yard Shooting: Fixing the Security Clearance Process*, 113th Cong. (Feb. 11, 2014) (Testimony of Hon. Patrick McFarland, Inspector Gen., U.S. Office of Personnel Mgmt.).
[115] Alexis Investigative Report at 18.
[116] Seattle Police Record at 3, 4.

05-07-04 1300 Case assigned by Sgt. [redacted] for follow-up. ***CASE SUMMARY***: On May 6th, 2004 at 0800 hours, **Aaron Alexis** exited his home located at 5523 13th Ave S. then walked next door where construction workers were building a new residence. **Alexis** aimed his Glock 30 .45 caliber pistol at the rear tires of a vehicle that belonged to construction worker [redacted] He then fired three rounds from his weapon at the rear wheels, which damaged both tires and wheels. After firing the weapon **Alexis** stood next to the vehicle long enough for the workers to investigate the shots and observe him conceal the firearm under his jacket, [redacted] stated that neither prior provocation nor words were exchanged between he and Alexis.

06-03-04 1000 I obtained a post-Miranda confession from **Alexis**. He explained how he perceived [redacted] had disrespected him and how that perception lead to what **Alexis** described as a "black-out" fueled by anger. He said that he didn't remember pulling the trigger of his firearm until about one-hour later. **Alexis** also told me how he was present during the tragic events of September 11th, 2001 and how those events had disturbed him. **Alexis** was then booked for Malicious Mischief.

06-04-04 0930 I received a P/C from **Alexis**' father who lived in New York City. He was curious about his son's predicament and since I had prior approval from **Aaron Alexis**, I explained to him the facts of the case. Mr. Alexis then told me that his son had experienced anger management problems that the family believed associated with PTSD. He confirmed that his son was an active participant in rescue attempts of September 11th, 2001.

As discussed in more detail below, because an actual copy of the criminal record resulting from the 2004 arrest was not obtained, the investigator who interviewed Alexis only knew that he had been arrested in 2004, that the case had been dismissed, and that Alexis had not disclosed the arrest on his SF-86. The investigator had no knowledge of the cause of the arrest, or that Alexis' father believed that his son may have post-traumatic stress disorder.

b. Mental Health Issues Presented During an Investigation

An applicant's decision to seek mental health treatment should not, and does not, disqualify him or her from receiving a security clearance. This information, however, is important in understanding the "whole person" concept, which is critical in informing the adjudicator's determination of whether an individual should receive a security clearance. The current version of Question 21 on the SF-86 is as follows:[117]

[117] Standard Form 86, OMB No. 3206 005 (Dec. 2010).

Standard Form 86, Question 21 – Revised
(Feb 2008)

Mental health counseling in and of itself is not a reason to revoke or deny a clearance.

In the last 7 years, have you consulted with a health care professional regarding an emotional or mental health condition or were you hospitalized for such a condition?

Answer "No" if the counseling was for any of the following reasons and was not court-ordered:

- ***strictly marital, family, grief not related to violence by you; or***
- ***strictly related to adjustments from service in a military combat environment.***

If you answered "Yes," indicate who conducted the treatment and/or counseling, provide the following information, and sign the Authorization for Release of Medical Information Pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

Under current processes, if an applicant answers "yes" to Question 21, then the applicant must sign a HIPAA release that permits an investigator to obtain certain types of information from the treating mental health professional. The mental health professional must answer whether the condition of the person under investigation "could impair his or her judgment, reliability, or ability to properly safeguard classified national security information."[118] If yes, the mental health professional must provide additional information about the treatment.[119]

For Use By Practitioner(s) Only

Does the person under investigation have a condition that could impair his or her judgment, reliability, or ability to properly safeguard classified national security information?

☐ YES ☐ NO

If so, describe the nature of the condition and the extent and duration of the impairment or treatment.

What is the prognosis?

Dates of treatment?

Signature *(Sign in ink)*	Practitioner name	Date signed *(mm/dd/yyyy)*

If an applicant does not truthfully answer that he has consulted with a mental health professional, the information may still be uncovered during the course of the investigation. Miller testified:

[118] *Authorization for Release of Medical Information Pursuant to the Health Insurance Portability and Accountability Act*, Standard Form 86, OMB No. 3206 0005 (Dec. 2010).
[119] *Id.*

> Q. If an applicant currently says that, no, they have not consulted with a mental health professional, is there any way for an investigator to verify that?
>
> A. Maybe. And I'll say that because it depends on the kind of investigation you're conducting. If it's a secret investigation where most of the checks are automated, there is no interviews associated with it, the chances are, no, you would not uncover the mental health history, unless there was an arrest that you uncovered.
>
> If it's a SSBI where you have to provide references, you go talk to employers, coworkers, neighbors, there potentially is a chance that information would be uncovered that, oh, my neighbor told me he was seeing a mental health professional for whatever it might be. So there is potentially -- you know, you could uncover the fact that they were seeing a mental health professional when they didn't. But it's a good chance it will not be uncovered.[120]

Given the difficulty of uncovering such information, however, it is critically important that applicants answer truthfully about any required mental health treatment.

Despite OPM's approval of the HIPAA waiver, some health care providers require applicants to complete a proprietary waiver, claiming that the HIPAA waiver is insufficient.[121] This requirement adds substantial extra time to an investigation, as the investigator must go to the health care professional with the first form, obtain the second form when the first form is deemed insufficient, return to the applicant to complete the form, and then return to the health care professional with the proprietary form completed. This lengthy process increases pressure on investigators to complete their work in a timely manner according to federal law.

In April 2013, OPM requested comments on a potential revision to Question 21 for the purpose of "clarifying support for mental health treatment and encouraging pro-active management of mental health conditions to support wellness and recovery."[122] OPM requested the comments in connection with a comprehensive review conducted by the Director of National Intelligence along with DOD, OPM, and other agencies.[123] The proposed change focuses more on the behavior of the individual, and less on whether or not the person has consulted with a mental health professional.

> **In the last seven (7) years, have you had a mental health condition that would cause an objective observer to have concern about your**

---

[120] Miller Tr. at 154-155..
[121] Briefing by the Department of Defense to H. Comm. on Oversight & Gov't Reform Staff (Nov. 21, 2013) [hereinafter *Nov. 21 DOD briefing*].
[122] Office of Personnel Management, *Submission for Renewal: Information Collection; Questionnaire for National Security Positions, Standard Form 86 (SF 86)*, 78 Fed. Reg. 15755-56 (Mar. 12, 2013).
[123] *Id.* (emphasis in original).

> **judgment, reliability, or trustworthiness in relation to your work?** Evidence of such a condition could include exhibiting behavior that was emotionally unstable, irresponsible, dysfunctional, violent, paranoid, or bizarre; receiving an opinion by a duly qualified mental health professional that you had a condition that might impair judgment, reliability, or trustworthiness; or failing to follow treatment advice related to a diagnosed emotional, mental, or personality condition (e.g., failure to take prescribed medication). These examples are merely illustrative. Merely consulting a mental health professional is not, standing alone, evidence of such a condition.[124]

OPM has adjudicated comments to the proposed change;[125] however, no final changes have been made to Question 21 of the SF-86.

c. Personal Subject Interviews

Not all types of security clearance investigations require a subject interview. While mandatory for Top Secret clearance investigations, a subject interview only takes place during a secret clearance investigation if an issue uncovered during the investigation requires it.[126]

Alexis' national agency check and law check (NACLC) investigation for a Secret clearance normally would not have included a subject interview.[127] However, Alexis' failure to

---

[124] Questionnaire for National Security Positions, OMB No. 3206-0005, DRAFT for 60 Day Notice, http://images.politico.com/global/2013/04/13/clearancedraftqnaire.html.

[125] *See* Office of Personnel Management, *Submission for Renewal: Information Collection; Questionnaire for National Security Positions, Standard Form 86 (SF 86)* 78 Fed. Reg. 42983-86 (July 18, 2013).

[126] Miller Tr. at 184-85.

[127] OPM, Background Investigations, Federal Investigations Notices, Letter No. 97-02 (July 29, 1997), http://www.opm.gov/investigations/background-investigations/federal-investigations-notices/1997/fin97-02/. Investigative standards recommended by the Security Policy Board and approved by President Clinton in 1997 set the following guidelines for the use of NACLC:

> The NACLC will be used as the initial investigation for contractors at the Confidential, Secret, and L access levels. It will also be used as the reinvestigation product for both contractors and Federal employees at the same access levels.
>
> This new product includes:
>
> Basic National Agency Checks (Security/Suitability Investigations Index, Defense Clearance and Investigations Index, fingerprint classification, and a search of the Federal Bureau of Investigations [sic] investigative index).
>
> Credit search covering all residence, employment, and education locations during the last 7 years.
>
> Law Checks covering all locations of residence, employment, and education during the last 5 years and to all locations of admitted arrest. If 35-day service is requested, all law checks will be scheduled by Record Search. If 75-day service is requested, law checks

disclose his 2004 arrest, and his failure to disclose thousands of dollars in debts triggered the interview. At the time of Alexis' interview, investigators only discussed the trigger issues.[128] Thus, Alexis' interview only discussed his 2004 malicious mischief arrest and his financial debts. The interviewer was not allowed to cover any other topics.

Today, if an interview is required for secret-level investigations, or if a second interview is required for persons applying for a top secret clearance, the investigator will go through every question on the SF-86 to verify the information provided by the applicant.[129] Investigators are also permitted to probe the subject further if the investigator believes the subject to be lying or otherwise hiding information.[130]

This improvement is a step in the right direction, but if the investigation fails to uncover factual information about relevant issues, then there is still no way to verify the applicant's statements. Aaron Alexis told the investigator conducting his interview that he "deflated" the tires on a vehicle, resulting in his 2004 arrest.[131] The investigator's interview note stated:

> The subject and the male person had been aggravating each other by taking retaliatory action toward each other's parked cars. The male person had put some foreign substance in the subject's gas tank and **the subject retaliated by deflating the male person's tires**.
>
> * * *
>
> The subject committed this offense because he was retaliating for being intimidated by the male person. The subject does not intend to repeat this type of behavior because he would avoid any confrontation and notify authorities if a similar situation were to occur in the future.[132]

Alexis' description of the event omits key information included in the police report. He did not tell the investigator that he used a gun to shoot out the tires. Nor did he tell the investigator that he committed this act during a self-described "black out fueled by anger," that he did not respond to officer's attempts to contact him multiple times, or that his family believed he had anger management issues associated with PTSD.[133]

The investigator was unaware that Alexis was lying—and there was no way for him to know unless he had seen the police report. The field investigator who conducted the Alexis interview told the Committee that, had he known that a gun was involved in Alexis' 2004 arrest, he would have specifically asked Alexis about the gun and included a note in his report about

---

will be scheduled by a combination of inquiry and record coverage. (See Service Availability below for additional information about law checks).

[128] Miller Tr. at 186.
[129] *Id.*
[130] Interview of [Alexis Investigator 3] (Oct. 25, 2013).
[131] Alexis Investigative Report at 20.
[132] *Id.* (emphasis added).
[133] Seattle Police Report at 4.

the use of a gun.[134] Similarly, had he known the underlying facts of the arrest, he would have challenged Alexis' description of the events, and would have included a note in his report that Alexis was not fully truthful when he first described the incident.[135]

When investigators are unable to uncover factual details about prior criminal activity, then the applicant is able to create a set of facts that fit the arrest, or leave out key details that would cast them in a negative light. Secret level investigations present a particular challenge in this regard because no other sources—family members, neighbors, or coworkers—are interviewed. As seen with Aaron Alexis, Secret clearance-holders maintain access to controlled spaces like the Washington Navy Yard, Fort Hood, and other secure facilities around the world.

In the near future, OPM plans to implement a system that allows for digital images of any hard copy records obtained during an investigation to be uploaded into the OPM system for review by other investigators.[136] But such imaging is useless if investigators fail to obtain the records in the first place. Alexis' interviewer, for example, told the Committee that he had never received a police report before interviewing an applicant about a criminal issue.[137] Nor did he recall ever receiving substantive records on any topic before conducting an interview.[138] Such a lack of critical information severely compromises the quality of the background investigation as a whole.

ii. Quality Review of Contractor Investigations

Numerous studies and audits have been completed by GAO and OPM's Office of the Inspector General about the quality of OPM security clearance investigations.[139] The results are consistent – OPM has a problem maintaining the quality of its investigations. A 2009 GAO study, for example, found that 87 percent of OPM investigations were incomplete.[140] While OPM and the Contractors have processes and procedures in place to review investigative files for quality and completeness, more needs to be done to improve quality in this area.

During the course of this investigation, the Committee learned that OPM, DOD, and numerous other agencies are currently participating in a Quality Assessment Working Group that

---

[134] Interview of [Alexis Investigator 3] (Oct. 25, 2013).
[135] *Id.*
[136] Miller Tr. at 186.
[137] Interview of [Alexis Investigator 3] (Oct. 25, 2013).
[138] *Id.*
[139] *See, e.g.*, Gov't Accounting Office, *Background Investigations: Office of Personnel Management Needs to Improve Transparency and of its Pricing and Seek Cost Savings* (Feb. 2012) (GAO-12-197); U.S. Office of Personnel Mgmt., Office of the Inspector General, *Audit of the Quality Assurance Process Over Background Investigations* (June 22, 2010) (Report 4A-IS-00-09-060); Gov't Accounting Office, *DOD Personnel Clearances: Comprehensive Timeliness Reporting, Complete Clearance Documentation, and Quality Measures are Needed to Further Improve the Clearance Process* (May 2009) (GAO-09-400); U.S. Office of Personnel Mgmt., Office of the Inspector General, *Audit of the Security of Personally Identifiable Information in the Federal Investigative Services Division of the U.S. Office of Personnel Management* (Apr. 2009) (Report 4A-IS-00-08-014).
[140] Gov't Accounting Office, *DOD Personnel Clearances: Comprehensive Timeliness Reporting, Complete Clearance Documentation, and Quality Measures are Needed to Further Improve the Clearance Process* (May 2009) (GAO-09-400). OPM disputes this figure, instead noting that less than two percent of files are returned to OPM by the agencies for rework. *See* Miller Tr. at 132.

is evaluating quality standards for completed security clearance investigations across the Federal government.[141] The Committee looks forward to receiving the final quality standards and other recommendations made by this group. Outside of creating consistent quality standards, however, OPM must continue to find ways, potentially utilizing new technologies, to improve the quality of its investigations.

Contractors must review each investigative file in its entirety for completeness and quality before sending the file to OPM. This quality review is required under the terms of the contract. Each of the three contractors have internal quality review processes to ensure that investigative files are complete and meet quality standards before they are sent to OPM.[142] If the investigative file is incomplete or a lead has not been exhausted, OPM sends the file back to the field for further investigation.

Since OPM's PIPS system monitors the status of all background investigation cases, if the contractor does not complete a quality review within a certain time period, a case can potentially "auto-release" and go directly into OPM's quality review process without having gone through a contractor review. Miller described this "auto-release" function during a transcribed interview with Committee investigators. He testified:

> A. No, well, the auto release function, to the best of my [knowledge], is auto releases to review, because there are certain timeliness mandates that we have in the system. There is a function in the system that when a contractor or a Fed finishes an investigation, that the system notices, okay, all the items are there, all the ROIs are there. It gives the contractor on their side a certain time period to conduct their initial quality review before they provide it to the Federal staff for our quality review.
>
> If they exceed that time period, the system is scheduled to automatically release it to full Fed review. My understanding, it was put in the system, one, to keep the cases moving and to not allow a backlog in review, contract review side of the house.
>
> Q. So it sounds like there is the potential that a case could be released once all the items are there, but potentially before the contractor has performed their quality review.
>
> A. Their quality review. That's exactly right.[143]

According to Miller, FIS can tell whether a case was auto-released or released by the contractor upon completion of the quality review.[144] Miller testified that, in his opinion, the auto-release function was necessary to the process. He stated:

---

[141] Miller Tr. at 7.
[142] One of the contractors, USIS, is currently under investigation for failing to perform a quality review of investigative files before sending them to OPM for final review.
[143] Miller Tr. at 94.

Q. Is this auto release function still necessary?

A. Oh, it is necessary.

Q. Do you know how frequently it's used?

A. I do not know how frequently it's used.

Q. And why is it still necessary?

A. Timeliness. It is all based on making sure we meet the timeliness mandates of 40 days.[145]

Miller did not express concern that auto-released cases skipped the mandated contractor quality review because "the purpose of the contract review is for us, OPM-FIS, not for our customer . . . because if the contractor's mandated to do a quality review of that case before they turn it over to us, there should be less work on our Federal review staff when they go through it."[146] When a case is auto-released, not only does the case undergo one fewer level of quality review at the contractor level, but any problems with the file found during OPM's quality review process may be held against the contractor.

OPM explained to Committee staff that a contractor has a certain amount of time once all reports of investigation have been submitted to quality review the case before a case is auto-released.[147] One of the contractors, however, told the Committee staff that a case can be auto-released as soon as the last report of investigation is submitted if the case is past the date by which it must be returned to OPM.[148] Based on its investigation, the Committee believes that contractors should have a limited amount of time to perform a quality review once all reports of investigation have been submitted, even if the case is past the critical date.

Investigations performed by OPM employees do not undergo a preliminary quality review as with investigations performed by contractors. Still, OPM does have policies and practices in place to monitor quality before the final review. Quality review for OPM investigations starts with an informal review by an investigator's supervisor. The review process focuses on newer investigators or investigators who need extra assistance. These supervisors are also responsible for supervising and managing the workload of 18 to 22 federal investigators.[149] In short, for field investigations conducted by OPM employees, these informal supervisor reviews take the place of formal quality assurance reviews for field investigations conducted by contractors.

---

[144] *Id.* at 95.
[145] *Id.* at 96.
[146] *Id.* at 96-97.
[147] Briefing by FIS to H. Comm. on Oversight & Gov't Reform Staff (Jan. 17, 2014) [hereinafter Jan. 17 FIS Briefing].
[148] Contractor 1 Briefings.
[149] Miller Tr. at 99-100.

iii. Final Quality Review by OPM FIS

Before investigations are complete and the results are delivered to the client agency, FIS' Investigations Quality Group reviews all background investigations, whether conducted by a contractor or by OPM investigators. OPM has approximately 300 federal employees who perform these reviews.[150] Miller described the quality review process during his interview. He stated:

> A. So they evaluate the investigation to the investigative standards to make sure all the piece parts are there, that issues that are identified during the investigation are resolved for issue resolution, and that it is complete. If there is an item missing, for instance, if there is an employment that is not in the case, there has got to be a notation as to why that employment was not obtained. So they do the final overall review of the investigation before it gets delivered.
>
> Q. And is that of every investigation?
>
> A. Yes. Every investigation that OPM does goes through a Federal controlled quality review. We have 50 contractors that are responsible for doing a quality review of low level cases.[151]

OPM's quality reviewers examine all components of the investigation, including all reports of investigation, to ensure that the investigation is complete. OPM's quality review also examines whether all issues were resolved and all leads were covered. Miller stated:

> Q. [D]oes the quality review performed by OPM before it goes to the customer, does that look at the substance of the investigative report. So, for instance, does it look at whether a lead was thoroughly covered?
>
> A. Yes. And typically that section of the quality review is called issue resolution. You know, if there was issues [sic] identified, did we resolve it. In other words, did we explain the circumstances and the background to it.[152]

OPM quality reviewers send investigations back to the field for rework approximately 16 percent of the time.[153]

---

[150] Briefing by OPM FIS to H. Comm. on Oversight & Gov't Reform Staff (Oct. 7, 2013).
[151] Miller Tr. at 13-14. The approximately 50 contractors are USIS employees reviewing certain types of cases as part of the support services contract.
[152] *Id.* at 177.
[153] Briefing by OPM FIS, to H. Comm. on Oversight & Gov't Reform (Oct. 7, 2013).

Cases that involved only automated records checks and have no leads sent to the field, include Secret-level NACLC or NAC investigations.[154] The Closing Authorization and Support Team (CAST), a group of USIS employees working on the support services contract, perform the quality check on these investigations.[155] Miller has lowered the number of cases that undergo CAST review in the past two years.[156] Today, CAST reviewers perform quality review on special agreement checks[157] and cases that have no issues.[158] CAST reviewers cannot clear cases that have any issues—such cases must be sent to OPM employees for final review.[159] Federal employees review nearly all, if not all, cases with field work.[160]

iv. Integrity Assurance

There have been unfortunate instances in which investigators—both OPM and contract—have intentionally falsified investigation data. To date, 21 investigators have either pleaded to, or been found guilty of, falsification of data.[161] To combat falsification, OPM and the contractors each employ programs to randomly re-contact sources that provided information on applicants to determine if the investigator actually contacted them, and whether the investigator followed proper procedures.[162] OPM also finds potentially falsified data through supervisor reviews, external referrals, audits, and the quality review process.[163]

Under the terms of their contracts with OPM, the contractors must also randomly re-contact at least three percent of sources contacted by each contract field investigator. OPM performs a similar review, re-contacting at least three percent of sources for each OPM and contractor field investigator each month.[164] If a contractor discovers potential misconduct on the part of one of its employees, it must report the misconduct to OPM within 24 hours.[165] OPM and contractors also perform operational and compliance audits to determine, among other things, that investigative files include all relevant information.

If OPM receives or develops an allegation that the investigator either did not contact the source, or did not accurately report information the source provided, then FIS either open an internal inquiry or allows the contractor to open an inquiry to determine whether the allegation can be substantiated.[166] The Integrity Assurance Division, using either OPM or contract

---

[154] Miller Tr. at 67.
[155] *Id.*
[156] *Id.* at 136-37.
[157] Special agreement checks are single or multiple record checks that do not constitute a complete investigation.
[158] Miller Tr. at 138-39.
[159] *Id.* at 68-69. The PIPS software can determine whether any issues arose during the investigation through the use of issue codes. *Id.*
[160] *Id.* at 67.
[161] *See*, Falsification Convictions [OPM011102]. To date, eleven federal investigators and ten contract investigators have been convicted for falsifying information on security clearance investigations. *Id.*
[162] Miller Tr. at 71. Contractor 3 briefing (Contractor 3 representatives told the Committee that, while the contract requires a 3 percent recontact rate, their recontact rate is closer to 10 percent); Contractor 2 briefing (Contractor 2 representatives told the Committee that their recontact rate is approximately 6 percent).
[163] Jan. 17 FIS Briefing.
[164] Miller Tr. at 142.
[165] *Id.* at 144-45.
[166] *Id.* at 72.

investigators, will re-run investigations performed by the individual suspected of falsification. If the allegations are substantiated, a contract investigator is immediately removed from the contract, while an OPM employee is placed on administrative leave. At that point, Integrity Assurance will re-investigate all investigative work performed by the individual during a pre-determined period of time.[167]

Two contractors explained to the Committee that if OPM investigates one of their investigators, they do not always receive the results of OPM's investigation—particularly if a criminal investigation emerges.[168] OPM charges the contractor for the cost of OPM's investigation, but does not itemize the costs incurred for the investigation. If a contract employee is under OPM investigation, OPM should keep the contractor informed not only of the allegations against the employee, but also of the outcome of the investigation, and the means by which the employee falsified information, if such conduct occurred. Such information is necessary in order for contractors and OPM to better train employees.

C. Adjudication by the Department of Defense

Once the investigative file has been assembled and quality checked by OPM, it is sent to the requesting agency for adjudication. The Department of Defense, OPM's largest customer, adjudicated approximately 680,000 cases in 2013, and approximately 767,000 cases in 2012. DOD-CAF (Centralized Adjudicative Facility), the centralized adjudicating agency for the Department, employs 460 adjudicators.[169]

The Department of Defense's adjudicative process has multiple levels of review. In the absence of any derogatory information contained in an applicant's file, a certified first-level adjudicator has the authority to decide whether to grant a clearance.[170] The existence of derogatory information requires at least a second-level review. A second-level review is also necessary whenever the applicant has foreign citizenship, the initial adjudicator requests a second level review, or the case involves a warning or conditional letter (described below) requiring a supervisor's signature.[171] A third-level review is necessary if the first and second level adjudicators disagree on how to adjudicate the case, if they both agree that clearance should be denied, or if the case is particularly difficult.[172] A fourth-level review by the Branch Chief may also be necessary.[173]

Approximately 25 percent of secret clearances are "zestfully clean," a description both DOD and OPM used to indicate that no issues arose in the course of the investigation.[174] In

---

[167] *Id.* at 72.
[168] Contractor 3 briefing; Contractor 1 briefing.
[169] Briefing by the DOD to H. Comm. on Oversight & Gov't Reform Staff (Oct. 22, 2013). Ninety-five percent of DOD adjudications are conducted at the DOD-CAF. *Id.*
[170] Nov. 21 DOD Briefing. A first-level adjudicator can adjudicate cases with "minor" issues, such as traffic tickets. *Id.* A first-level adjudicator, who is sometimes only at the GS-7 level, is also able to grant Top Secret clearances.
[171] Adjudicator 2 Interview.
[172] *Id.*
[173] *Id.*
[174] Miller Tr. at 69-70; Nov. 21 DOD Briefing.

these cases, a computer reviews the file and has the ability to grant the clearance; since there is nothing for the first-level adjudicator to review, no such review takes place.[175]

If an investigative file is not complete when delivered by OPM to the Department, then the adjudicator is supposed to send the file back to OPM for further investigation. The Department of Defense noted that while it only sends approximately two percent of cases back to OPM for additional work, approximately 31 percent of cases delivered by OPM contained deficiencies.[176] Department representatives stated it would in fact take more time to work with OPM to determine if a file was deficient, and then correct the deficiency, than it would take to simply obtain the information themselves. In addition, the Department and OPM often disagree on whether an investigation is deficient, and OPM charges the Department for any additional information it seeks on an applicant. Therefore, the Department has created its own internal process to correct these deficiencies, usually by obtaining information straight from the applicant.

The Committee spoke with both of the DOD adjudicators who granted Alexis' clearance. They explained that 70 to 80 percent of all investigative files sent by OPM are missing at least some information.[177] The file is frequently missing financial information, such as documentation of debt repayment or payment arrangements.[178] Both adjudicators expressed a preference to obtain missing information from the applicant directly via the applicant's command rather than going back to OPM for the information.[179] This preference was not due to cost, but timeliness. Requesting additional information from OPM requires that OPM reopen the case, contact and potentially interview the subject, close the case, and send the information back to the adjudicator.[180] The two adjudicators explained that they only go back to OPM if the missing information is something that OPM must provide, such as a missing subject interview or a missing FBI legal check.[181]

Both adjudicators, and other DOD representatives, told the Committee that it would be extremely helpful if investigative reports to included actual records, including arrest records and financial records showing timely debt repayment, as opposed to simply an investigator summary of the records.[182] OPM, however, told the Committee that any records obtained in the course of an investigation are sent to the adjudicating agency with the investigative report.[183] It is therefore not clear whether records obtained in the course of an investigation are actually sent with the investigative report to the adjudicator.

In numerous meetings with the Committee, Miller expressed a desire for more open communication with DOD-CAF about areas for improvement in OPM investigations. Miller

---

[175] Nov. 21 DOD Briefing.
[176] *Id.*
[177] Adjudicator 1 Interview (Dec. 6, 2013); Adjudicator 2 Interview (Dec. 6, 2013).
[178] *Id.*
[179] *Id.*
[180] Adjudicator 2 Interview.
[181] Adjudicator 1 Interview; Adjudicator 2 Interview.
[182] Nov. 21 DOD Briefing; Adjudicator 1 Interview; Adjudicator 2 Interview.
[183] Jan. 17 FIS Briefing.

also explained that adjudicators often request information that is not part of a certain type of investigation. He stated:

> It's a secret case, and they've got all the elements of that secret case, but because they don't want to make an adjudicated decision without some additional investigative work that goes beyond the investigative product that was requested, they'll come back to us and say, I know you don't do a law check in these cases, but go do a law check on this, and that is an RSI. It's not -- it's not because it didn't make standard. It's because they want additional information beyond the investigation that was requested. And that -- that happens frequently. [184]

If an investigative file leads an adjudicator to believe that the applicant may have mental health issues, then the adjudicator can order a mental evaluation by an approved psychiatrist. The second-level adjudicator for Alexis' case said that, if the investigative file included a notation that family members said Alexis may have PTSD, then the adjudicator would have likely ordered a mental evaluation prior to adjudication. [185]

Adjudicators can grant clearance to applicants whose investigations showed financial or other issues with a "warning letter" or "conditional letter." These letters are sent to the applicant's command within the Department. A warning letter makes the applicant and the applicant's command aware of issues uncovered during the investigation, and informs the applicant that the issues need to be resolved by the next evaluation.[186] A conditional letter requires an additional step before a full clearance is granted. For example, a conditional letter may grant an applicant a clearance on the condition that the applicant will take steps to improve his or her finances in the next six months.[187] Further, a conditional letter requires some sort of response from the applicant. If the applicant does not respond, then the file is flagged for the security officer.[188] A warning letter does not include follow-up by DOD-CAF; instead, the applicant and the applicant's command must report any relevant information. In the case of Aaron Alexis, despite several instances of improper conduct by Alexis, neither he nor his command reported anything to the adjudicators.

Contractors employing cleared individuals do not receive copies of warning letters. The letter is instead sent to the security officer of the agency holding the contract. One adjudicator told the Committee that contract employers should be made aware of any warning or conditional letters.[189] The Experts, the company where Alexis was employed at the time of the Navy Yard shooting, told the Committee that the company did not receive a copy of Alexis' warning letter when he started working there, nor was the company aware that a warning letter accompanied his original security clearance.[190] Further, representatives of The Experts told the Committee that

---

[184] Miller Tr. at 132.
[185] Adjudicator 2 Interview.
[186] *Id.* In the case of Aaron Alexis and other Secret-level clearance holder, the "next evaluation" would occur in ten years.
[187] *Id.*
[188] *Id.*
[189] *Id.*
[190] Dec. 19 Experts Briefing.

they unaware of any instances in which they had been informed that a warning or conditional letter accompanied the clearance of one of their cleared employees.[191]

D. Periodic Reinvestigation

An applicant who receives a clearance does not undergo reinvestigation for five to fifteen years, depending on the clearance.[192] An applicant must "self-report" any derogatory information in between clearance investigations. Aaron Alexis was arrested several times after he received his Secret clearance. Apparently, neither Alexis nor his commanding officers reported those arrests. His commanding officers clearly knew about the incidents, as evidenced by the non-judicial punishments filed against Alexis.

New federal investigative standards will require reinvestigation of Secret clearances every five years instead of every ten years.[193] Yet, even this shortened time period is insufficient. As discussed below in Part III, a continuous investigation system is long overdue.

IV. Legislative Improvements: How to Patch Holes in the Process

Given the sheer volume of background checks that OPM conducts annually, issues are bound to arise on occasion. No system will be foolproof. However, the Committee's investigation uncovered a number of holes that exist in the federal security clearance process, and it is because of these holes that an individual like Aaron Alexis was able to slip through the cracks and receive a clearance. In the coming weeks, the Committee plans to consider legislation to patch some of these holes, so that fewer issues—and fewer Aaron Alexises—will occur in the future. Aspects of this legislation under consideration by the Committee are described below.

A. Continuous Evaluation

Under current law, a person holding a Top Secret clearance must be reinvestigated every five years in order to continue holding the clearance, those holding a Secret clearance must be reinvestigated every ten years, and those holding a Confidential clearance must be reinvestigated every fifteen years.[194] In the intervening years, cleared individuals and their supervisors must report any derogatory information. Not only are these time periods simply too long, but the required self-reporting simply does not regularly take place. Aaron Alexis' conduct in the years after he received his Secret clearance should have raised serious questions about his ability to hold a clearance. Yet, neither Alexis nor his commanding officers reported any of this behavior. Given that he was not due for reinvestigation until 2017, there was little that adjudicators could do, absent such reporting.

---

[191] *Id.*

[192] Currently, reinvestigation of a top secret clearance occurs after five years, a secret clearance after ten years, and a confidential clearance after fifteen years.

[193] Miller Tr. at 205.

[194] Intelligence Reform & Terrorism Prevention Act of 2004, P.L. 108-458, 118 Stat. 3706.

In order to capture relevant conduct between periods of investigation, a system of continuous investigation needs to be implemented. This is not a new concept. In June 2005, the Department of Defense completed beta testing the Automated Continuous Evaluation System and expected to have initial operating capability within the year.[195] In a 2008 Executive Order, President George W. Bush stressed the importance of continuous evaluations.[196]

Testifying before the Subcommittee on Intelligence Community Management of the House Permanent Select Committee on Intelligence in 2010, then-FIS Associate Director Kathy Dillaman explained that OPM would soon launch a continuous evaluation investigation product.[197] Dillaman testified:

> [A] new investigation product in FY 2011 that provides for a validated suite of automated records checks that can be used as an annual assessment of individuals cleared at the Top Secret level . . . provides agencies with a quick and cost effective method for assessing employees and supports a more robust continuous evaluation program.[198]

In August 2013, the President commissioned a Review Group on Intelligence and Communications Technology to review "how in light of advancements in communications technologies, the United States can employ its technical collection capabilities in a manner that optimally protects our national security and advances our foreign policy while respecting our commitment to privacy and civil liberties, recognizing our need to maintain the public trust, and reducing the risk of unauthorized disclosure."[199] The Group, led by experts in the intelligence and legal fields, issued a 300-page report with 46 recommendations.[200] Recommendation 38 stated:

> We recommend that the vetting of personnel for access to classified information should be ongoing, rather than periodic. A standard of Personnel Continuous Monitoring should be adopted, incorporating data

---

[195] S. Comm. on Homeland Security & Gov't Affairs, Subcomm. On Oversight of Gov't Mgmt., the Fed. Workforce & the Dist. Of Columbia, *Hearing on Modernizing the Security Clearance Process*, 109th Cong. (June 28, 2005) (Statement of Heather Anderson, Dir., Strategic Integration, Office of the Deputy Under Sec'y of Defense, Counterintelligence & Security, & Acting Dir., Defense Security Service).

[196] Exec. Order No. 13467, 73 Fed. Reg. 38103 (June 27, 2008) ("An individual who has been determined to be eligible for or who currently has access to classified information shall be subject to continuous evaluation under standards (including, but not limited to, the frequency of such evaluation) as determined by the Director of National Intelligence.).

[197] H. Permanent Select Comm. on Intelligence, Subcomm. On Intelligence Community Mgmt, *Hearing on Personnel Security Clearance Reform*, 111th Cong. (Dec. 1, 2010) (Statement of Kathy Dillaman).

[198] *Id.*

[199] About the Review Group on Intelligence and Communications Technologies, *available at* http://www.dni.gov/index.php/intelligence-community/review-group (last visited Feb. 3, 2014).

[200] *Liberty and Security in a Changing World,* Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies (Dec. 12, 2013), *available at*http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

> from Insider Threat programs and from commercially available sources, to note such things in credit ratings or any arrests or court proceedings.[201]

In November 2013, the Chief Security Officer of the Department of Homeland Security, Gregory Marshall, testified before the House Committee on Homeland Security about the merits of a continuous evaluation system. He stated:

> 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 five-year increments, with a government-led process that examines a person's conduct within his or her normal re-investigation timeframes. 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.[202]

Current FIS Associate Director Merton Miller also believes a continuous evaluation program is the future of security clearance investigations. He testified:

> I mean, actually Alexis wasn't due for a reinvestigation until 2017. So somebody along the way, and I'm not pointing fingers because I'm sure it was a cost in a risk management decision to say, secret level, we investigate you every 10 years. Top secret, every 5 years. But the reality is, we need to know when there is an adjudicatively relevant event, when it happens. And part of this is this continuous evaluation. I know the DNI is very committed to it. We are very committed to it. We think that's the future of background investigations, where you don't ever close a case. This is my vision, okay, so attribute it to me only. But it's a living document. It never closes. We're going to constantly update that information with information that's relevant to your character and conduct.[203]

The concept of a continuous investigation or evaluation is not new. Despite efforts and promises by multiple government agencies over the past decade, a continuous evaluation system is still not in use. Given the proliferation of clearances since September 11, 2001, such a system is more

---

[201] *Id.* at 39.
[202] H. Comm. on Homeland Security, Subcomm. On Counterterrorism and Intelligence, *Hearing on The Insider Threat to Homeland Security: Examining Our Nation's Security Clearance Process*, 112th Cong. (Nov. 13, 2013) (Statement of Gregory Marshall).
[203] Miller Tr. at 161-62.

critical than ever. Without legislation to implement the idea, however, a system of continuous investigation seems destined to never become a reality.

The Committee is considering legislation to address the problem of the lengthy timeframe between reinvestigations, including adding legislative muscle to finally push through completion of continuous investigations for security clearance investigations. Potential legislation could require the Director of OPM to set up a process, within a strict timeline after the legislation's passage, to obtain relevant information about cleared employees. Information should be updated continuously to provide real-time notifications of relevant information with respect to the suitability of a covered employee to maintain a security clearance. The continuously updated information should include information relating to criminal or civil legal proceedings to which the individual with a clearance is a party. Information on financial difficulties the individual might encounter after receiving the initial clearance should also be under continuous evaluation.

Legislation may also require OPM to "push" any such notifications from a continuous investigation to the agency that granted the individual's clearance. The adjudicating agency would then make a determination as to whether or not the individual may still maintain a clearance or request a reinvestigation of the individual.

One of the main challenges in creating this system is how to pull records from other state and local databases around the country to update the OPM database in near-real time. As Miller explains, this objective is already becoming a priority for OPM. Miller testified:

> I mean, the issue, and I'm getting off topic here, but the issue is the record repositories. And engaging in the PAC [Performance Accountability Council], we had a record repository working group that was supposed to look at consistent data standards, data exchange standards, and that wasn't, unfortunately, it wasn't the priority at the time. But I think it should be now, getting those records, getting access to those records.[204]

Miller also testified that the "DNI is very committed to [continuous evaluation]."[205] As such, the legislation requires OPM to consult with the DNI as well as OPM's top two customers—the Department of Defense and Department of Homeland Security—when creating the database.

B. Use of the Internet and Social Media for Background Investigations

OPM last updated its Investigator's Handbook on July 23, 2007. Since that time, the use of social media has risen dramatically. In 2007, Twitter had 50,000 active weekly users.[206] Today, the company has over 230 million active monthly users.[207] In April 2007, Facebook had

[204] Miller Tr. at 165.
[205] *Id.*
[206] Michael Arrington, "End of Speculation: The Real Twitter Usage Numbers," (Apr. 29, 2008), *available at:* http://techcrunch.com/2008/04/29/end-of-speculation-the-real-twitter-usage-numbers/.
[207] About Twitter, Inc., *available at:* https://about.twitter.com/company (last visited Jan. 30, 2014).

only 20 million active users.[208] Today, the company has 1.23 billion active monthly users.[209] In 2007, Google conducted an average of 1.2 billion searches per day.[210] Today, that number has grown to 5.92 billion.[211] These three social media and search sites, among others, contain a treasure trove of information about their users. And the Americans that hold, or will apply for, federal security clearances use them frequently.

Unfortunately, investigators conducting federal security clearance background checks do not see, search, or receive reports of the vast amount of information available online. Nor do current federal security process guidelines allow the adjudicators who grant the clearances to access this information.

When it comes to social media and modern technology, the Investigator's Handbook is antiquated. The current Handbook guidelines strictly prohibit the use of the internet to obtain information about an investigative Subject. The Handbook does not address the use of social media, but instead includes a near-blanket restriction on the use of the Internet. Page 22 of the Handbook states:

> **The general use of the internet to obtain investigative information is strictly prohibited.** Do not use the Subject's identifiers (e.g., SSN) on internet sites to obtain investigative results unless you have received specific authorization. Such authorization to utilize particular sites will be disseminated to investigators when the use of those sites has been vetted through the FIPC Records Access and R/D Group. Authorization is granted only for use on an approved system. Inquiries regarding the approval of internet sites for information gathering should be directed through your local supervisor for referral to the Records access and R/D Group at FIPC.[212]

In fact, federal background investigators may only use the Internet, for example, to look up the addresses of businesses. The manual states:

> Use of the internet is permissible for lead purposes. 'Lead purposes' are those activities which may assist an investigator in conducting investigations more efficiently; however they do not achieve an investigative result. For example, an investigator might visit a contractor webpage to locate the address of the facility or the homepage of a government office to locate points of contact.[213]

This restrictive policy keeps nearly every piece of information on a Subject's social networking site outside the reach of security clearance investigators. Given that tens of millions of

---

[208] "Number of active users at Facebook over the years," ASSOC. PRESS (Oct. 23, 2012), *available at:* http://finance.yahoo.com/news/number-active-users-facebook-over-years-214600186--finance.html.
[209] Facebook Newsroom, *available at*: http://newsroom.fb.com/Key-Facts (last visited Jan. 30, 2014).
[210] Google Annual Search Statistics, *available at:* http://www.statisticbrain.com/google-searches/.
[211] *Id.*
[212] OPM Investigator's Handbook (July 2007) at 1-21. (emphasis added)
[213] *Id.*

Americans visit social media sites daily, an updated policy that appropriately considers privacy concerns would allow federal investigators to pull information about Subjects from of these and other websites.

According to Merton Miller, Associate Director for the Federal Investigative Services, discussions about obtaining information on Subjects from these sites are underway. He testified:

> Q. Can [investigators] currently use the Internet to obtain any other information or material –
>
> A. There is not a policy in place, although **there has certainly been a great deal of dialogue with the Security Executive Agent, the ODNI, about establishing a policy for the use of social media for a background investigation.**[214]

Miller agrees that investigators can find valuable information pertaining to a Subject's background on these sites, and federal investigators should be able to mine them to verify facts or acquire new information. He stated:

> Yes. **I think most people would say it's a no-brainer**, that with all the information available about individuals on the Internet today, with Facebook, Myspace, LinkedIn, you know, you name it, that you could very easily go out and verify potential information about an individual's background. In fact, postings of people drinking when they were under age might be on the Internet.[215]

Allowing federal investigators to use these social media sites, however, does present potential challenges. Miller explained:

> So I think right now the real keys have been is everybody sees it as a potential lead development tool, but not a tool to be used for investigative purposes because of the potential privacy issues, number one. And then, from my perspective, it's the analytics that would be required behind the information you collect. For example, having worked counterintelligence operations, it's one thing collecting information. It's a whole other process, more costly, to verify the veracity of that information and then connect the dots. So I could, as you could, you could go out and build an Internet persona for me tonight. You could go home and say, Miller, you know, put that out there, and all I would have to do is do a search and I would see what you wrote.
>
> Now, so what is the veracity of that information? You wrote it. You posted it. Somebody is going to have to determine the reliability of that. So that's the hard part, I think, in applying the social media role in

[214] Miller Tr. at 158. (emphasis added).
[215] *Id.*

background investigations. **It's not collecting it, it's not finding it, it's then doing the analysis, because when you run an investigation you shouldn't be incorporating information that isn't true about the subject in that investigation.**[216]

The Committee is considering legislation to require OPM to allow its background investigators to use social media sites and other Internet resources to develop information on Subjects under investigation for a possible clearance. Such legislation would give OPM flexibility to determine how to access these sites, and how to verify information from the sites effectively. One possibility would be to have the investigator search for publicly available information on a Subject, and then confirm the veracity with the Subject and his or her friends and family. Another possibility would ask a Subject to disclose the social media and other Internet sites he or she visits on a regular basis on the SF-86. According to Merton Miller, discussions about requesting social media information from applicants have not taken place at OPM:

> Q. A couple questions on that. Because a lot of this is on self-reporting, why not have questions in the SF-86 as to please list links to your social media sites?
>
> A. You could potentially do that.
>
> Q. Is there dialogue about that?
>
> A. I have not heard any dialogue about adding individual social media sites to the SF-86.[217]

Regardless, by allowing the use of information from these sites as part of a Subject's background investigation, federal investigators, and ultimately the adjudicators, will be able to develop a more complete picture of the Subjects under consideration for a security clearance than currently exists today.

C. Communication between Adjudicators and Investigators

Currently, agency adjudicators do not speak with the OPM or contract investigators who investigated a security clearance application. When adjudicators receive an applicant's file to make a determination on a security clearance, the content within the file is the full universe of information the adjudicators can consider. Adjudicators cannot simply contact investigators to ask follow-up questions about the file. The ability to do so would be extremely helpful to adjudicators in certain instances. In the case of Aaron Alexis, the adjudicators could have asked the interviewer about Alexis' demeanor when discussing his 2004 arrest or his multiple credit issues. The adjudicators could have asked a different investigator about their efforts to track down the police report pertaining to Alexis' arrest. Instead, these questions were left

---

[216] *Id.* at 159.
[217] *Id.* at 159.

unanswered, and the adjudicators were left to evaluate Alexis solely based on the investigative file, which presented an incomplete picture of Aaron Alexis.

Merton Miller agreed that allowing adjudicators to contact investigators with follow-up questions would be beneficial. He testified:

> Q. Do you think it would be useful to allow adjudicators to directly speak with investigators if they so desired, so if the adjudicator received a file and had questions about the work performed, are there benefits or detriments to allowing those?
>
> A. I think there would -- I think there would be some benefits for an adjudicator being able to talk directly to the investigator, you know, about -- about that interview, you know, what was captured. I think there would be some benefits to that. Now, thinking how many adjudicators there are versus the number of investigators, that might be a challenge actually to be able to do that, but even after the fact, being able to reach out and talk [to] an agent who was involved in the investigation, I think, would -- could be beneficial to the adjudicator.[218]

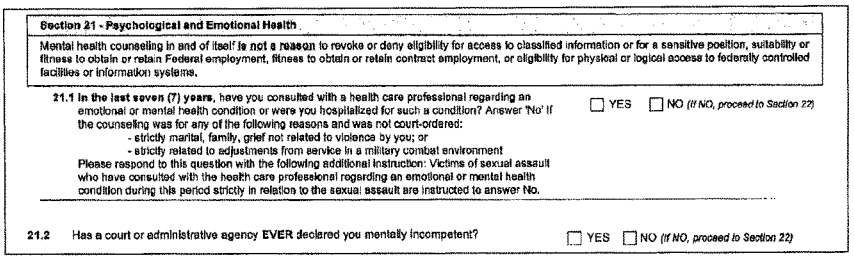
The Department of Defense agrees. Department representatives told the Committee that there would be "tremendous benefit" to allowing adjudicators and investigators to speak about an investigation.[219] Both adjudicators interviewed by Committee staff also expressed a desire to be able to ask questions of investigators directly.

The Committee is considering legislation to address this issue by allowing adjudicators and investigators to speak with one another to assist the adjudicators in making their clearance determinations. Such legislation would afford the Department of Defense and other client agencies the ability to coordinate with OPM individually in order to determine the most effective way for these discussions to occur, and to set information-sharing guidelines between the two parties. This first step is long overdue.

D. Mental Health Evaluation

Each applicant for a security clearance is required to answer a basic question about their mental health. Section 21 of the SF-86 states:

[218] Miller Tr. at 161.
[219] Nov. 21 DOD Briefing.



Section 21 - Psychological and Emotional Health

Mental health counseling in and of itself **is not a reason** to revoke or deny eligibility for access to classified information or for a sensitive position, suitability or fitness to obtain or retain Federal employment, fitness to obtain or retain contract employment, or eligibility for physical or logical access to federally controlled facilities or information systems.

21.1 In the last seven (7) years, have you consulted with a health care professional regarding an emotional or mental health condition or were you hospitalized for such a condition? Answer 'No' if the counseling was for any of the following reasons and was not court-ordered:
- strictly marital, family, grief not related to violence by you; or
- strictly related to adjustments from service in a military combat environment

Please respond to this question with the following additional instruction: Victims of sexual assault who have consulted with the health care professional regarding an emotional or mental health condition during this period strictly in relation to the sexual assault are instructed to answer No.

☐ YES ☐ NO *(If NO, proceed to Section 22)*

21.2 Has a court or administrative agency **EVER** declared you mentally incompetent?

☐ YES ☐ NO *(If NO, proceed to Section 22)*

If an applicant answers "Yes" on Section 21 of the SF-86, the applicant is then required to sign a Health Insurance Portability and Accountability Act (HIPAA) release form. If an applicant answers "No" to Section 21 of the SF-86, no HIPAA release form is required.

A problem arises when the applicant has in fact been treated for mental health issues, yet answers "No" on the form. Currently, investigators are unable to cross-check whether or not the applicant has been treated for such issues, unless the applicant mentions so during the personal interview—which is only required for a Top Secret level clearance, or if information arises during an investigation for a Secret level clearance to trigger such an interview.

The Committee is considering legislation that would assist investigators in better capturing mental health information.

E. Cooperation From State and Local Law Enforcement Agencies

As discussed earlier, federal law requires local law enforcement agencies to provide criminal history information to federal security clearance investigators. Unfortunately, many local law enforcement agencies frequently shun federal security clearance investigators, either refusing to provide this criminal history information, or providing only limited information. Without any enforcement mechanism against local law enforcement agencies that refuse to comply, federal security clearance investigators are unable to obtain pivotal information pertaining to their cases. Often—as was the case with Aaron Alexis—this information is critical for an adjudicator responsible for deciding whether to grant a security clearance.

Background investigators did not obtain the police report for Alexis' 2004 arrest for malicious mischief during the course of his Secret level clearance investigation. As such, Alexis' file did not include important information contained in the arrest report, and DOD adjudicators never learned the details of that arrest. When Committee staff interviewed the adjudicator who performed the second-level review of Alexis' file, the adjudicator stated that the malicious mischief arrest—a very broad offense—could have been for "hitting a mailbox with a can."[220] The adjudicator never learned that Alexis used a gun or that his family believed he might have had post-traumatic stress disorder, two seemingly important pieces of information to

[220] Telephone Interview of [Former U.S. Navy Adjudicator] by the H. Comm. on Oversight & Gov't Reform Majority and Minority Staff (Dec. 6, 2013).

help decide whether to grant Alexis a clearance. Additionally, the federal background investigators working on Alexis' case did not learn of this information, and were therefore unable to confront Alexis about it during his interview.

Instead of cooperating with OPM investigators, many local law enforcement offices simply refer the investigators to the local courts to obtain records. This was the typical procedure in Seattle at the time of Aaron Alexis' 2007 security clearance investigation. Miller stated:

> And so, I mean, just, you know, cutting to the Seattle situation, you know, with Alexis, **Seattle advised back in 2007 for the staff to go to the courts** to obtain the criminal history record information that would be available on Alexis. So the process at that time was to go into the court records in an automated way and obtain, basically download the record of what's in the system. You know, malicious mischief was the charge. The disposition was dismissed. And that's what was put into the file.[221]

The difference between a record from a court and a record of the police report from the law enforcement office is enormous. Even statewide databases that OPM has approved for investigator use, such as the Washington Statewide Database, provide only cursory information about a criminal incident, such as the date of offense, charge, and disposition.

As discussed earlier, the police report from Aaron Alexis' 2004 arrest contained highly relevant details about Alexis' conduct—including his use of a gun. Yet, the file OPM sent to the Navy adjudicator regarding this arrest, obtained from the Washington Statewide Database, contained simply the words "malicious mischief." Unquestionably, the police report contains more detailed and relevant information about the 2004 Alexis incident. An adjudicator needs the type of information in the police report. Yet, too often, that information is never passed along.

Shortly after Aaron Alexis went on his murderous rampage, Navy Secretary Ray Mabus recommended that "all Office of Personnel Management investigative reports involving security clearances include any available police documentation."[222] Merton Miller agreed that, at least in theory, this would be helpful for adjudicators. Miller testified:

> Personally, I think there would be great benefit of having the most detail possible regarding the circumstances of the arrest to address character and conduct issues on the individual.

Miller noted, however, that doing so could prove costly. He stated:

> And so, personally, there may be significant cost challenges associated with actually obtaining the level of record, not necessarily just for the government, but for the local jurisdictions as well to provide resources

[221] Miller Tr. at 102.
[222] Kris Osborn, "Mabus Wants Changes to Clearances After Shooting," Military.com (Sept. 23, 2013), *available at:* http://www.military.com/daily-news/2013/09/23/mabus-wants-changes-to-clearances-after-shooting.html.

> who can actually respond to and, oh, by the way, do it in a timely manner.[223]

Responding directly to Secretary Mabus' suggestion that OPM include any available police documentation in its investigative reports, Miller again mentioned the cost and challenges to local law enforcement offices. Miller testified:

> I understand why he made that recommendation. I guess the real question is, the Secretary does not know the challenges associated with obtaining those records from the jurisdictions and how it varies. Plus, I'm not sure the Secretary would understand what the cost implications of that recommendation would be. . . . There were -- there are significant efficiencies there that could potentially be lost if we were to ask to have every piece part, but I understand why he would say that.[224]

When local law enforcement agencies do not cooperate with OPM investigators in any way, they risk running afoul of federal law. Agencies that provide only cursory information to OPM investigators rather than complete copies of arrest records or detailed information about the causes of an arrest or other criminal activity are circumventing the spirit of the law. When OPM investigators are not able to determine crucial details of a Subject's criminal history, the results, as in the case of Aaron Alexis, could prove deadly. OPM maintains a list of the local law enforcement agencies that do not fully cooperate with OPM or its retained investigators when they request records on investigation Subjects. Unfortunately, some of the country's largest local law enforcement agencies, such as the Los Angeles Police Department, are on that list.[225]

The New York City Police Department is also on that list, with a note that says "Does not cooperate in any way, shape, or form."[226] The Newark Police Department is on the list, with a note that says "Will not fulfill any requests other than for law enforcement agencies"[227]—despite the requirement in 5 U.S.C. § 9101 to cooperate with OPM. Baltimore, Maryland and Washington, D.C.—two cities compromising the metropolitan region where the largest number of individuals holding clearances reside in the country—are also on the list. The Baltimore police department does "not release any records without an individual's fingerprints."[228] The Metropolitan Police Department in Washington, D.C. simply "does not cooperate" and suggests that an investigator "[g]o to the courthouse."[229]

In all, OPM lists over 450 uncooperative local law enforcement offices. These offices hold millions of arrest records and police reports. Withholding these records is illegal, and it seriously hinders the background investigation process.

---

[223] Miller Tr. at 103-4.
[224] *Id.* at 114.
[225] "Uncooperative Law Agencies Master List, FIS" (Jan. 23, 2014) [OPM014538].
[226] *Id.* [OPM014545].
[227] *Id.*
[228] *Id.* [OPM014543].
[229] *Id.* [OPM014539].

OPM appears to have tacitly endorsed the uncooperative practices of local law enforcement agencies. Not only has OPM agreed to allow investigators to use databases that do not include all information OPM requests from local law enforcement agencies[230] in a pamphlet explaining how to cooperate with security clearance investigations, but it appears to encourage investigators not to spend too much time obtaining arrest and other criminal records.[231]

The Committee is considering legislation to address the problem of non-cooperation by local law enforcement offices. Such legislation could both clarify what information local law enforcement agencies must provide to security clearance investigators, and also tie certain grants from the federal government to cooperation with OPM.

V. Allegations of Fabrication and Fraud

It is clear from the Committee's investigation that OPM takes quality issues very seriously. As discussed previously in Section III.B, OPM and its contractors employ various policies to ensure quality and find potential instances of fabrication at an individual level. This is evidenced by the 21 investigators—11 federal and 10 contractor—who have been convicted for fabrication.

In the course of this investigation, the Committee learned of issues of fabrication and fraud not raised by the Aaron Alexis background investigation. For the last several years, OPM and the Department of Justice have been investigating allegations of fraud committed by USIS. The Department has joined a False Claims Act lawsuit against USIS seeking over $1 billion in damages. The current management of the company was brought on after the allegations were made, and has told the Committee they are fully cooperating with the investigation.

On July 1, 2011, a former USIS employee filed a *qui tam* lawsuit in federal court alleging that the company defrauded the federal government. Before he left the company, the whistleblower was Director of Fieldwork Services. In this position, he managed USIS employees responsible for performing quality reviews on investigative reports USIS performed for the federal government. USIS was obligated to conduct these quality reviews under its contract with the government.

USIS managers informed him that the company had been employing a practice known within the company as "dumping." The whistleblower described dumping as such:

[230] *See Law Enforcement & The U.S. Office of Personnel Management*, Federal Investigative Services (June 2013) ("The Investigator will request pertinent information about each offense, including the data/place of the offense, statement of the actual charge, circumstances of the offense, and its disposition. In addition, the Investigator may ask for a copy of the police report.).

[231] Office of Personnel Mgmt, *Case Management or, How to Complete a 30-day Caseload in 30 Days or Less*, (Sept. 2005) at 17 ("LAW CHECK/OTHER RECORDS: they've either got 'em, or they don't. If they decline to look for records and you've tried normal appeals, explain situation to supervisor and follow their guidance.") [OPM006216].

> Dumping is the releasing of Cases to OPM that were represented as Field Finished that were not reviewed by a [Quality] Reviewer and/or had not been investigated at all.[232]

The whistleblower stated that he was directed to dump in order to "collect full compensation on the contract for February 2011."[233] The whistleblower, however, refused to dump cases, "causing USIS to miss receiving its maximum profits."[234] He allegedly was fired from USIS in June 2011 "as a result of his refusing to dump cases to OPM that were not field finished."[235]

On January, 21, 2014, the Department of Justice filed a civil complaint against USIS for violating the False Claims Act, alleging that USIS management "dumped" incomplete background investigation reports to OPM without performing the quality review required by its contract with OPM.

According to the Department, "[i]nternal USIS documents confirm that USIS Senior Management was aware of and directed the dumping practices," including directives to "clear out our shelves in order to hit revenue."[236] This alleged fraud was enormous and persistent. According to the Department, USIS "dumped" approximately 665,000 background investigations, comprising about 40% of the total number of investigations conducted by the company during this four-year period.[237]

Although allegations of dumping were not within the scope of the Committee's investigation, the Committee will continue to monitor the Department's investigation as it proceeds.

VI. Conclusion

The Committee's investigation over the past several months, started in the wake of the Navy Yard shooting, demonstrates that reforms and updates are necessary to ensure that security clearances are granted only to qualified individuals who have the ability to safeguard our nation's secrets. The legislative fixes contained in the accompanying legislation must be supplemented by common sense practices and reforms at the Office of Personnel Management. The Committee looks forward to the continuing cooperation from all the stakeholders—OPM, the Department of Defense, other client agencies, and the three contractors—as it works towards strengthening this clearance process and improving the safety of confidential information and facilities.

---

[232] Qui Tam Complaint , ¶ 29 (July 1, 2011), *U.S. ex rel., [Whistleblower] v. U.S. Investigations Services, LLC.*, M.D. Ala. (No. 2:11-CV-527-WKW).
[233] *Id.* at ¶ 39.
[234] *Id.* at ¶ 44.
[235] *Id.* at ¶ 47.
[236] United States' Complaint, ¶ 53 (Jan. 22, 2014), *U.S. ex rel. [Whistleblower] v. U.S. Investigations Services, LLC*, M.D. Ala. (No. 11-CV-527-WKW).
[237] *Id.* at ¶ 57.

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
REP. ELIJAH E. CUMMINGS, RANKING MEMBER

CONTRACTING OUT SECURITY CLEARANCE INVESTIGATIONS: THE ROLE OF USIS AND ALLEGATIONS OF SYSTEMIC FRAUD

DEMOCRATIC STAFF REPORT
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES
113TH CONGRESS
FEBRUARY 11, 2014

TABLE OF CONTENTS

INTRODUCTION

On September 16, 2013, Aaron Alexis killed twelve people and injured several others at the Washington Navy Yard. Alexis entered the facility with a shotgun using his credentials as an employee of a federal subcontractor that performed computer software updates for the Navy. Alexis qualified for this position because he had received a Secret level security clearance in 2008 when he served in the Navy Reserve.

Last fall, the Committee initiated a bipartisan investigation to examine the circumstances by which Alexis received and retained his security clearance, particularly given subsequent revelations about his multiple arrests involving firearms.

This week, the Republican staff of the Committee issued a report focusing primarily on the role of the Office of Personnel Management (OPM) in overseeing its contractors that conduct background investigations.

This Republican staff report was incomplete because it did not present the full findings of the Committee's investigation into the role of U.S. Investigations Services, Inc. (USIS)—the company that conducted Alexis' background investigation and that conducts more background investigations than any other federal contractor.

For these reasons, the Committee's Ranking Member, Rep. Elijah E. Cummings, asked Democratic staff to set forth additional information regarding USIS, including new allegations of a massive fraud committed by the company's top executives over 4½ years that may have endangered national security.

In the wake of these devastating allegations, USIS experienced an exodus of senior officials. Twenty-four executives have resigned, retired, or been terminated, including the company's Chief Executive Officer and Chief Financial Officer. In addition, Committee staff learned that the President of its Investigations Services Division also resigned suddenly just last week.

The Committee's investigation, which has included a review of tens of thousands of pages of documents and interviews with multiple government officials, raises serious concerns about the massive scale of this alleged fraud and the sophisticated means by which it evaded detection for so long.

Despite these revelations, however, the Committee has not conducted any transcribed interviews of USIS officials to date. Although the record before the Committee answers many questions about how Alexis obtained a security clearance, the Committee must do much more to answer and address the much broader and systemic concerns involving USIS.

I. CONTRACTING OUT AND THE RISE OF USIS

Throughout the 1990s and early 2000s, background investigations for security clearances were overseen by the Department of Defense (DOD), and its stewardship was criticized for excessive delays and large backlogs.

In 1999, the former General Accounting Office (GAO) reviewed a sample of 530 investigations conducted by DOD and found that the vast majority did not comply with federal investigative standards. GAO also reported that half of the 530 investigations it reviewed took 204 or more days to complete, missing the 90-day deadline requested by its customers. In addition, less than one percent of the 530 investigations met the 90-day timeframe. GAO also found a backlog of 600,000 cases pending reinvestigation.[1] Hundreds of thousands of applicants, federal employees, and contractors were waiting an average of 200 days for background investigations to be completed. As a result of these backlogs and delays, GAO placed DOD's security clearance process on its high risk list.[2]

In 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act, which set tighter deadlines for completing background investigations.[3] In addition, President George W. Bush's fiscal year 2004 budget proposal transferred DOD's investigation services to OPM.[4]

Today, OPM's Federal Investigative Services oversees 90% of security clearance background investigations and performs more than 2 million background investigations annually. OPM conducts investigations through more than 2,500 federal investigators and 6,700 contractor investigators. OPM contracts primarily with three firms: USIS, CACI Premier Technology, and KeyPoint Government Solutions.[5]

USIS started as an Employee Stock Ownership Plan in 1996 when the federal Office of Investigations, a division of OPM, was outsourced during a wave of privatizations of federal

---

[1] General Accounting Office, *DOD Personnel Clearances: Preliminary Observations Related to Backlogs and Delays in Determining Security Clearance Eligibility for Industry Personnel* (May 6, 2004) (GAO-04-202T); General Accounting Office, *DOD Personnel: Inadequate Personnel Security Investigations Pose National Security Risks* (Oct. 1999) (GAO/NSIAD-00-12).

[2] *Backlogs in Security Clearance Program Reduced After GAO Raises Concerns,* Washington Post (Feb. 21, 2011); *Expect Security Clearance Delays: NSA Leak Could Mean Less Info-Sharing, More Polygraphs*, Federal Times (June 24, 2013).

[3] Pub. L. No. 108-458 (2004).

[4] *Defense Background Check Authority May Transfer to OPM*, Government Executive (Feb. 5, 2003).

[5] Government Accountability Office, *Decision in the Matter of OMNIPLEX World Services Corporation* (Mar. 14, 2012) (online at www.gao.gov/assets/590/589781.pdf).

government services.[6] At the time, the Office of Investigations' largest customers for background investigations were the U.S. Postal Service, Energy Department, and Immigration and Naturalization Service.[7]

The employee-owned U.S. Investigations Services soon became the focus of private equity investors. In 1999, the Carlyle Group invested $50 million, and it later invested an additional $25 million for a 25% total stake.[8] In 2003, the private equity firm Welsh, Carson, Anderson & Stowe invested $545 million and became the company's majority owner.[9] U.S. Investigations Services explained its buy-out by the private equity firm as important to "continue to grow our capabilities in order to address the increased demand for our services from various homeland security initiatives."[10]

In 2005, U.S. Investigations Services paid a $185 million dividend to its owners.[11]

In 2006, the company was rebranded as USIS to reflect "the much wider scope of security-related screening and background solutions provided by the company to government and commercial clients."[12]

In 2007, the private equity firm Providence Equity Partners, Inc. purchased USIS for $1.5 billion from Welsh, Carson, Anderson & Stowe and the Carlyle Group.[13] At the time, Randy Dobbs, then-CEO of USIS, stated:

> This acquisition represents an opportunity for USIS to grow our current businesses and look for potential opportunities that broaden our services in other areas of the overall screening and security markets.[14]

In 2011, OPM awarded USIS a five-year contract for fieldwork investigations worth $2.46 billion.[15] The same year, it also awarded USIS a five-year support services contract worth

---

[6] *OPM, in a First, Acts to Convert an Operation Into Private Firm*, Washington Post (Apr. 14, 1996).

[7] *Id.*

[8] *Welsh to Score in Dividend*, Daily Deal (Sept. 26, 2005).

[9] *US Investigations Services, Inc. Announces Completion of Recapitalization*, Business Wire (Jan. 10, 2003) (LexisNexis 2014).

[10] *Id.*

[11] *Welsh to Score in Dividend*, Daily Deal (Sept. 26, 2005).

[12] USIS, *Fact Sheet* (online at usis.com/Fact-Sheet.aspx) (accessed Feb. 8, 2014).

[13] *Providence Buying USIS for $1.5B*, Daily Deal (May 14, 2007).

[14] *Id.*

[15] Office of Personnel Management, *Fieldwork Contract with U.S. Investigations Services* (Dec. 1, 2011) (Contract No. OPM 15-11-C-0015).

up to $288 million.[16] According to its website, USIS today holds 100 federal contracts.[17] Seventy percent of background investigations are performed by contractors, and USIS performs almost half of the investigations assigned to federal contractors.[18] As a private company, USIS does not publicly report its revenues.

II. ALLEGATIONS OF SYSTEMIC FRAUD BY USIS

USIS has been accused by one of its own long-time employees of a massive, multi-year contracting fraud scheme. In addition, the Department of Justice has joined a False Claims Act lawsuit against the company seeking over a $1 billion on behalf of the American taxpayers. Twenty-four of the company's officials, including the former Chief Executive Officer and Chief Financial Officer, have now resigned, retired, or been terminated, and the OPM Inspector General has warned that "USIS's fraud may have caused serious damage to national security."[19]

A. USIS Employee Allegations of Illegal "Dumping"

On October 30, 2013, a federal court lifted the seal on a *qui tam* lawsuit filed by Blake Percival, a former USIS employee, alleging a multi-year effort by the company to defraud U.S. taxpayers. Mr. Percival had spent a decade at USIS, rising to become the Director of Fieldwork Services, where he oversaw the work of 350 employees. In this position, Mr. Percival met with subordinates who directly managed USIS employees responsible for performing quality reviews on investigative reports performed for the federal government.

USIS held indefinite-delivery, indefinite-quantity contracts with OPM that required the company to perform two major functions: (1) conduct fieldwork for background investigations; and (2) conduct a quality review of each case before submitting it to OPM.[20] When USIS sent a completed case to OPM, it received 90% of its contract payment for that type of case. The remaining 10% was paid when the case was formally closed. The more cases USIS submitted to OPM, the more revenues it generated.

---

[16] Office of Personnel Management, *Support Services Contract with U.S. Investigations Services* (June 30, 2011) (Contract No. OPM 15-11-C-0004).

[17] USIS, *Fact Sheet* (online at usis.com/Fact-Sheet.aspx) (accessed Feb. 8, 2014).

[18] Congressional Research Services, *Security Clearance Process: Answers to Frequently Asked Questions* (Sept. 9, 2013) (R43216).

[19] House Committee on Oversight and Government Reform, Testimony of Patrick McFarland, Inspector General, Office of Personnel Management, *Hearing on D.C. Navy Yard Shooting: Fixing the Security Clearance Process* (Feb. 11, 2014).

[20] Office of Personnel Management, *Fieldwork Contract with U.S. Investigations Services* (July 7, 2006) (Contract No. OPM 04-06-00013); Office of Personnel Management, *Fieldwork Contract with U.S. Investigations Services* (Dec. 1, 2011) (Contract No. OPM 15-11-C-0015).

According to Mr. Percival, USIS managers informed him that the company had been "dumping" cases on OPM for which it had conducted fieldwork, but not the required quality reviews. His complaint explained:

> Dumping is the releasing of Cases to OPM that were represented as Field Finished that were not reviewed by a [Quality] Reviewer and/or had not been investigated at all.[21]

According to Mr. Percival, although USIS failed to conduct quality reviews required by its contracts, the company sought and obtained payment nonetheless. He stated that he was directed to continue the practice of dumping by Robert Calamia, the Vice President of Field Operations, in order to "collect full compensation on the contract for February 2011."[22]

Mr. Percival asserted that he refused to dump cases, "causing USIS to miss receiving its maximum profits."[23] Mr. Percival was fired from USIS in June 2011 "as a result of his refusing to dump Cases to OPM that were not field finished."[24]

B. Justice Department False Claims Act Case

On January, 21, 2014, the Justice Department filed a civil complaint against USIS for violating the False Claims Act and alleged that top USIS management devised a scheme of "dumping" incomplete background investigation reports to OPM without performing quality reviews required by its contracts. The Department filed its complaint after determining that Mr. Percival's case against USIS had merit and should proceed with the intervention and support of the federal government. According to the Justice Department's investigation:

> Beginning in at least March 2008 and continuing through at least September 2012, USIS management devised and executed a scheme to deliberately circumvent contractually required quality reviews of completed background investigations in order to increase the company's revenues and profits.[25]

According to the Department, high-level USIS executives, including the former President and CEO, devised this scheme to meet internal revenue goals:

> USIS Senior Management was fully aware of and, in fact, directed the dumping practices. Beginning in at least March 2008, USIS's President/CEO established the internal revenue

---

[21] Qui Tam Complaint, ¶ 29 (July 1, 2011), *United States of America, ex rel., Blake Percival v. U.S. Investigative Services, LLC.*, M.D. Ala. (No. 2:11-CV-527-WKW).

[22] *Id.* at ¶ 39.

[23] *Id.* at ¶ 44.

[24] *Id.* at ¶ 47.

[25] United States' Complaint, ¶ 42 (Jan. 22, 2014), *United States of America ex rel. Blake Percival v. U.S. Investigations Services, Inc.*, M. D. Ala. (No. 11-CV-527-WKW).

> goals for USIS. USIS's Chief Financial Officer determined how many cases needed to be reviewed or dumped to meet those goals.[26]

The Department explained how senior USIS executives communicated these decisions to lower-level USIS employees:

> The number of cases needed to be reviewed or dumped to meet revenue goals was conveyed to USIS's Vice President of Field Operations and USIS's President of Investigative Service Division, who in turn communicated this information to other members of USIS management, including USIS's Production Support Senior Manager. The Production Support Senior Manager and others, in turn, would convey those goals to other USIS employees, namely USIS's Director of National Quality Assurance and the Quality Control Manager in Western Pennsylvania, and would provide instructions to those employees on when and how many cases needed to be reviewed or dumped to meet USIS's goals.[27]

According to the Department, "Internal USIS documents confirm that USIS Senior Management was aware of and directed the dumping practices," including directives to "clear out our shelves in order to hit revenue."[28] This alleged fraud was enormous and persistent. According to the Department, USIS "dumped" at least 665,000 background investigations, comprising about 40% of the total number of investigations conducted by the company during this 4½ year period.[29]

C. Committee Investigation

The Committee's investigation identified a number of facets of the alleged fraud not previously reported. Documents obtained by the Committee indicate that USIS withheld information about its fraudulent activities when confronted by OPM and instead claimed that OPM was to blame for the problem. In addition, witnesses interviewed by Committee investigators revealed how USIS allegedly misused a secondary contract it held to obtain information about OPM's oversight efforts and evade detection of its alleged fraudulent activities for more than four years. The Committee's investigation also identified bonuses received by USIS executives, noting a sharp increase when the alleged fraud began. The Committee's investigation raised numerous questions that have yet to be answered, including the extent to which officials at USISs' parent company, Altegrity, knew about the alleged fraud.

1. Withholding of Information from OPM

On April 4, 2011, after conducting an internal analysis, OPM sent a Problem Notification Letter to Robert Calamia, Vice President of Field Operations at USIS, expressing concern after

---

[26] *Id.* at ¶ 51.

[27] *Id.* at ¶ 52.

[28] *Id.* at ¶ 53.

[29] *Id.* at ¶ 57.

discovering that only four USIS employees had released thousands of reports to OPM, apparently without ever conducting the required quality reviews. The letter stated:

> The analysis also revealed that 4 USIS SIDS were responsible for the release of 13,113 ROI's [Reports on Investigation] over the course of the same 1 week timeframe representing an average of 3,278 ROI's per person.[30]

In light of these concerns, OPM requested that:

> USIS provide a response to this concern insuring that all ROI's are being reviewed by qualified reviewers and clarification of any automated systems or mechanism being use [sic] to complete or assist in the processing of ROI's including details of how the process is being utilized.[31]

On April 19, 2011, Mr. Calamia sent a response letter suggesting that cases were being "erroneously submitted" not because of any fraudulent activities by USIS, but rather due to a "gap" with OPM systems. He proposed that OPM provide USIS with greater control over when cases could be submitted—which would also trigger OPM payments to USIS—and he described his proposal as "the best opportunity to create contractor ownership."[32]

At no point did Mr. Calamia acknowledge that the reason OPM had found anomalously high numbers of reports released by very few quality reviewers was that USIS was dumping cases to maximize revenues.

2. Misuse of Secondary Contract to Conceal Fraudulent Activity

Under a secondary contract, USIS performed administrative functions to support the processing of cases submitted by contractors and prepare them for release to customer agencies. On January 8, 2014, Committee staff conducted a transcribed interview with Merton Miller, the Associate Director of Federal Investigative Services at OPM. Mr. Miller suggested to Committee investigators that USIS used information obtained through this support services contract to avoid detection of the company's fraudulent dumping. Mr. Miller told Committee investigators:

> [T]hey circumvented OPM's oversight of their performance of their quality review. I'm not splitting hairs, but they knew how we were auditing. They knew what kind of reports we generated to oversee that they were actually performing the activities they were

---

[30] Letter from [redacted], Branch Chief, Field Investigations Oversight Branch, Office of Personnel Management, to Robert Calamia, Vice President of Field Operations, USIS (Apr. 4, 2011).

[31] *Id.*

[32] Letter from Robert Calamia, Vice President of Field Operations, USIS, to [redacted], Branch Chief, Field Investigations Oversight Branch, Office of Personnel Management (Apr. 19, 2011).

> within PIPS. ... so they circumvented our oversight process, and they falsified records to help do that.[33]

When Mr. Miller was asked if USIS was able to use the support services to help dump cases without OPM detection, he replied:

> I don't know for a fact. However, there was certainly the opportunity for USIS members on the support contract to help notify the field work contract folks what activities OPM might be taking relative to our audits. So, there is certainly that potential. I haven't seen any—again, I haven't seen any investigative report, whether they've identified anybody who was colluding, I guess would be the word, you know, with—between the two contracts that help circumvent our oversight process.[34]

After Mr. Miller's interview with Committee staff, the Department of Justice reported collusion between the fieldwork contract and the support services contract:

> USIS employees responsible for the review of background investigations under the Fieldwork Contracts would determine which categories or types of cases FIS was likely to be targeting for review by the federal staff. ... The Workload Leader ... and other designated personnel would then avoid dumping those types of cases.[35]

3. Financial Rewards to USIS and Its Executives

In 2007, USIS was purchased for $1.5 billion by Providence Equity Partners, a private equity firm that owns or has owned brands such as Metro-Goldwyn-Mayer, Warner Music Group, Univision and Whitepages.[36] Providence Equity Partners formed a holding company known as Altegrity to house two background investigation businesses, including USIS and another company known as HireRight.[37] Altegrity has grown in recent years to include two additional entities: Kroll Advisory Solutions and Kroll On-Track.

Soon after it was acquired in 2007, USIS announced a new compensation incentive policy. In April 2008, USIS reported that it was "piloting variable compensation incentives to

---

[33] House Committee on Oversight and Government Reform, Interview of Merton Miller (Jan. 8, 2014).

[34] *Id.*

[35] United States' Complaint, ¶ 71 (Jan. 22, 2014), *U.S. ex rel. Percival v. U.S. Investigations Services, Inc.*, M.D. Ala. (No. 11-CV-527-WKW).

[36] Providence Equity Partners, *Portfolio* (online at www.provequity.com/Portfolio/All-Regions) (accessed on Feb. 9, 2014).

[37] Altegrity, *Fact Sheet* (online at www.altegrity.com/fact-sheet.aspx) (accessed on Feb. 9, 2014).

drive quality and production, reward performance."[38] Following this announcement, the company reported increasingly surprising progress:

- By October 2008, USIS reported that it had reduced the number of cases that were 180 days old from 21,000 to 50 in the prior quarter. The company reported that its productivity was at an all-time high, that it decreased its inventory by 51%, and that it could take on more background investigations work.[39]

- By May 2009, USIS represented that it achieved a 96% reduction in cases more than 90 days old during a one year period.[40] USIS also reported that it set a 30 day goal for completing background checks, allocating 23 days for the field investigations and 7 days for quality reviews.[41]

- By January 2011, USIS reported submitting 99% of all cases to OPM before the assigned Completion Date and that the company's timeliness for background investigations was the best in USIS history.[42]

The alleged dumping of cases appears to have greatly reduced backlogs and resulted in significant financial rewards under the company's contract with OPM. OPM awarded USIS the following annual incentive awards under its contract:

Fiscal year 2008:	$2.4 million
Fiscal year 2009:	$3.5 million
Fiscal year 2010:	$5.8 million
Fiscal year 2011:	$4.3 million
Total	**$16 million**[43]

Senior USIS executives also benefitted financially since at least 75% of their personal bonuses were dependent on the company's meeting earnings and revenue targets.[44] For example, over the course of the alleged fraud:

- Bill Mixon, the former President and CEO who set internal corporate revenue goals, obtained bonuses and stock totaling more than $1 million.

---

[38] USIS, *PMR Fieldwork Services Q2 FY 2008* (Apr. 21, 2008).

[39] USIS, *PMR Fieldwork Services Q4 FY 2008* (Oct. 22, 2008).

[40] USIS, *PMR Fieldwork Services Q2 FY 2009* (May 28, 2009).

[41] *Id.*

[42] USIS, *PMR Fieldwork Services, Q1 FY 2011* (Jan. 26, 2011).

[43] Office of Personnel Management, *Annual Incentive Awards to USIS, CACI, KeyPoint.*

[44] USIS, *FY 2009 Annual Incentive Plan*; Altegrity, *FY 2010 Annual Incentive Plan*; Altegrity, *FY 2011 Annual Incentive Plan*; Altegrity, *FY 2012 Annual Incentive Plan.*

- The former Chief Financial Officer, who allegedly calculated the number of cases that needed to be reviewed and dumped to meet corporate goals, was awarded about $470,000 in bonuses.

- The former President of the Investigative Services Division, who allegedly instructed his employees to flush cases, obtained over $375,000 in bonuses.[45]

The bonus payments received by USIS executives raise questions about the extent of potential knowledge or complicity in the alleged fraud by executives at USIS's parent holding company, Altegrity, which is a privately held firm.

During the four years of the alleged fraud, Altegrity's subsidiaries received over $2.7 billion in federal contracts, performing investigative and cyber-security functions for a dozen federal agencies, including the Departments of Defense, State, Justice, and Homeland Security. Altegrity's board of directors consists exclusively of officials at Providence Equity Partners and the CEO of Altegrity.[46]

The bonus formula for USIS executives reserved 20-25% for personal performance during the period of the alleged fraud.[47] The Committee has not determined who at Altegrity evaluated the former USIS CEO's personal performance to determine his bonuses. The Committee also did not determine whether Altegrity officials had knowledge of the alleged fraud at any time, or what steps they may or may not have taken to address it.

4. Exodus of Two Dozen USIS Officials

In the wake of revelations about USIS misconduct under its contracts with OPM, 24 USIS employees have resigned, retired, or been terminated. According to a company spokesperson, "We have put in place new leadership, enhanced oversight procedures, and improved protocols that have been shared with OPM."[48]

These officials include Bill Mixon, the former President and Chief Executive Officer, as well as the former Chief Financial Officer, the former President of the Investigations Services Division, and the former Vice President of Field Operations.

In addition, just yesterday, USIS informed Committee staff that the company's most recent President of its Investigations Services Division of USIS resigned last week. From

---

[45] USIS, *Bonus Payment Recipients for FY 2008-2012.*

[46] Altegrity, *Board of Directors* (online at www.altegrity.com/BoardofDirectors.aspx) (accessed on Feb. 9, 2014).

[47] USIS, *FY 2009 Annual Incentive Plan;* Altegrity, *FY 2010 Annual Incentive Plan*; Altegrity, *FY 2011 Annual Incentive Plan.*

[48] *Justice Joins Whistleblower Suit Against USIS*, Wall Street Journal Washington Wire Blog (Oct. 30, 2013) (online at http://blogs.wsj.com/washwire/2013/10/30/justice-joins-whistleblower-suit-against-usis/).

January 2011 to December 2012, this official served as Vice President of Support Operations, "where he was responsible for quality, training, mobile technology, and communications."[49] He was promoted to his most recent position in December 2012 and had been "the primary point of contact for USIS's current five-year Background Investigations Fieldwork Services contract."[50]

As part of its investigation, the Committee determined that this official had been copied on the April 4, 2011 Problem Notification Letter in which OPM first expressed concerns that USIS had been releasing thousands of cases to OPM without conducting quality reviews required under its contract with OPM. (See Section II.C.1, above.)

III. LEGISLATIVE PROPOSALS

A. Preventing Contractor Conflicts of Interest

According to FIS Associate Director Merton Miller and DOJ, USIS's alleged fraud evaded detection for as long as it did in part because USIS misused a support services contract it held at the same time it was performing background investigations for OPM. Under that second contract, USIS employees reportedly were able to learn in advance about OPM's oversight auditing efforts and schedules, communicate that information to USIS management, and then adjusted their dumping efforts to avoid detection.

The conflict of interest posed by USIS holding these two contracts undermined OPM's oversight of the USIS fieldwork contract. Although OPM requires contractors like USIS to report conflicts of interest, that requirement was inadequate. Congress should prohibit a single contractor from simultaneously holding a background investigative fieldwork contract and an investigative support services contract.

OPM Director Archuleta announced last week that as of February 24, 2014, only federal employees will perform final reviews of background investigations and the 50 USIS workers currently performing this function under a secondary support services contract will no longer be conducting those reviews.[51]

Congress also should reconsider the extent to which outsourcing critical investigative functions may impact national security, such as the performance of Top Secret level investigations, subject interviews, and final quality reviews of investigations.

B. Improving Local Law Enforcement Agency Cooperation

Several subsequent investigations found that Alexis had a history of gun violence and anti-social behavior. These investigations determined that critical information about Alexis' past

---

[49] USIS, *Management Team* (online at www.usis.com) (accessed Feb. 7, 2014).

[50] *Id.*

[51] *U.S. Scales Back USIS's Role in Security Clearances*, Wall Street Journal (Feb. 7, 2014).

use of a gun and violent outbursts were not fully identified or understood by background investigators whose research informed Navy adjudicators' decision to award a security clearance to Alexis.

A significant challenge in the Alexis case was non-cooperation by the Seattle Police Department, which had a reputation for not responding to requests for information from background investigators. Section 9101 of Title 5 requires local law enforcement agencies to cooperate with federal background investigators, but OPM has determined that about 450 law enforcement agencies do not fully comply with this requirement.

Current law provides no means to encourage compliance or punish non-compliance with Section 9101. Congress should consider ways of incentivizing compliance by local law enforcement agencies. Congress should also clarify in statute the scope of reporting that is required.

C. Implementing Continuous Evaluation

The Committee's investigation found that Alexis' behavior grew increasingly erratic after he was granted a security clearance in 2008. In addition to his arrest in 2004, Alexis was arrested in Georgia in 2008 for disorderly conduct and in Texas in 2010 after firing his gun through the ceiling of his downstairs neighbor. A month before the Navy Yard incident, Rhode Island police were called to the hotel at which Mr. Alexis was staying, where he complained that he was hearing voices that were keeping him awake.[52]

Under current background investigations procedures, individuals possessing security clearances receive periodic reevaluations. Secret clearance holders are revaluated every 10 years. Top Secret clearance holders are reevaluated ever 5 years.[53]

Until periodic reevaluation, cleared individuals are required to self-report information, including derogatory information, to their employing agency. Federal contracting employers must also report potentially derogatory information to the federal agencies for which they provide contract services. But this system of reporting was clearly insufficient in the case of Aaron Alexis.

Congress should consider the creation of a system providing for continuous evaluation or monitoring of federal personnel holding security clearances through which federal agencies will have real-time access to critical information relevant to background check investigations, including arrest records, court records, financial credit history, currency transactions, foreign travel, social media, and terrorist and criminal watch lists.

---

[52] *Navy Yard Gunman Had History of Mental Illness, Checkered Military Career, Official Say*, Washington Post (Sept. 17, 2013); *Alleged Navy Yard Shooter Got Clearances Despite Troubled Past*, NPR (Sept. 17, 2013).

[53] Congressional Research Services, *Security Clearance Process: Answers to Frequently Asked Questions* (Sept. 9, 2013) (R43216).

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF ALABAMA
NORTHERN DIVISION

UNITED STATES OF AMERICA ex rel. BLAKE PERCIVAL	)	
Plaintiff,	)	
	)	Civil Action No. 2:11-CV-WKW
v.	)	
	)	**FILED EX PARTE AND UNDER SEAL**
U.S. INVESTIGATIONS SERVICES, INC.,	)	
Defendant.	)	

THE GOVERNMENT'S NOTICE OF ELECTION TO INTERVENE

Pursuant to the False Claims Act, 31 U.S.C. § 3730(b)(2) and (4), the United States notifies the Court that it hereby intervenes and intends to proceed with this action. The United States requests that it be given 90 days, up to January 22, 2014, in which to file its complaint.

The Government requests that the relator's Complaint, this Notice, and the attached proposed Order be unsealed. The United States requests that all other papers on file in this action remain under seal because in discussing the content and extent of the United States' investigation, such papers are provided by law to the Court alone for the sole purpose of evaluating whether the seal and time for making an election to intervene should be extended.

The United States reserves the right to seek the dismissal of the relator's action or claim on any appropriate grounds, including under 31 U.S.C. §§ 3730(b)(5) and (e)(4).

A proposed order accompanies this notice.

Respectfully submitted,

STUART F. DELERY
Assistant Attorney General
Civil Division

GEORGE L. BECK, JR.
United States Attorney
Middle District of Alabama

By: 
JAMES J. DUBOIS
Assistant United States Attorney
GA Bar Number: 231445
P.O. Box 197
Montgomery, AL 36101-0197
Telephone No.: (334) 223-7280
Facsimile No.: (334) 223-7418
E-mail: **James.DuBois2@usdoj.gov**

MICHAEL D. GRANSTON
TRACY L. HILMER
MELISSA R. HANDRIGAN
Attorneys, Civil Division
Commercial Litigation Branch
Post Office Box 261
Ben Franklin Station
Washington, D.C. 20044
Telephone: (202) 305-3083
Email: **Melissa.R.Handrigan@usdoj.gov**

Dated: October 24, 2013

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF ALABAMA
NORTHERN DIVISION

UNITED STATES OF AMERICA ex rel. BLAKE PERCIVAL	)	
Plaintiff,	)	
v.	)	Civil Action No. 2:11-CV-527-WKW
U.S. INVESTIGATIONS SERVICES, INC.,	)	**FILED EX PARTE AND UNDER SEAL**
Defendant.	)	

ORDER

The United States having intervened in this action, pursuant to the False Claims Act, 31 U.S.C. § 3730(b)(4), the Court rules as follows:

IT IS ORDERED that,

1. the relator's complaint, the Government's Notice of Intervention, and this Order be unsealed;

2. the United States serve its Complaint upon defendant, together with this Order, by January 22, 2014;

3. all other papers or Orders on file in this matter shall remain under seal; and

4. the seal shall be lifted on all matters occurring in this action after the date of this Order.

IT IS SO ORDERED,

This _____ day of _____, 2013.

_____
United States District Judge

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Federal Investigative Services
P.O. Box 618
1137 Branchton Rd
Boyers, PA 16018-0618

April 4, 2011
OPM04-06-00013

[redacted]
7500 Viscount, Suite 222
El Paso, TX 79925

SUBJECT: Quality Review Analysis

Quality of investigations is paramount within OPM Federal Investigative Services (FIS). This has been communicated and reiterated on numerous occasions with USIS and was recently emphasized again as a point of focus during a site visit to USIS WPA in Grove City on 2/3/11. The OPM contract speaks to the quality review requirements within section C.6.1.2 stating, [redacted] This is supported under sections B.1.2 *Quality Requirements* and B.2 *Pre-Submission Quality Review and Inspection and Evaluation System* of the USIS statement of work submitted to OPM May 15, 2006.

An analysis was conducted on Reports of Investigation (ROI) submitted to OPM between the dates of 2/21-2/28 to validate quality inspections as defined in the above cited contract and SOW sections. The results of the inspection reflect that of 6,560 ROI's there were over 750 that were Review Complete (RC) by USIS, but the first display (DR), print (PR) or modify (MO) event was completed by a federal staff member. This represents a significant number of ROI's that were released to OPM for final review and closing without appearing to receive the appropriate level of quality review expected from USIS.

The analysis also revealed that 4 USIS SIDS were responsible for the release of 13,113 ROI's over the course of the same 1 week timeframe representing an average of 3,278 ROI's per person. This indicates the utilization of a tool to release ROI's. Also noted is that two of the 4 SIDS associated with the release of these ROI's are not reflected in PIPS as reviewers and in many instances released all of the ROI's for a case. These same SIDs have also been observed to have completed both the DR and RC of other ROI's on many cases. This action is not in compliance with contract requirements as defined under Attachment 4 of the OPM contract reflecting qualification requirements for a Reviewer.

The expectation of OPM is that best practices are to be applied throughout the entire investigative process to insure that only ROI's that have been quality reviewed by qualified members of USIS Review are being submitted to OPM. This is necessary to fully support timely case closing to the requesting agencies as expected within the established timelines of the case service. Any failure of USIS to deliver a quality reviewed ROI to OPM results in the need to complete rework and inhibits the ability of OPM to deliver cases to requesting agencies in a timely manner.

OPM is requesting that USIS provide a response to this concern insuring that all ROI's are being reviewed by qualified reviewers and clarification of any automated systems or mechanism being use to complete or assist in the processing of ROI's including details of how the process is being utilized.

This correspondence is being sent via e-mail to [redacted]. A hard copy will not be sent unless specifically requested.

Sincerely,

Steven T. Anderson
Branch Chief
Field Investigations
Oversight Branch

cc: [redacted]
Larry Parson
J.C. Thieme

United States Congressman
STEPHEN LYNCH
Representing the 8th District of Massachusetts

For Immediate Release:
February 10, 2014

Contact: Meghan Aldridge
617-428-2009

LYNCH INTRODUCES BILL TO REFORM SECURITY CLEARANCE PROCESS

Congressman Stephen F. Lynch, the top Democrat on the Federal Workforce Subcommittee, today introduced comprehensive legislation to reform the security clearance process by which the federal government determines whether an individual is eligible to access classified national security information. The *Security Clearance Reform Act of 2014* (H.R. 4022) will better ensure that the security clearance process is defined by an efficient and high quality background check system, continuous federal oversight of issued security clearances, and maximum information-sharing between federal agencies and state and local law enforcement. H.R. 4022 is cosponsored by Rep. Elijah E. Cummings, Ranking Member of the House Oversight Committee.

The tragic shooting at the Washington Navy Yard in September of 2013 and other recent events involving government security clearances have again highlighted the need to implement comprehensive security clearance reform. As reported by the Washington Post, Navy Yard shooter Aaron Alexis applied for a security clearance in 2007 after enlisting as a full-time reservist in the U.S. Navy but without disclosing a 2004 arrest in Seattle, Washington, on a firearms-related offense. While USIS, the federal contractor responsible for performing Alexis's background check, discovered this prior charge, Navy officials have stated that the precise nature of the Seattle arrest was not included in Alexis's investigative file. Importantly, the background investigator was unable to obtain a copy of the police report from the Seattle Police Department and information available on the courts database did not include details of the arrest. As a result, Alexis was granted a security clearance in 2008. Despite additional arrests in Georgia and Texas in 2010, Alexis retained his security clearance following his discharge from the Navy in 2011 and worked as a defense contractor at military installations, including the Washington Navy Yard.

"The federal government's current background investigation process does not pick up events that arise in the interim period between a cleared individual's initial investigation and periodic reinvestigation, which in Alexis's case would not have occurred until 2017," said Congressman Lynch. "A review of the Aaron Alexis case reveals significant lapses in our security clearance process, including a deficiency in the ability to get criminal history information from state and local jurisdictions and a lack of continuous evaluation of security clearances that have already been issued," said Congressman Lynch. "H.R. 4022 would implement a continuous evaluation and monitoring system across the federal government so that we can immediately identify and address significant red flags that arise in a security clearance holder's background."

Most recently, the Department of Justice filed a breach of contract and false claims complaint against USIS, which handles almost 50% of background check investigations that the Office of Personnel Management assigns to contractors. According to the complaint, "beginning in at least March 2008 and continuing through at least September 2012, USIS management devised and executed a scheme to deliberately circumvent contractually required quality reviews of completed background investigations in order to increase the company's revenues and profits." In particular, the Department of Justice alleges that then-USIS senior management directed and engaged in the practice of "dumping" or "flushing" of cases which were released to the Office of Personnel Management without the quality review required by its federal government contract. While falsely representing that the company had performed these reviews, USIS allegedly "dumped" or "flushed" at least 665,000 background investigations which constituted 40% of the total number of investigations conducted by the company during this 4-1/2 year period.

"In light of these allegations regarding extended waste, fraud, and abuse in security clearance contracting, it is imperative that we bring key background investigative work back into the federal government," said Congressman Lynch. "My legislation will ensure that federal employees, rather than outside contractors, perform critical investigative functions, including Top Secret Clearance level investigations."

In particular, the *Security Clearance Reform Act of 2014* would require the President, within 6 months of enactment, to submit a strategic plan to Congress to improve security clearance and background investigation activities conducted by the federal government. Specifically, the plan must include the development of a continuous evaluation and monitoring system through which government agencies may access and receive real-time updates of critical information, including arrest records, currency transactions, and terrorist and criminal watch list reports, relevant to security clearance background investigations. In addition, the plan must contain guidance on improving information-sharing by state and local agencies with the federal

government as well as proposed methods for streamlining and eliminating outdated manual investigative processes in favor of electronic and accessible investigative databases. Moreover, the plan must require the in-sourcing of key background investigative functions in order to ensure that only federal employees, rather than outside contractors, are conducting quality reviews of Top Secret-level investigations and subject interviews. H.R. 4022 would require implementation of this strategic plan within 1 year of its submission to Congress.

As Ranking Member of the Federal Workforce Subcommittee, Congressman Lynch will also participate in a hearing held by the Oversight and Government Reform Committee entitled "DC Navy Yard Shooting: Fixing the Security Clearance Process." The hearing is scheduled for February 11th at 10:00am in room 2154 of the Rayburn House Office Building in Washington, D.C.

Statement of Congressman Gerald E. Connolly (VA-11)
Committee on Oversight and Government Reform
DC Navy Yard Shooting: Fixing the Security Clearance Process
February 11, 2014

Today nearly 5 million Federal employees and contractors hold some level of clearance. Yet, despite the recent proliferation of security clearances issued across the Federal Government, it is easy to forget that only a decade ago, the increasing demand for clearances resulted in a massive backlog that paralyzed our Nation's national security and intelligence apparatuses.

The lengthy delays left agencies and their private sector partners without enough cleared personnel to fulfill their missions – which endangered national security and forced Congress to act. After carefully investigating the causes of the problem, Congress concluded that it had to provide the agencies in charge of investigating clearance applicants with sufficient funds to leverage the services of private sector firms that specialize in background investigations.

Further, Congress enacted concrete statutory goals for timeliness of security clearance investigations, and most importantly, conducted diligent oversight to hold agencies accountable for meeting these goals. Meanwhile, the Executive Branch established effective interagency mechanisms to ensure agencies worked together to fulfill congressional mandates. And in an example of good governance that has become all too rare these days, the security clearance reform efforts worked.

Today, the backlog is gone and security clearance reform has been removed from the U.S. Government Accountability Office's High Risk List. Yet, recent high profile incidents remind us that our work is not done. In the wake of the Edward Snowden and Bradley Manning leak cases, and the horrific shootings at the Washington Navy Yard and Fort Hood, there is renewed attention on the current Federal security clearance process.

Once again, Congress must act to examine what additional improvements to the clearance process are needed, particularly with respect to quality. I'm hoping today's hearing held by the Committee on Oversight and Government Reform provides an opportunity for Members of Congress to work in a bipartisan fashion to strengthen the security clearance process and ensure we appropriately balance the need for timeliness with the need for full vetting.

Congress should address strengthening the security clearance process in a careful, balanced manner that eschews false solutions based on anecdotes and political expediency, in favor of a fact-based, dispassionate assessment of what must be fixed, and why. As we work to enhance the efficiency and effectiveness of the security clearance process, we must also ensure that we do not abandon the progress we have made to improve timeliness in exchange for more intensive vetting.

Further, we must accept the reality that the most effective security clearance enhancements will focus on improving collaboration between agencies *and* contractors, since each entity plays a critical role in security clearance suitability and determination operations. And finally, we must do some "myth-busting" to improve the accuracy and quality of the current debate revolving around security clearances.

For example, how many Americans are aware that *only the adjudicating agency* requesting a background investigation has the authority to grant a security clearance – and that in fact, neither the U.S. Office of Personnel Management (OPM) nor outside contractors possess that authority?

We've all seen news about the U.S. Department of Justice's complaint against one of the major contractors that does this work alleging that a small – though high level – group of employees were systematically submitting incomplete investigations to the government to maximize revenue. As I have always said, I will never defend the indefensible. If the charges are true, then this firm deserves to be held accountable for its actions. I would note that the firm did clean house in light of the allegations, removing the senior leaders who oversaw the questionable actions, and bringing in an entirely new management team to oversee strong internal reforms.

The bottom line is that we must improve the security clearance system to make sure it is working properly, and that our government knows all it needs to know about cleared personnel – whether a Federal worker or a contract employee – to preserve our national security interests and the basic safety of our Federal facilities.

Fortunately, the majority of legislative proposals to date have been serious, substantive measures that push for common sense reforms, such as increasing the frequency of random automated reviews of public records and databases to search for any information that might affect the status of those holding clearances. There is broad consensus that the current gap between initial and subsequent investigations – often 5 or 10 years – is far too long. Perhaps at one point this infrequent re-investigation rate simply reflected practical constraints and resource limitations. However, today we have the technology to make more continuous monitoring work.

My hope is that the Committee will also take a close look at legal and bureaucratic obstacles that currently hinder investigators, whether they are government or contractor employees, such as the lack of a government-wide Federal database with arrest records from State and Local law enforcement and State and Federal laws that restrict access by investigators to credit and employment information.

A decade ago Congress fixed the backlog. Today's Congress can improve the system that was put in place, but only if we resist temptations to unproductively pit Federal employees versus their contractor counterparts, and remember that the most effective reforms will strengthen the process for *all* security clearance reviews, whether conducted solely by Federal employees or by a combination of Federal worker and contractor.

-END-

GAO Highlights

Highlights of GAO-14-138T, a statement for the record to the Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

Recently the DNI reported that more than 5.1 million federal government and contractor employees held or were eligible to hold a security clearance. GAO has reported that the federal government spent over $1 billion to conduct background investigations (in support of security clearances and suitability determinations for federal employment) 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.

This statement addresses (1) a general overview of the security clearance process; (2) what is known about the quality of investigations and adjudications, which are the determinations made by executive branch agency officials to grant or reject clearance requests based on investigations; and (3) the extent of reciprocity, which is the decision of agencies to honor clearances previously granted by other agencies. This statement is based on GAO work issued from 2008 to 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 relevant statutes, federal guidance, and processes, (2) examined agency data on the timeliness and quality of investigations and adjudications, (3) assessed reform efforts, and (4) reviewed a sample of case files for DOD personnel.

View GAO-14-138T. For more information, contact Brenda S. Farrell at (202) 512-3604 or farrellb@gao.gov.

February 11, 2014

PERSONNEL SECURITY CLEARANCES

Actions Needed to Ensure Quality of Background Investigations and Resulting Decisions

What GAO Found

Several agencies have key roles and responsibilities in the multi-phased personnel security clearance process, including the Director of National Intelligence (DNI) who, as the Security Executive Agent, is responsible for developing policies and procedures related to security clearance investigations and adjudications, among other things. The Deputy Director for Management at the Office of Management and Budget chairs the Performance Accountability Council that oversees reform efforts to enhance the personnel security process. The security process includes: the determination of whether a position requires a clearance, application submission, investigation, and adjudication. Specifically, agency officials must first determine whether a federal civilian position requires 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 the Office of Personnel Management (OPM) conduct background investigations for most executive branch agencies. Adjudicators from requesting agencies use the information from these investigations and federal adjudicative guidelines to determine whether an applicant is eligible for a clearance. Further, individuals are subject to reinvestigations at intervals based on the level of security clearance.

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 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 risks will be scrutinized more closely. GAO reported in 2009 that, with respect to initial top secret clearances adjudicated in July 2008 for the Department of Defense (DOD), documentation was incomplete for most of OPM's investigative reports. GAO independently estimated that 87 percent of about 3,500 investigative reports that DOD adjudicators used to make clearance eligibility decisions were missing some required documentation, such as the verification of all of the applicant's employment, the required number of social references for the applicant, and complete security forms. In May 2009, GAO recommended that OPM measure the frequency with which its investigative reports met federal investigative standards to improve the completeness—that is, quality—of investigation documentation. In January 2014, DNI officials said that metrics to measure quality of investigative reports had not been established.

GAO reported in 2010 that executive branch agencies do not consistently and comprehensively track the extent to which reciprocity is occurring because no government-wide metrics exist to consistently and comprehensively track when reciprocity is granted. The acceptance of a background investigation or personnel security clearance determination completed by another authorized agency is an opportunity to save resources and executive branch agencies are required by law to grant reciprocity, subject to certain exceptions, such as completing additional requirements like polygraph testing. GAO's 2010 recommendation that the leaders of the security clearance reform effort develop metrics to track reciprocity has not been fully implemented.

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

Thank you for the opportunity to comment on the federal government's approach to background investigations. As you know, we have an extensive body of work on issues related to the personnel security clearance process. Since 2008, we have focused on the government-wide effort to reform the security clearance process. A high-quality personnel security clearance process is necessary to minimize the associated risks of unauthorized disclosures of classified information and to help ensure that information about individuals with histories of criminal activity or other questionable behavior is identified and assessed as part of the process for granting or retaining clearances. However, recent events, such as unauthorized disclosures of classified information, have shown there is more work to be done by federal agencies to help ensure that the clearance process functions effectively and efficiently, so that only trustworthy individuals obtain and keep security clearances and the resulting access to classified information.

Personnel security clearances allow government and industry personnel (contractors) to gain access to classified information that, through unauthorized disclosure, can in some cases cause exceptionally grave damage to U.S. national security. It is important to keep in mind that 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 either a military or federal civilian employee, or contractor for the federal government. Separate from, but related to, personnel security clearances are determinations of suitability that the executive branch uses to ensure that individuals are suitable, based on character and conduct, for federal employment in their agency or position.

The federal government processes a high volume of personnel security clearances at significant costs. Recently, the Director of National Intelligence (DNI) reported that as of October 2013, more than 5.1 million federal government and contractor employees held or were eligible to hold a security clearance. Furthermore, 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. The Department of Defense (DOD) accounts for the majority of all personnel

security clearances—788,000 background investigations that cost over $787 million in fiscal year 2011.[1]

My statement today will focus on three topics related to personnel security clearances. First, I will provide a general overview of the security clearance process, including how clearances are acquired and retained. Second, I will discuss what is known about the quality of clearance investigations and adjudications, which are the determinations made by agency officials to grant or reject clearance requests based on investigations. Third, I will discuss the extent of reciprocity, which is the decision of agencies to honor clearances previously granted by other agencies.

My statement 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, federal guidance, and processes; 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.

The work upon which this statement 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]GAO, *Background Investigations: Office of Personnel Management Needs to Improve Transparency of Its Pricing and Seek Cost Savings*, GAO-12-197 (Washington, D.C.: Feb. 28, 2012).

The Personnel Security Clearance Process

Multiple executive-branch agencies are responsible for different phases of the federal government's personnel security clearance process. For example, in 2008, Executive Order 13467 designated the DNI as the Security Executive Agent.[2] 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. In turn, executive branch agencies 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. Investigators—often contractors—from Federal Investigative Services within the Office of Personnel and Management (OPM)[3] conduct these investigations for most of the federal government using federal investigative standards and OPM internal guidance as criteria for collecting background information on applicants.[4] OPM provides the resulting investigative reports to the requesting agencies for their internal adjudicators, who use the information along with the federal adjudicative guidelines to determine whether an applicant is eligible for a personnel security clearance.

[2]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).

[3]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.

[4]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.

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 the authority, direction, and control of the USD(I), manages and administers the DOD portion of the National Industrial Security Program for the DOD components and other federal services by agreement, as well as providing security education and training, among other things.[5]

The Intelligence Reform and Terrorism Prevention Act of 2004 prompted government-wide suitability and security clearance reform.[6] 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 annually report on its timeliness expired in 2011. More recently, the Intelligence Authorization Act of 2010 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.[7] 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, including 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.

[5]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).

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

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

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. In a 2008 memorandum, the President called for a reform of the security clearance and suitability determination processes and subsequently issued Executive Order 13467, which in addition to designating the DNI as the Security Executive Agent, also designated the Director of OPM as the Suitability Executive Agent. Specifically, the Director of OPM, as Suitability Executive Agent, is responsible for developing policies and procedures to help ensure the effective, efficient, and timely completion of investigations and adjudications relating to determinations of suitability, to include consideration of an individual's character or conduct. Further, the executive order established a Suitability and Security Clearance Performance Accountability Council (Performance Accountability Council) to oversee agency progress in implementing the reform vision. Under the executive order, this council is accountable to the President 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 as the Chair of the council.[8]

Steps in the Personnel Security Clearance Process

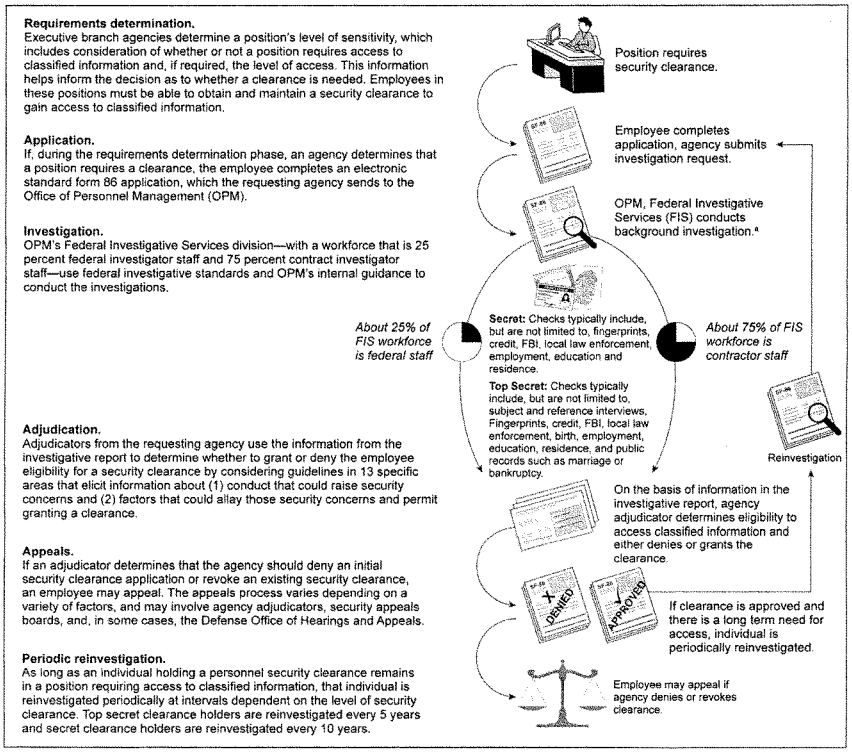
To help ensure the trustworthiness and reliability of personnel in positions with access to classified information, executive branch agencies rely on a personnel security clearance process that includes multiple phases: requirements determination, application, investigation, adjudication, appeals (if 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

[8]The Performance Accountability Council consists of the DNI 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 a Vice Chair and designate officials from additional agencies to serve as members. As of June 2012, the council included representatives from the Departments of, Energy, Health and Human Services, Homeland Security, State, the Treasury, and Veterans Affairs, and the Federal Bureau of Investigation.

have slightly different personnel security clearance processes, the phases that follow are illustrative of a typical process.[9]

[9]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 are more substantial than for a secret clearance. 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.

Figure 1: Steps in the Executive Branch 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

In the first step of the personnel security clearance process, executive branch officials determine the requirements of a federal civilian position, including 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.[10] 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.[11]

A sound requirements determination 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 resultant costs. In addition to cost implications, limiting the 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.

In 2012, we reported that the DNI, as the Security Executive Agent, had not provided agencies with clearly defined policy and procedures to consistently determine if a position requires a security clearance, or established guidance to require agencies to review and revise or validate existing federal civilian position designations.[12] We recommended that the DNI issue policy and guidance for the determination, review, and validation of requirements, and ODNI concurred with those recommendations, stating that it recognized the need to issue or clarify policy.

We routinely monitor the status of agency actions to address our prior report recommendations. As part of that process, we found that a January

[10]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.

[11]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. Executive Order 13526, *Classified National Security Information*, (Dec. 29, 2009).

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

25, 2013 presidential memo authorized the DNI and OPM to jointly issue revisions to part 732 of Title 5 of the *Code of Federal Regulations*, which provides requirements and procedures for the designation of national security positions. Subsequently, ODNI and OPM drafted the proposed regulation; published it in the *Federal Register* on May 28, 2013; and the comment period closed. We reported on October 31, 2013 that ODNI and OPM officials stated that they would jointly review and address comments and prepare the final rule for approval from the Office of Management and Budget.

Application Phase

Once an applicant is selected for a position that requires a personnel security clearance, a security clearance must be obtained in order for an individual 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. During the application submission phase, 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) using OPM's electronic Questionnaires for Investigations Processing (e-QIP) system or a paper copy of the Standard Form 86 to the individual to complete; (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 applicant's employment and education. However, many background investigation types have similar components. For instance, for all investigations, information that applicants provide on

electronic applications is 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.

Table 1: Information Gathered in Conducting a Typical Investigation to Determine Suitability and Eligibility for a Personnel Security Clearance

Type of information gathered by component	Type of background investigation	
	Secret	Top Secret
1. Personnel security questionnaire: The reported answers on an electronic Standard Form-85P or Standard Form-86	X	X
2. Fingerprints: Fingerprints submitted electronically or manually	X	X
3. National agency check: Data from the Federal Bureau of Investigation, military records, and other agencies as required (with fingerprints)	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. National agency check for spouse or cohabitant: Data from the 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, and resolution of significant issues or inconsistencies	[a]	X

Sources: DOD and OPM.

Notes: The content and amount of information collected as part of a personnel security clearance investigation depend on a variety of case-specific factors, including the history of the applicant and the nature of the position; however, items 1 through15 are typically collected for the types of investigations indicated.

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

[a]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, ODNI and OPM jointly issued a revised version of the federal investigative standards for the conduct of background investigations for individuals who 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.[13]

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.[14] To make clearance eligibility decisions, the adjudication guidelines specify that adjudicators consider 13 specific areas that elicit information about (1) conduct that could raise security

[13]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.

[14]For industry personnel, the Defense Security Service adjudicated clearance eligibility for DOD and 24 other federal agencies, by agreement, using OPM-provided investigative reports. DOD is in the process of consolidating its adjudication functions, including those for industry personnel. Per Department of Defense, *National Industrial Security Program: Operating Manual*, DOD 5220.22-M (Feb. 28, 2006), the 24 agencies are the (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.

concerns and (2) factors that could allay those security concerns and permit granting a clearance.[15]

If a clearance is denied or revoked, appeals of the adjudication decision are possible. We have work under way 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 he or she remains in a position that requires access to classified national security information, that individual is reinvestigated periodically at intervals that depend 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 local law enforcement agencies where an individual lived and worked since the last investigation. Further, the Joint Reform Team began an effort to review the possibility of continuing 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 or 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 of populations that could potentially represent risk to the government because they already have access to classified information. The revised federal investigative

[15]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, including knowledgeable participation; the frequency and recency of the conduct; and the individual's age and maturity at the time of the conduct, among others.

standards state that the top secret level of security clearances may be subject to continuous evaluation.[16]

Actions Needed to Ensure Quality of Clearance Investigations and Adjudications

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 process. We have emphasized—since the late 1990s—the need to build and monitor quality throughout 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.[17] For example, in 2008 two of the key factors we identified to consider in efforts to reform the security clearance process were building quality into every step of the clearance processes and having a valid set of metrics for evaluating efficiency and effectiveness.[18] We have begun additional work to review the quality of investigations.

As previously discussed, DOD accounts 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. [19] It remained on our list until 2011 because of ongoing concerns about delays in processing clearances and problems with the quality of investigations and adjudications. Specifically, we reported in 2009 on (1) incomplete investigative reports from OPM, the agency that supplies about 90

[16]In March 2009, the Joint Security and Suitability Reform Team issued an Enterprise Information Technology Strategy that included a concept of continuous evaluation that included automatic and randomly scheduled security evaluations using automated record checks. Such checks would provide an automatic notification to the person being investigated, security managers, or other designated personnel that continuous evaluation is being conducted.

[17]GAO, *DOD Personnel: Inadequate Personnel Security Investigations Pose National Security Risks*, GAO/NSIAD-00-12 (Washington, D.C.: Oct. 27, 1999).

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

[19]GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: Jan. 2005). Every 2 years at the start of a new Congress, GAO issues a report that identifies government operations that are high risk because of their vulnerabilities to fraud, waste, abuse, and mismanagement, or are most in need of transformation to address economy, efficiency, or effectiveness.

percent of all federal clearance investigations, including those for DOD; and (2) the granting of some clearances by DOD adjudicators even though some required data were missing from the investigative reports used to make such determinations.

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 decision were missing at least one type of documentation required by federal investigative standards.[20] 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 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.

In addition to incomplete investigative reports, our 2009 report also identified issues regarding the quality of DOD adjudications. With respect to DOD adjudicative files, in 2009, 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 regulation requires 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.[21] 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 review in 2009, neither OPM nor DOD measured the completeness of its investigative reports or adjudicative files, which limited the agencies'

[20]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.

[21]Department of Defense, *DOD Personnel Security Program* Regulation 5200.2-R (January 1987, incorporating changes Feb. 23, 1996).

ability to explain the extent to which or the reasons why some files are incomplete.

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. 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.

As a result of the incompleteness of OPM's investigative reports on DOD personnel and the incompleteness of DOD's adjudicative files that we first identified in our 2009 report, we made several recommendations to OPM and DOD. We recommended 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.[22] OPM did not agree or disagree with our recommendation.

In a subsequent February 2011 report, we noted that the Office of Management and Budget, ODNI, DOD, and OPM leaders had provided congressional members and executive branch agencies with metrics to assess the quality of investigative reports and adjudicative files and other aspects of the clearance process. For example, the Rapid Assessment of

[22]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, D.C.: May 19, 2009).

Incomplete Security Evaluations was one tool the executive branch agencies planned to use for measuring quality, or completeness, of OPM's background investigations.[23] However, in June 2012 an OPM official said that OPM chose not to use this tool and opted to develop another tool. We currently have work under way to review any actions OPM has taken to develop and implement metrics for measuring the completeness of OPM's investigative reports. However, ODNI officials confirmed in January 2014 that OPM did not have such metrics in place.

According to OPM officials, OPM also continues to assess 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. 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 affect timeliness. Further, relying on agencies to voluntarily provide information on investigation quality may not reflect the quality of OPM's total investigation workload.

We also recommended in 2009 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.[24] 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 DOD 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

[23]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 percentage of investigations completed that contained deficiencies.

[24]GAO-09-400.

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 because of funding shortfalls. DOD restarted the use of RADAR in fiscal year 2012.

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.

We initially placed DOD's personnel security clearance program on our high-risk list in 2005 because of delays in completing clearances.[25] 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.[26] 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,

[25]GAO-05-207.

[26]*GAO, High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

monitor, and update outcome-focused performance measures.[27] 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 has 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.

Extent of Clearance Reciprocity Is Not Measured

Although 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, we reported in 2010 that agencies do not consistently and comprehensively track the extent to which reciprocity is granted government-wide. 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.[28] Further, in October 2008, ODNI issued guidance on the reciprocity of personnel security clearances.[29] The guidance requires, except in limited circumstances, that all Intelligence Community elements "accept all in-scope[30] security clearance or access determinations." Additionally, Office of Management and Budget guidance requires agencies to honor a clearance when (1) the prior clearance was

[27]GAO, Personnel Security Clearances: Continuing Leadership and Attention Can Enhance Momentum Gained from Reform Effort, GAO-12-815T (Washington, D.C.: June 21, 2012).

[28]Pub. L. No. 108-458 § 3001 (2004).

[29]Office of the Director of National Intelligence, *Reciprocity of Personnel Security Clearance and Access Determinations, Intelligence Community Policy Guidance 704.4* (Oct. 2, 2008).

[30]Although there are broad federal investigative guidelines, the details and depth of an investigation vary by agency depending upon agency mission.

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) 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.[31]

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. 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 stated that they routinely honor other agencies' security clearances, and personnel security clearance information is shared between OPM, DOD, and, to some extent, Intelligence Community databases.[32] 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

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

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

steps to ensure that 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, we reported in 2010 that according to agency officials since there is no government-wide standardized training and certification process for investigators and adjudicators, 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 or adjudications conducted by other agencies or organizations.[33] To achieve fuller reciprocity, clearance-granting agencies seek to have confidence in the quality of prior investigations and adjudications.

Because of these issues identified by agency officials as hindrances to reciprocity and because the extent of reciprocity was unknown, we recommended in 2010 that the Deputy Director of Management, Office of Management and Budget, 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 the Office of Management and Budget 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)

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

contractor to government, and (4) contractor to contractor. The ODNI report stated that data fields necessary to collect the information described above do not currently reside in any of the data sets available, and the process was completed in an agency-specific, semimanual method.

The Deputy Assistant Director for Special Security of ODNI noted in testimony in June 2012 that measuring reciprocity is difficult, and despite an abundance of anecdotes, real data are hard to come by. To address this problem, in 2013 ODNI planned to develop a web-based form for individuals to use to submit their experience with reciprocity issues to ODNI. According to ODNI, this would allow it to collect empirical data, perform systemic trend analysis, and assist agencies with achieving workable solutions. However, in January 2014, ODNI officials told us that required resources and information technology were not available to support the development and implementation of a web-based form. Instead, ODNI is conducting a Reciprocity Research Study that will involve, among other things, agencies identifying their ability to collect reciprocity metrics. This study would assist ODNI in developing reciprocity performance measures and a new policy for reciprocity. ODNI would also use the study to determine if a web-based form would be of value.

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 is imperative. The progress that was made with respect to reducing the amount of time required for 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.

Further, ensuring the quality of personnel security clearance investigations and adjudications is important government-wide, not just for DOD. While reciprocity is required by law and, if implemented correctly, could enhance efficiency and present cost savings opportunities, much is unknown about the extent to which previously granted security clearance investigations and adjudications are honored government-wide. Therefore, we recommended that metrics are needed to track reciprocity, which have yet to be fully developed and implemented. Assurances that all clearances are of a high quality may further encourage reciprocity of investigation and adjudications. We will

continue to monitor the outcome of the agency actions discussed above to address our outstanding recommendations.

Chairman Issa, Ranking Member Cummings and Members of the Committee, this concludes my statement for the record.

GAO Contact and Staff Acknowledgements

For further information on this testimony, please contact Brenda S. Farrell, Director, Defense Capabilities and Management, who may be reached at (202) 512-3604 or farrellb@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony include Margaret Best (Assistant Director), Lori Atkinson, Kevin Copping, Elizabeth Hartjes, Jeffrey Heit, Suzanne Perkins, Amie Steele, Erik Wilkins-McKee, and Michael Willems.

Altegrity and Subsidiary Co. Federal Contracts, FY08-FY12

System for Award Management: www.sam.gov

○