

**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

Table of Contents	1
I. Executive Summary	2
II. Aaron Alexis: A Case Study for Reform	4
A. 2004: Alexis’ Malicious Mischief Arrest.....	4
B. 2008 – 2011: Alexis’s Time in the Navy Reserve	5
C. 2013: The Newport Incident	7
D. Interactions with the VA	9
E. September 16, 2013: The Navy Yard Shooting	10
III. The Federal Security Clearance Process.....	12
A. Initiation of a Security Clearance Investigation.....	13
B. Field Investigation and Quality Review of a Security Clearance Application	15
i. Investigator Field Work	15
ii. Quality Review of Contractor Investigations	24
iii. Final Quality Review by OPM FIS	27
iv. Integrity Assurance.....	28
C. Adjudication by the Department of Defense.....	29
D. Periodic Reinvestigation	32
IV. Legislative Improvements: How to Patch Holes in the Process	32
A. Continuous Evaluation.....	32
B. Use of the Internet and Social Media for Background Investigations	35
C. Communication between Adjudicators and Investigators.....	38
D. Mental Health Evaluation.....	39
E. Cooperation From State and Local Law Enforcement Agencies	40
V. Allegations of Fabrication and Fraud	43
VI. Conclusion	44

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 Prevention Act 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 length³. 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.faihtstreet.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, 2013); 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?		
<input type="checkbox"/> YES <input type="checkbox"/> 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 NACLIC 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 checks¹⁵⁷ 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 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: YES NO (If NO, proceed to Section 22)

- 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.

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 comprising 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 agencies²³⁰ 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.