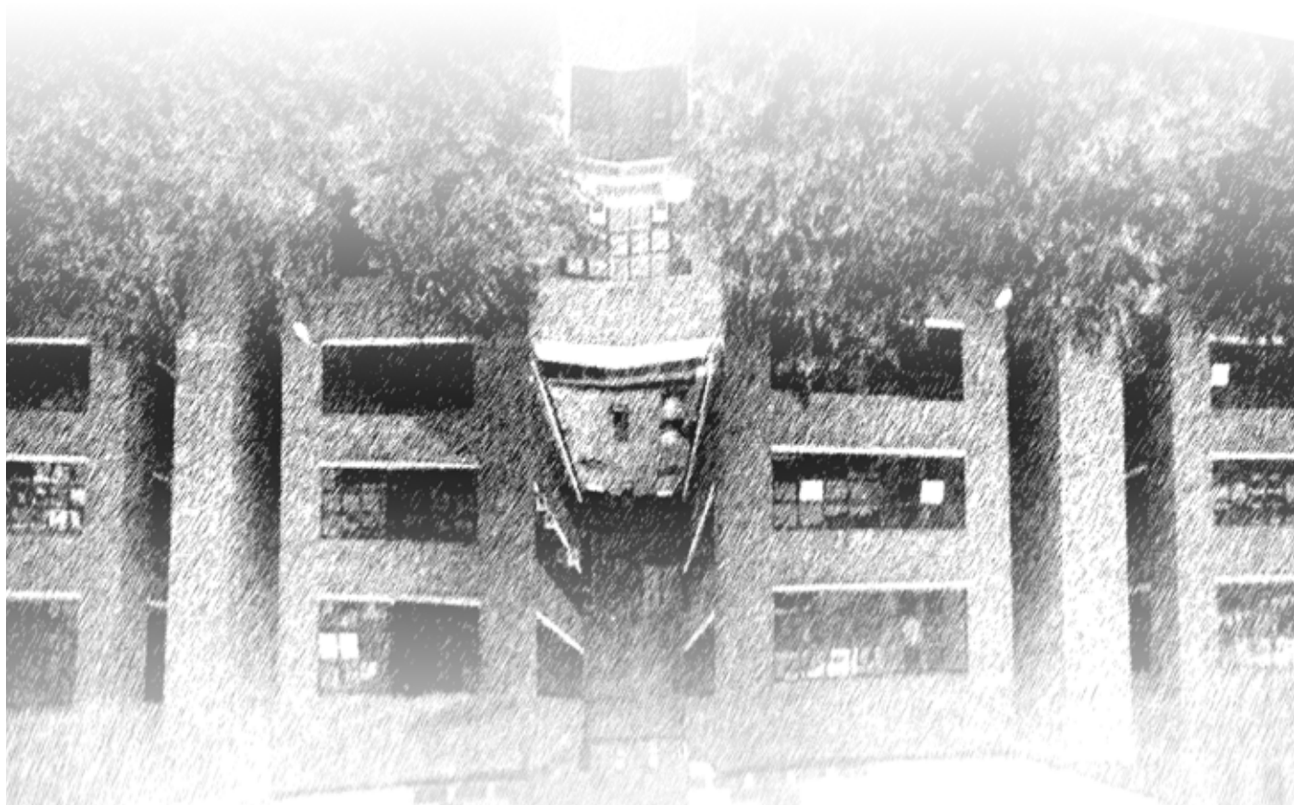
DEPARTMENT OF DEFENSE

Internal Review of the Washington Navy Yard Shooting

A Report to the Secretary of Defense

APPROVED FOR PUBLIC RELEASE

Under Secretary of Defense for Intelligence • November 20, 2013



DEPARTMENT OF DEFENSE

Internal Review of the Washington Navy Yard Shooting

A Report to the Secretary of Defense

Executive Summary

Approximately 5 million people employed by or affiliated with the Department of Defense are eligible for access to classified information.

"We like to give people the benefit of the doubt." Response by a Navy official when asked why records of Aaron Alexis' arrests and non-judicial punishment were never reported in the Joint Personnel Adjudication System

"Insiders are always the most dangerous." Gavin de Becker[1]

1. Introduction

On September 16, 2013, Aaron Alexis, a Navy contractor employee with a Secret security clearance, shot and killed 12 U.S. Navy civilian and contractor employees and wounded several others at the Washington Navy Yard. Alexis was also killed.

Alexis was employed by The Experts, Inc., a private information technology firm cleared under the National Industrial Security Program. The Experts was a subcontractor to Hewlett-Packard Enterprise Services, which was performing work under a contract with the Department of the Navy. Pursuant to his employment with The Experts, Alexis was assigned to a project at the Washington Navy Yard and began working there on September 9, 2013.

On September 14, 2013, Alexis purchased a Remington 870 12-gauge shotgun and ammunition at a gun shop in Northern Virginia. He also purchased a hacksaw and other items at a home improvement store in Northern Virginia, using the hacksaw to modify the shotgun for concealment.

On the morning of September 16, Alexis arrived at the Washington Navy Yard. He had legitimate access to the Navy Yard as a result of his work as a contractor employee and used his valid building pass to gain entry to Building 197. Shortly after his arrival in the building and over the course of about one hour,

1 Gavin de Becker is president of Gavin de Becker & Associates, Inc., a private security company. Mr. de Becker provided a briefing to the Internal Review Team on an automated threat assessment system designed to predict and prevent acts of targeted violence.

Alexis used the Remington 870 shotgun and a Beretta handgun he obtained during the attack to kill 12 individuals and wound 4 others before he was shot and killed by law enforcement officers.

On September 30, 2013, the Secretary of Defense initiated concurrent independent and internal reviews to identify and recommend actions that address gaps or deficiencies in DoD programs, policies, and procedures regarding security at DoD installations and the granting and renewing of security clearances for DoD employees and contractor personnel.

2. Conclusions and Significant Findings

Following mass shootings and other incidents of targeted violence, the immediate question that springs to mind is "What did we miss?" The Department asked this question in 2009 after Major Nidal Hasan shot and killed 13 people and wounded 43 others in Fort Hood, Texas. We asked this question in 2012 after Specialist Ricky Elder fatally shot his battalion commander and then turned the gun on himself. We are asking this question again today, in the wake of the tragedy at the Washington Navy Yard. Guided by the Terms of Reference (Appendix A), the Internal Review Team conducted an exhaustive examination of Alexis' historical record provided by the Department of the Navy (Appendix B) and applicable personnel security and installation access policy. The team also analyzed previous incidents in which an insider inflicted significant harm, in order to gain a better understanding of the causes and common characteristics of these events. The results of the team's examinations provide the basis for the findings and recommendations in this report.

At the time of the shooting, Aaron Alexis was a vetted member of the U.S. Navy Individual Ready Reserve and a defense contractor employee cleared to the Secret level. He was authorized access to the Washington Navy Yard and to Building 197 through the use of his DoD Common Access Card (CAC) and valid building pass. The Internal Review Team found the Washington Navy Yard was in general compliance with DoD installation access policies, although random vehicle or bag inspections were not conducted in accordance with DoD policy. There is no way to know, however, whether more frequent inspections might have given law enforcement personnel the opportunity to discover the weapon Alexis carried onto the installation and neutralize or minimize the immediate threat.

At various points during Alexis' military service and subsequent employment as a cleared contractor — from the background investigation in 2007 to the disturbing behaviors he exhibited in the weeks leading up to the shooting — the review revealed missed opportunities for intervention that, had they been pursued, may have prevented the tragic result at the Washington Navy Yard. When examining events in Aaron Alexis' history individually, they yield little in the way of warning. Combined, however, they demonstrate a pattern of misconduct and disturbing behavior that would have prompted investigators, for a position of trust in the Federal workforce, if they had been aware of his history in aggregate.

What vulnerabilities in DoD programs, policies, or procedures regarding physical security at DoD installations and the security clearance and reinvestigation process can be strengthened?

The Internal Review Team identified several vulnerabilities that may have alerted the Department to the potential threat before the incident occurred. The team's significant findings, summarized below, are detailed in section 7 of this report:

- The Office of Personnel Management (OPM) background investigation was missing critical information.
- The Navy granted Alexis a Secret security clearance with specified conditions, but there was no oversight mechanism in place to ensure compliance.
- Alexis' Navy command did not report in the security system of record multiple incidents of adverse information during Alexis' active duty service.
- Alexis' employer, The Experts, Inc., had no insight into Alexis' chronic personal conduct issues during his Navy service when they hired him and placed him in a position that required access to classified information.
- Alexis' employer did not report behaviors indicating psychological instability and did not seek assistance from a mental health professional or guidance from the Defense Security Service.
- Although the Review found no direct ties to gaps in physical security practice and the actual events of September 16, planned cuts in physical

security and vulnerability assessments funding and an overall lack of compliance with installation access control policy[2] are likely to leave the Department vulnerable to threats to mission assurance.

Although the findings above did ultimately play a role in the events that occurred on September 16, it is important to note that the vulnerabilities the team identified in personnel security clearance or installation access processes do not signify culpability for this mass shooting. Even if those vulnerabilities had not been present, neither the personnel security process nor the physical security capability is equipped or designed to prevent the kind of violence exhibited by Aaron Alexis. A holistic, centralized threat management capability, as directed in the Secretary of Defense's March 26, 2013, memorandum,[3] is essential to effectively prevent violent behavior in the workplace.

How should the Department address these vulnerabilities to prevent incidents of targeted violence in the future?

The most effective methods to prevent targeted violence in the workplace must be employed long before someone enters an installation with a weapon. The Internal Review Team developed a series of recommendations, outlined in section 7 and summarized below, designed to provide the Department with such a threat prevention strategy. Pillars of an effective threat prevention strategy should include:

- A centralized insider threat management capability that leverages multidisciplinary subject matter experts and links to functional and organizational areas of responsibility.
- A continuous evaluation program that provides actionable information in real time on the entire cleared DoD population, is serviced by the DoD Consolidated Adjudications Facility (CAF), folds in DoD Intelligence Community personnel as appropriate, and is scalable to include all DoD personnel subject to suitability or fitness adjudications.
- A physical security approach that employs defense in depth using technology and manpower to reduce risk and mitigate potential threats.

2 DoD Inspector General Report, "Navy Commercial Access Control System Did Not Effectively Mitigate Access Control Risks," September 16, 2013

3 Secretary of Defense memorandum, "Final Recommendations of the Defense Science Board on Predicting Violent Behavior," March 26, 2013

Transforming DoD Security and Insider Threat Assessment Capabilities

To achieve these objectives, the Internal Review Team recommends the Department:

- Establish a DoD Insider Threat Management and Analysis Center (DITMAC) to provide a centralized capability that can quickly analyze the results of automated records checks and reports of behavior of concern and recommend action as appropriate.
- Leverage existing continuous evaluation capability while continuing to develop and implement a DoD Continuous Evaluation Program.
- Accelerate the Defense Manpower Data Center's development of the Identity Management Enterprise Services Architecture (IMESA) to enable DoD Components to share access control information and continuously vet individuals against U.S. Government authoritative databases.

Way Ahead

The Deputy Secretary of Defense will synthesize the findings of the Independent Review Team with those from the Internal Review and concurrent reviews conducted by the Secretary of the Navy. The Deputy Secretary will consolidate key recommendations from each of these reviews into a final report to be provided to the Secretary of Defense by December 20, 2013.

If approved, the key components of the effective threat management capability described above should be placed under the authority, direction and control of a single Principal Staff Assistant that would align multiple security disciplines and enable cross-functional insider threat assessment and response. The Principal Staff Assistant would develop an implementation plan in coordination with the DoD Components and the Office of the Director of National Intelligence.

DEPARTMENT OF DEFENSE

Internal Review of the Washington Navy Yard Shooting

A Report to the Secretary of Defense

Internal Review of the Washington Navy Yard Shooting

3. Overview and Methodology

On September 30, 2013, the Deputy Secretary of Defense directed the Under Secretary of Defense for Intelligence, in coordination with senior representatives from each of the Military Departments, the Joint Staff, and the Office of the Secretary of Defense, to lead a DoD-wide Internal Review to:

- Examine the security programs, policies, processes, and procedures related to the shooting;
- Identify vulnerabilities or weaknesses that may have alerted the Department to the threat before the incident occurred; and
- Recommend actions to enable the Department to prevent such incidents from occurring in the future.

Concurrently, the Secretary established an Independent Review Team to focus on the same objectives as the Internal Review without any potential institutional constraints with regard to its findings and recommendations. In parallel with these efforts, the Secretary of the Navy commissioned his own series of "rapid reviews" focused on Department of the Navy installations, procedures, and policy.

The three review teams established a shared foundation of facts to avoid duplicative requests to the Department and other organizations for the same information. The teams each assessed the data and arrived at conclusions independently. Following the submission of this report to the Deputy Secretary of Defense, the Internal Review Team's findings and recommendations will be consolidated with those of the Independent Review Team and the Department of the Navy reviews.

The Internal Review Team established working groups to review the principal areas identified in the Terms of Reference: the personnel security clearance and reinvestigation process and physical security at DoD installations. The working groups hosted focused interviews and discussions to inform the assessment process and provided regular input to the Internal Review Team, which came

together twice weekly to receive briefings and interview briefers in accordance with the task. The Internal Review Team consolidated the input of both working groups with data extracted from the research of policy and other documentation to develop this report. As directed in the Terms of Reference, the team:

- Considered findings and recommendations from previous relevant reports and studies.
- Examined all applicable laws, policies, and regulations, including DoD directives, instructions, and manuals.
- Included interviews with appropriate senior officials (health affairs, law enforcement and force protection, first responders, intelligence) and other pertinent individuals.
- Formulated recommendations for correcting problems and enhancing internal controls to prevent similar incidents in the future and mitigate associated risk.

4. Personnel Security Clearance Process

4.1 Overview

The personnel security clearance process is governed primarily by Executive Order 12968[4], Executive Order 13467[5], and the Federal Investigative Standards. DoD governing issuances include the January 1987 DoD Regulation 5200.2.R, "DoD Personnel Security Program" (with changes), and the April 1999 DoD Directive 5200.2, "DoD Personnel Security Program." The DoD issuances have undergone significant revision over time, and new versions are in various stages of the formal coordination process in the Department.

The DoD directive will be replaced by DoD Instruction 5200.02, which has been under review with the Office of Management and Budget (OMB) since September 2012. The DoD regulation will be replaced by a comprehensive two-volume DoD manual. DoD Manual 5200.02 – Volume 1, "DoD Personnel Security Program (PSP): Investigations for National Security Positions and Duties," is en route to the Office of Management and Budget for interagency review and posting in the Federal Register for comment. DoD Manual

4 Executive Order 12968, "Access to Classified Information," August 2, 1995, as amended

5 Executive Order 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information," June 30, 2008

5200.02 – Volume 2, "DoD Personnel Security Program (PSP): Adjudications, Due Process, Continuous Evaluation, and Security Education," is in formal coordination within the Department. The Department has also developed a new issuance, DoD Instruction 5200.kk, "Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)." After formal coordination in the Department, this instruction will be forwarded to OMB for interagency review and posting in the Federal Register for comment.

The Department of Defense has about 4.6 million non-intelligence agency military, civilian, and contractor personnel who have been deemed eligible for access to classified information. Of these, 2.5 million currently have access to classified information as follows:

- ☐ Top Secret or Top Secret/Secret Compartmented Information: 875,785
- ☐ Secret: 1,670,495
- ☐ Confidential: 1,824

4.2 Background Investigations and Clearance Adjudication

A "personnel security investigation" (PSI) is any investigation required to determine the eligibility of military, civilian, or government contractor personnel for a national security position, including those with access to classified information. All PSIs are conducted by the designated investigative service provider. In the case of the Department of Defense, the U.S. Office of Personnel Management (OPM) is the designated investigative service provider.

There are different PSIs required for the levels of security clearance based on position sensitivity. For a Secret clearance, applicants must have a National Agency Check with Local Agency Checks and Credit Check (NACLC) or an Access National Agency Check with Written Inquiries (ANACI). NACLCs and ANACIs are valid for continued eligibility for 10 years from the date of investigation closure, provided the subject does not have a consecutive break in service of more than 2 years.

For a Top Secret clearance or Top Secret with access to Sensitive Compartmented Information (SCI), an applicant must have a Single Scope Background Investigation (SSBI) at a minimum. SSBIs are valid for 5 years from the date of investigation closure, provided the subject does not have a consecutive break in service of more than 2 years.

OPM forwards completed investigations to the DoD Consolidated Adjudications Facility (CAF) or the intelligence agency CAFs, as appropriate, for adjudication. An adjudicator assigned to a case will review the PSI and make a clearance determination, identifying potential disqualifying information and applicable mitigating factors within the parameters of the 13 National Adjudicative Guidelines.

A "periodic reinvestigation" (PR) is an investigation conducted to update a previously completed background investigation. Currently, PRs are required at the following intervals:

- ☐ every 5 years for a Top Secret clearance or access to a highly sensitive program
- ☐ every 10 years for a Secret clearance
- ☐ every 15 years for a Confidential clearance

4.3 U.S. Office of Personnel Management

In 2005, the Department of Defense transferred most of its personnel security investigative workload and investigators to OPM. The Department pays OPM approximately $700 million annually to complete investigations.

How much does an initial security clearance cost per person?

SSBI for Top Secret and Top Secret/SCI clearance: $3,959
ANACI for civilian employee Secret clearance: $272
NACLC for military and contractor Secret clearance: $210*

****20–25% of investigations for Secret access require subject interviews to resolve issues, at an additional cost of $550 per person.***

(Cost data effective FY 2014)

4.4 DoD Consolidated Adjudications Facility

In 2011, the Department's personnel security adjudicative organizations relocated to Fort Meade, Maryland, as part of the 2005 Base Realignment and Closure Committee recommendations. The Department subsequently established the DoD CAF to consolidate resources and standardize adjudicative processes. Beginning in October 2012, the DoD CAF began a phased consolidation of the seven non-intelligence agency CAFs:

- The Joint Staff
- Army
- Navy
- Air Force
- The Adjudicative Division of the Defense Office of Hearings and Appeals
- Defense Industrial Security Clearance Office
- Washington Headquarters Services

Today, the DoD CAF comprises more than 700 employees, manages clearances for a population of about 4.6 million non-intelligence agency personnel with security clearance eligibility, and provides support to about 43,500 DoD organizational security managers and contractor facility security officers.

The DoD CAF determines the security clearance eligibility of non-intelligence agency DoD personnel occupying sensitive positions and/or requiring access to classified material. These determinations involve all military service members, civilian employees, contractor personnel working at 26 Federal agencies under the National Industrial Security Program, and consultants affiliated with the Department of Defense. The DoD CAF also makes favorable adjudicative determinations for employment suitability of DoD civilian employees and determinations for CAC credentialing of non-cleared DoD contractor personnel.

A Snapshot of Security Clearance Statistics

Average annual personnel security clearance determinations in FY 2013	*850,000*
Clearances denied or revoked annually in FY 2013	*10,500 (1.2%)*
Conditional clearances and waivers granted annually in FY 2013	*4,600*
Percentage of OPM investigations assessed as inadequate or incomplete	*31%*

4.5 Intelligence Reform and Terrorism Prevention Act

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) required the Executive branch to establish a plan that, beginning in December 2009, would require, to the extent practicable, 90 percent of all background investigations and adjudications for personnel security to be completed within an average of 60 days from date of receipt of investigation requests by the designated investigative agency. The 60-day average period allowed:

- no more than 40 days to complete the investigative phase of the clearance review; and
- no more than 20 days to complete the adjudicative phase of the clearance review.

IRTPA also required that determinations on clearances not made within 60 days would be made without delay.

In 2012, the Director of National Intelligence, pursuant to his authority in Executive Order 13467 as Security Executive Agent, further refined the original IRTPA standards by establishing timeliness requirements specific to Top Secret-level clearances. The fastest 90 percent of Top Secret-level investigations and adjudications must be completed within 100 days.

4.6 Adverse Information Reporting

DoD policy requires commanders, heads of organizations, and cleared contractors in the National Industrial Security Program to develop and maintain a program that ensures all pertinent derogatory information regarding cleared

personnel is forwarded for consideration in the personnel security clearance determination process. The DoD CAF is notified of derogatory information typically through the Joint Personnel Adjudication System (JPAS), which is the DoD system of record for personnel security clearance adjudication and management. Derogatory information is reported in the form of "incident reports" in JPAS.

The DoD CAF receives about 45,000 incident reports a year on cleared personnel who have had security-related issues; examples include bankruptcies, arrests for driving under the influence, mental health issues, and security violations. Most of these incident reports are based on information that is self-reported by the cleared individual. Other reports are based on information reported by supervisors, co-workers, or other government agencies.

4.7 Personnel Security Program Continuous Evaluation Initiatives

The Federal Investigative Standards (FIS), which set the parameters for conducting PSIs and PRs in the Federal Government, were revised in December 2012. Once the FIS are fully implemented in the Department of Defense, all personnel in national security positions will be required to have a PR every 5 years (regardless of the level of clearance), and a portion of personnel with Top Secret clearances will be subject to a continuous evaluation process as prescribed by the Director of National Intelligence as the Security Executive Agent.

The Department has pursued numerous initiatives to implement some form of continuous evaluation as part of the Personnel Security Program. Executive Order 12968 was amended in 2008 by Executive Order 13467 to add Subsection 3.5, "Continuous Evaluation," which established that all individuals who have access to classified information are subject to continuous evaluation.

In 2005, the Defense Personnel Security Research Center (PERSEREC) developed the Automated Continuing Evaluation System (ACES) to electronically check records for the continuous evaluation of cleared DoD employees. Currently, ACES is capable of checking over 40 government and commercial databases in areas relevant to personnel security and even applying business rules to identify those individuals who may present a potential security risk. ACES complies with legal and regulatory provisions for the protection of individual privacy and permissible uses of government and commercial data. ACES provides some current capability for the Department to conduct some

continuous evaluation of up to 100,000 personnel annually as authorized by national policy while the Department develops the "next generation" ACES capability.

A recent pilot test with a sample of 3,370 Army service members, civilian employees, and contractor personnel demonstrated that ACES was able to identify 731 individuals with previously unreported derogatory information (21.7 percent of the tested population), prompting 176 reinvestigations to resolve or adjudicate that derogatory information. Of this group, 99 individuals had serious derogatory information (e.g., financial issues, domestic abuse, drug abuse, or prostitution). Based on the results of this test, the Army revoked the clearances of 55 of these individuals and suspended the access of the remaining 44.

Implementation of ACES, as approved by the Director of National Intelligence, would enable the Department to detect unreported derogatory information and greatly improve its ability to mitigate risk. ACES' functionality also has the potential to serve as a continuous evaluation tool for employment suitability and CAC credentialing pursuant to Homeland Security Presidential Directive 12 (HSPD-12), discussed immediately below.

5. Installation Access Control Process

DoD minimum installation access control standards are based on the mandate of HSPD-12 to provide a common identification standard for all Federal employees and contractors. Federal Information Processing Standard 201-2 prescribes the standards for identity verification, issuance, and use of the common identity standard.

All Federal departments and agencies are required to use an eligible personal identity verification credential to ensure interoperability for access to facilities, installations, and information systems. The DoD personal identity verification credential is the CAC. The CAC provides a level of identity assurance and a standardized method of authentication for Federal and contractor employees, and it is the principal identity credential for supporting interoperable access to DoD installations, facilities, buildings, and controlled spaces. Upon presentation of a CAC at a perimeter access control point, the individual's identity is verified either electronically or through physical/visual inspection to enable the holder to access the installation or facility.

DoD policy directs non-Federal Government and non-DoD-issued card holders who are given unescorted access to DoD installations to be identity proofed and vetted to determine fitness and eligibility for access. DoD policy further directs that personnel must be vetted against government authoritative data sources, to include the National Crime Information Center (NCIC) and Terrorist Screening Database (TSDB).

Key policies of the Department's physical security access control program require the Military Departments to implement the following:

- Biometrically enabled background security screening
- Identification card security features
- Identity-proofing and vetting
- Database interfaces
- Access control point widening and construction (e.g., vehicle and pedestrian gates/lanes and entrapment and inspection areas)
- DoD-wide installation of interoperable security hardware (e.g., CAC/identification card readers, computer systems, closed circuit television monitors, barriers)
- Trained security and law enforcement personnel
- CAC/identification card visual inspection requirements and issuance/revocation procedures

6. The Insider Threat Perspective: Comparative Incidents

Fort Hood, Texas, 2009

On November 5, 2009, U.S. Army Major Nidal Malik Hasan shot and killed 13 people and wounded 43 others in Fort Hood, Texas. It was the single largest mass shooting event on a U.S. military installation in the Nation's history. Before his assignment to Fort Hood, Hasan worked as an intern and resident at Walter Reed Army Medical Center. His colleagues and superiors there expressed concern about his behavior and comments. Hasan was described as socially isolated, increasingly and vocally opposed to the wars in Afghanistan and Iraq, and troubled by his work with traumatized Soldiers returning from combat. In the year leading up to the attack, Hasan was known to have been in

communication with Anwar Al-Awlaki expressing interest in jihad and suicide attack. Army commanders were notified of his e-mails to Awlaki, but at the time their communications were deemed non-threatening.

> ***"Whether internal threats target a computer system, classified information, or personnel, research suggests they may often share common indicators. The effort to identify threats may be enhanced by exploiting any common indicators and integrating the disparate programs designed to defend against these threats."***
>
> ***"Protecting the Force: Lessons from Fort Hood," Report of the DoD Independent Review, January 2010***

WikiLeaks, 2010

In May 2010, U.S. Army Specialist Bradley Manning was arrested for leaking the largest number of classified documents to the public in U.S. history through the website operated by WikiLeaks, an international organization opposing secrecy. In the months leading up to the unauthorized disclosure, Manning displayed behaviors indicating instability through multiple emotional and physical outbursts, expressed discontent with the Army and the Federal Government, and disregarded basic security measures common to all classified working environments.

Washington Navy Yard, 2013

On September 16, 2013, then-Navy contractor employee Aaron Alexis concealed a sawed-off shotgun in a backpack and used it to kill 12 Navy employees and injure 4 others at the Washington Navy Yard before he was killed by law enforcement personnel. He was previously an active duty Sailor, had several arrests — two of which involved firearms — and, in the weeks leading up to the incident, he was observed complaining of being followed, hearing voices, and of being under attack by vibrations and microwaves.

Although these incidents differ in both circumstances and outcome, all three incidents — each inflicting historic damage to the Department and to DoD employees — have several common characteristics:

- The perpetrators had all been granted security clearances. They were all trusted insiders.
- Before causing such damage to the Department, all had telegraphed their personal dissatisfaction with their employers or were observed exhibiting aberrant behavior.
- All had legitimate access to the facilities in which they committed their offenses.

It is through these commonalities that the Internal Review Team sought to apply lessons learned from the previous incidents to its examination of the Washington Navy Yard shooting. To support this effort, the team reviewed the August 2012 Defense Science Board report on predicting violent behavior[6] and other authoritative sources, to include briefings from the Federal Bureau of Investigation's Behavioral Analysis Unit and other experts on violent behavior. The Defense Science Board report's final recommendations relating to violent behavior, approved by the Secretary of Defense in March 2013, included a Department-wide "threat management approach employing multidisciplinary professionals" as a holistic method of addressing targeted violence.

The team's research revealed that both acts of violence and of deliberate unauthorized disclosure have the same root causes, and perpetrators engage in planning and preparation steps that are often detectable, providing an opportunity to disrupt an intended act.[7] Threat management principles, therefore, can be employed to avert not only incidents of targeted violence but also deliberate acts of unauthorized disclosure.

As a direct result of the WikiLeaks disclosures, the President issued "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs" in November 2012. The cover memorandum signed by the President states, "... elements [of an insider threat program] include the capability to gather, integrate, and centrally analyze and respond to key threat-related information; monitor employee use of classified networks; provide the workforce with insider threat awareness training; and protect the civil liberties and privacy of all personnel."

While some elements of such a departmental program may exist today, they are not organized under policy, oversight and funding into compliance with national policy. In September 2013, the Deputy Secretary of Defense designated

6 Defense Science Board Task Force Report, "Predicting Violent Behavior," August 2012

7 Ibid.

the Under Secretary of Defense for Intelligence (USD(I)) as the senior official charged with overseeing insider threat efforts in the Department. [8]

7. Findings and Recommendations

7.1 Key Findings

Finding 1. The OPM investigation was missing critical information.

Although the 2007 OPM background investigation of Alexis did include a follow-up subject personal interview to resolve discrepancies in Alexis' SF-86 information, multiple discrepancies remained undetected and unchallenged by OPM. During this subject interview, Alexis characterized his 2004 arrest in Seattle for "malicious mischief" as nothing more than an altercation with another individual that escalated, in which he (Alexis) retaliated by "deflating the tires" of the other individual's car.

Alexis did not disclose that he accomplished this by shooting out the tires with his Glock .45 caliber handgun in a residential area. The Seattle Police Department incident report (Appendix B), which OPM did not obtain, reveals an account that is markedly different from the one Alexis portrayed in his subject interview. He was initially charged in the King County District Court with malicious mischief (a felony), although this charge was dismissed. The Seattle Police Department then referred the incident to the Seattle Municipal Court on the lesser charges of property destruction and discharge of a firearm (these charges were likewise dismissed).

In addition to the 2004 arrest, which may have brought to light early behaviors of potential mental instability, there was incomplete or discrepant information in Alexis' reported references, education, delinquent debts, places of address, and foreign travel. A more thorough investigation may have given the Department of the Navy Central Adjudication Facility (DONCAF) sufficient facts on which to simply deny Alexis security clearance eligibility instead of granting eligibility with specified conditions.

8 Secretary of Defense Memorandum, "Appointment of the DoD Senior Official Charged With Overseeing Insider Threat Efforts," September 25, 2013

Finding 2. The Navy granted Alexis a Secret security clearance with specified conditions, but there was no oversight mechanism in place to ensure compliance.

Upon review of the OPM investigation, DONCAF identified potentially disqualifying conditions in the areas of personal conduct, financial considerations, and criminal conduct. However, DONCAF determined these conditions were mitigated under the National Adjudicative Guidelines and granted Alexis' Secret security clearance eligibility in 2008, with a warning letter to Alexis via his commanding officer advising that his eligibility was granted only under the conditions that he seek financial counseling, resolve his outstanding indebtedness, and maintain financial solvency. Although this warning was entered in JPAS, there was no process in place for DONCAF to monitor compliance, and there is no evidence Alexis' commanding officer took action to ensure Alexis met the conditions, as was required in the warning letter.

Finding 3. Alexis' Navy command did not report in the security system of record multiple incidents of adverse information during his active duty service.

During his active duty, despite two additional arrests (one of which also involved discharge of a firearm) and chronic personal conduct issues resulting in formal counseling and imposition of non-judicial punishment, the Navy reported none of this adverse information in JPAS. Alexis' command at the time did not consider reporting his misconduct in any security system of record, because Alexis did not need to access classified information in the course of his regular duties. This perception is common in the Department, as the existing DoD policy is not clear. Volume 2 of the new DoD Manual 5200.02, which is in the formal coordination process, contains language that clarifies the requirement to report adverse information on all individuals who are eligible for access to classified information, regardless of whether they actually access classified information. DoD Manual 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)," states that "Contractors are required to report certain events that impact the status of an employee's personnel security clearance (PCL)."

Finding 4. Alexis' employer, The Experts, Inc., had no insight into Alexis' chronic personal conduct issues during his Navy service when they hired him and placed him in a position that required access to classified information.

With no adverse information recorded in JPAS and no break in service in excess of 2 years, Alexis remained eligible for a Secret security clearance after his release from active duty and transition to the Individual Ready Reserve in the Navy in January 2011. Subsequently, Alexis was hired in September 2012 by The Experts, Inc., which served as a subcontractor to Hewlett Packard Enterprise Services (HPES), LLC. When The Experts first hired Alexis, there was no information available in JPAS that would have alerted the company to any misconduct while on active duty in the Navy. The Experts did perform a background check as required by the terms of its contract with HPES, but this background check revealed no issues of concern. It is not known whether The Experts, as part of its hiring process, contacted any references such as Alexis' former Navy supervisor to ascertain his fitness for employment. If The Experts had been aware of Alexis' prior history, this information may have led The Experts to assess his erratic, troubling behavior in August 2013 as that indicative of an individual who might pose a threat to himself or others.

Finding 5. Alexis' employer did not report behavior indicating psychological instability and did not seek assistance from a mental health professional or guidance from the Defense Security Service.

The Experts became aware of Alexis' erratic behavior during August 2013 and was sufficiently concerned to remove Alexis' access in JPAS temporarily but did not report the incident in JPAS or seek guidance from the Defense Security Service about whether it should be reported. The employer's decision not to report Alexis' behavior appears to be influenced by a lack of awareness about what types of behaviors are considered "adverse" information that must be reported (particularly those related to mental health issues). Anecdotal evidence suggests a reluctance to report adverse information for a variety of reasons (for example, reluctance to "ruin a career" over something that may be deemed minor

or isolated, or because of a personal relationship). This lack of awareness and reluctance to report is not limited to the cleared contractor community, but is also prevalent government-wide.

This illustrates a gap in existing processes and training of security personnel regarding psychological conditions associated with significant security or safety risks. While reporting of criminal behavior is a relatively straightforward area, reporting of behaviors that indicate psychological impairment is not well defined in policy. Compounding this problem is the lack of a centralized structure that can receive and assess such reports and recommend interventions or caretaking actions that may disrupt an individual's potential path to committing violence.

There may be reluctance to report mental health-related behaviors in particular and confusion on when to report such behaviors, because an adverse information report is often viewed as potentially punitive rather than a caretaking or intervening measure. Additionally, JPAS is the DoD system of record for personnel security clearance adjudication and management, not a mechanism designed to seek help from mental health professionals. Consequently, even if The Experts had reported the August incidents in JPAS, it is unknown whether such reporting might have provided an opportunity for intervention measures to prevent the shooting in September. However, The Experts did not seek assistance from a mental health professional to assess the potential for violence based on Alexis' behavior.

Finding 6. Although the Review found no direct ties to poor physical security practice and the actual events of September 16, planned cuts in physical security and vulnerability assessment funding and an overall lack of compliance with installation access control policy introduce risk and could be a factor in the future.

The Fiscal Year 2008 National Defense Authorization Act directs the Secretary of Defense to develop access standards applicable to all military installations in the United States, to include the ability to determine the fitness and verify the identity of all visitors. Not all visitors are being vetted before gaining unescorted access to DoD installations. The Defense Installation Access Control (DIAC) Working Group, under the auspices of the DoD Physical Security Equipment Action Group, is developing a Joint Concept Technology Demonstration effort

called the Identity Management Enterprise Services Architecture (IMESA) to serve as the overarching architecture. This architecture will allow all Military Departments' physical access control systems to share information and provide a continuous information management capability that continuously updates information in the authoritative databases.

Vulnerability assessments are a critical tool to enable commanders to identify vulnerabilities and mitigate risk. A Joint Staff Integrated Vulnerability Assessment (JSIVA) evaluates an installation's ability to deter and/or respond to a terrorist incident. Due to fiscal constraints, beginning in FY 2015, the Defense Threat Reduction Agency will reduce the number of JSIVAs from 80-100 each year to 30 (up to a 70 percent reduction). Fiscal constraints also impact the Military Departments' ability to initiate their own assessment programs. As a result, some installations will go without a higher headquarters vulnerability assessment.

7.2 Key Recommendations

Transforming DoD Security and Insider Threat Assessment Capabilities

Effective insider threat mitigation requires a more coordinated and consolidated approach to security policies and reporting capabilities. These roles provide distinct challenges for mitigation of associated threats and are not always integrated or synchronized. Information that could identify DoD personnel who are insider threats is available from numerous sources (e.g., personnel security, physical security, information assurance, counterintelligence, human resources, and law enforcement), to include mental health evaluations, but is not centralized or integrated. This inability to integrate and evaluate information in a "whole person" context is, in large part, because of the lack of a single centralized function or authority with the responsibility to aggregate, evaluate, and appropriately disseminate insider threat information. [9]

"Continuous evaluation" is traditionally viewed as an information system; rather, it is a process and capability to generate informed decisions regarding the trustworthiness of DoD personnel based on the composite of organizational information and the linkage of that information through technology

9 The September 25, 2013 Deputy Secretary of Defense memorandum appointed the USD(I) as the senior official charged with overseeing DoD insider threat efforts. The Department is drafting its Insider Threat Policy and Implementation Plan, in accordance with the National Insider Threat Policy and Minimum Standards and E.O 13587.

infrastructure. To get to that capability, the Department should create a DoD Insider Threat Management and Analysis Center (DITMAC). The DITMAC would serve as the "one stop shop" to consolidate and analyze all DoD reporting of potentially adverse information, to include potential insider threat information. The DITMAC would also be responsible for:

- Tasking the automated records checks system
- Analyzing the results for continuous evaluation
- Sending identified issues to the appropriate responding organization for further evaluation and action

The DITMAC should be a multifunctional team composed of law enforcement, mental health, counterintelligence, security, human resources, information assurance, cybersecurity, and legal personnel. The DITMAC should include a 24-hour watch center to respond to emergent issues, which would satisfy a Department of Justice requirement for 24-hour command center capability to access the TSDB. It should also be responsible for developing training requirements for identification and mitigation of insider threats.

The DITMAC must be closely aligned and should perhaps be co-located with the DoD CAF. In implementing a continuous evaluation program, the number of new investigations and additional adjudicative responsibility can be expected to increase, at least initially. The DoD CAF would need to be augmented to handle the additional workload imposed by continuous evaluation.

Both the DITMAC and the DoD CAF would depend on two critical information technology platforms: the Defense Information System for Security (DISS) and the Automated Continuous Evaluation System (ACES). DISS has more capability and flexibility than JPAS, was developed in 2005 and has not yet been fully resourced as a DoD system of record. For the DITMAC to be effective and for the DoD CAF to reach its full potential, DISS should be funded, built, and maintained appropriately.

As described in section 4.7, ACES is the first-generation automated continuous evaluation system. This system operates on an "on demand" basis and can evaluate up to 100,000 personnel annually. In its present state, ACES has limited operational utility for continuous evaluation of the entire cleared population. Further, it does not have the ability to gather and present new information continuously and in real time. However, with sufficient funding, the Department can begin immediately to evaluate potentially high-risk populations (e.g., personnel with overdue PRs, those with access to Special Access Program

information, and those cleared for access to Top Secret information and above) while the next-generation system is completed.

Development of the next-generation system is already under way; however, additional research is required before its concepts are fully realized and its compliance with Director of National Intelligence continuous evaluation requirements established. The next-generation system leverages IMESA, a continuous evaluation platform to be used at the local command level for installation access. Because IMESA is still in the concept demonstration phase, it is not yet a DoD system of record.

ACES, IMESA, and the DITMAC would constitute the critical elements of a Departmental continuous evaluation program and provide the foundation for an effective insider threat program. To avoid stovepipes in policy and procedures that inhibit effective threat management, the resourcing, policy requirements, and oversight responsibility should fall under a single Principal Staff Assistant in the Office of the Secretary of Defense. Currently, ACES is led by the Under Secretary of Defense for Personnel and Readiness, and IMESA is led by the Under Secretary of Defense for Acquisition, Technology and Logistics.

Implementation of all of these elements, in aggregate, would address most of the findings in this review. In addition, it will facilitate DoD compliance with the National Insider Threat Policy issued by the President in 2012.[10]

The concept of bringing critical security components under a single governance structure is not new: in 2010, the Under Secretary of Defense for Intelligence conducted a study on improving DoD security through the establishment of a DoD security field activity. [11] On a smaller scale, the Defense Intelligence Agency has already established such a structure, which serves as a model for a successful cross-functional effort for mitigating insider threat through continuous evaluation of personnel.

10 Presidential Memorandum, "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs," November 21, 2012

11 Office of the Under Secretary of Defense for Intelligence, "Feasibility Study for the Establishment of a DoD Security Field Activity, December 15, 2010

Primary Recommendations: Mitigating Insider Threat Through Continuous Evaluation

Recommendation 1.
Establish an organizational framework under the authority, direction and control of a single Principal Staff Assistant that would align multiple security disciplines and enable cross-functional insider threat assessment and response.

Recommendation 2.
Within such an organizational framework, establish a DoD Insider Threat Management and Analysis Center to provide a centralized capability that can quickly assess reports of behavior that may be of concern and recommend action as appropriate. Establishment of the DITMAC :

- Leverages the 2012 Defense Science Board recommendation for a Threat Management Unit concept to prevent and mitigate various types of insider threat.
- Aligns with DoD efforts to implement a DoD insider threat program.
- Integrates and aligns existing information reporting to counterintelligence, information assurance, law enforcement, human resource, and security entities.
- Serves as a "one stop shop" leveraging the capabilities of subject matter experts.
- Synchronizes efforts with those of the DoD CAF and the DoD Intelligence Community CAFs.

Recommendation 3.
Leverage existing ACES capability while continuing to develop and implement a DoD Continuous Evaluation Program. The first-generation ACES could enable the Department to assess high-risk populations within the pool of cleared personnel and identify potential issues that may not have been reported. The next-generation ACES capability would:

- Support the CAFs and proposed DITMAC.
- Assist with local level vetting/installation access control through IMESA.
- Be executed in compliance with the Director of National Intelligence requirements under his role as Security Executive Agent.

Recommendation 4. Accelerate the Defense Manpower Data Center's development of IMESA to enable DoD Components to share access control information and continuously vet individuals against U.S. Government authoritative databases. Procure electronic physical access control systems that provide capability to rapidly and electronically authenticate credentials and individuals authorized to enter an installation.

Supporting Recommendations: Enabling the DITMAC

- Provide additional human resources to the DoD CAF to enable more thorough evaluation of investigative products.
- Accelerate implementation of the Defense Information System for Security.
- Based on insider threat training requirements and standards established by the DITMAC, develop an education and awareness program to train the trusted population and continuously reinforce:

  - The importance of reporting any concerning behaviors via a centralized, objective, automated mechanism that is not designed to be negative or punitive.
  - The importance of supervisors' roles in "managing the 90 percent and referring the 10 percent" who cause concern.
  - The message that early intervention on behalf of people struggling with real or perceived issues is a win-win for everyone, including the organization.

Interim Recommendations: Closing Gaps in Existing Policies and Procedures

Background Investigations

- Establish standards for completeness of background investigation forms and facilitate their electronic management and storage.
- Accelerate and expand efforts to reformat SF-86 data and reports of investigation to support more automated, efficient, consistent, and reliable detection of potential security concerns.
- Revise the Federal Investigative Standards to require OPM to provide copies of all records reviewed in the course of investigations to the DoD CAF, including arrest records or other documentation associated with criminal conduct. This will ensure investigators and adjudicators have the information they need to detect and resolve discrepancies adequately, enabling a more informed adjudicative process.
- Require OPM to obtain signed statements from the subjects of significant issue cases.
- Director of National Intelligence reconsider adopting the Question 21 language recommended in a PERSEREC technical report,[12] which proposes a two-part relevant risk approach to Question 21 focusing on standardized clinical conditions that could pose a security risk as well as mental health-related hospitalizations.

Adjudication and Security Clearance Oversight

- Update the National Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, Guideline I,

12 Jonathan Shedler and Eric Lang, Executive Summary of PERSEREC Technical Report, "A Relevant Risk Approach to 'Question 21': Security Clearance Inquiries Regarding Mental Health," May 4, 2012 (revised September 3, 2013

"Emotional, mental, and personality disorders," to specify standardized clinical conditions associated with heightened security, safety and reliability risk.

- Consider expanding the mission of the DoD CAF to include adjudications, both favorable and unfavorable, of background investigations to support HSPD-12 suitability determination.
- Ensure adjudicators have the means by which to request additional information or investigative activity when they believe the information they have is insufficient or leaves discrepancies unresolved.
- Develop a mechanism by which the DoD CAF can track waivers and conditional clearances granted and take action to revoke or deny continued clearance eligibility for non-compliance.
- Task the DoD Components to review their JPAS records to ensure data accuracy.
- Require DoD Component and agency heads to validate annually the need for security clearances for individuals who are eligible but have not required access in the past 12 months.
- Hold security personnel accountable for incident reporting.
- Working with the Office of the Director of National Intelligence, identify appropriate protocols for the inactivation of eligibility at a time less than 24 months after a break in service occurs.

Security Education and Training

- Develop more rigorous training requirements for component security managers and industry facility security officers.
- Evaluate, update, and standardize security education and training on identifying reportable behaviors and events, how they should be reported, and to whom. Establish recurring training requirements to ensure that all personnel — including supervisors, commanders, and security managers — are continuously reminded and demonstrate knowledge of their responsibility to report incidents of security concern.
- Include security training at all commanders' courses and in professional military education.

Installation Vulnerability Assessments

- Fund the JSIVA program in FY 2015 and beyond until the Department transitions to a broader Mission Assurance Assessment Capability in order to retain the Chairman's critical independent vulnerability assessment capability.

8. Detailed Assessment of DoD Programs, Policies, and Procedures

The Internal Review Team examined a variety of DoD programs, policies, and procedures in the context of the Washington Navy Yard shooting to identify issues that may present Department-wide vulnerabilities. Using the Terms of Reference in Appendix A as the overarching guideline, the team assessed the adequacy and effectiveness of DoD policy and procedures related to:

- Personnel security background investigations, clearance adjudications and reinvestigations
- Suitability and fitness determinations for personnel in positions that don't require access to classified information
- Continuous evaluation of DoD personnel and contractors between investigation periods
- Information-sharing and the accuracy and completeness of investigation and adjudication verification databases
- Self-reporting, suspicious activity reporting, and incident reporting
- Access to DoD facilities
- Privately-owned weapons on DoD installations
- Vulnerability assessment capabilities to address gaps in physical security procedures

The team also examined:

- Leadership roles and responsibilities for suspension or revocation of facility access credentials, or for initiating a security clearance reinvestigation
- Impact of changes to "insider threats" on security requirements, programs and policies

- Programming, budgeting and resourcing for physical security infrastructure

The team established two working groups to assess each of the areas defined in the Terms of Reference. The results of their assessments are detailed below and include supporting recommendations to address gaps or inconsistencies in existing DoD policy, procedures, and processes. These recommendations augment the key recommendations of the Internal Review Team in section 7 and will serve to strengthen the Department's overall security posture.

Personnel Security Clearance Process

Initiating the Investigation: Standard Form 86, Questionnaire for National Security Positions

Alexis provided incomplete and inaccurate information on the Standard Form 86, "Questionnaire for National Security Positions," which was required to initiate his background investigation. In addition to failing to disclose arrests, criminal conduct, delinquent debts, and foreign travel, Alexis provided invalid information regarding employment, education, and personal references that should have been detected when his application was reviewed and approved. As an example, Alexis claimed he lived in Washington State from March 2001 – February 2007, yet he also claimed he was employed in the State of New York from January 2001 – March 2003.

OPM's published guidance to those initiating investigations advises only that the submitting offices are responsible for ensuring the completeness of forms and does not explain how to review the SF-86 information.[13]

Current DoD policy contains little guidance on the roles and responsibilities for officials initiating personnel security investigations. Policies state that those initiating officials should provide instructions and applicants should follow instructions, but do not articulate standards for either.

The Department lacks policy and specific standards to ensure the quality and completeness of the SF-86 and other standard forms. Consequently, DoD Components do not use consistent instructions for completing the SF-86 forms and give inconsistent guidance to personnel completing the forms regarding what to include and the level of detail they should provide.

13 OPM's INV 15 Handbook, "Requesting OPM Personnel Investigations," states at page 14: "The Submitting Office is responsible for ensuring completeness of the SF-85, SF-85P, SF-85PS, and SF-86. The agency must have an individual complete all information required, as OPM will not accept incomplete investigation requests."

Most personnel complete the SF-86 electronically using OPM's Electronic Questionnaires for Investigations Processing (e-QIP) system. Electronic forms offer an excellent opportunity to leverage technology to detect anomalies or inconsistencies in reported information. OPM's electronic application validation rules are not currently configured to evaluate the validity and logical consistency of information applicants provide; rather, they only reject entries based on the format of the data entered.

Recommendations:

- Improve assessments and accountability for the quality and completeness of information submitted on background investigation application forms.
- Strengthen requirements, clarify roles and responsibilities, and enhance the capability to detect falsification, invalid information, and other inaccuracies on the SF-86 and other standard forms.
- Develop and require the use of minimum standards for completeness of information in applications for national security positions, including those that do not require access to classified information. [14]
- Enforce penalties that can be imposed on subjects who falsify information on the SF-86 such as fines, imprisonment, or denial of security clearance eligibility.
- Establish a database of DoD personnel's SF-86 application data for electronic analysis to detect anomalies and to inform decisions about risk thresholds more effectively.

Availability of Records in the Report of Investigation

The OPM Report of Investigation (ROI) did not contain a copy of the incident report associated with the 2004 arrest in Seattle. Electronic queries of Federal and state-wide criminal and court record databases typically do not return arrest reports or court transcripts and thus cannot provide critical details about circumstances surrounding charges and arrests.

14 The Defense Security Service Center for Development of Security Excellence has two training products that provide guidance on completing the SF-86, but they do not specifically advise reviewers to look for discrepancies or gauge investigative usefulness. Guidance for industry facility security officers (FSOs) in NISPOM Section 2-202, "Procedures for Completing the Electronic Version of the SF 86" addresses the requirement to review the SF-86 for adequacy and completeness, but does not provide guidance on determining adequacy.

While the FBI and the Washington statewide checks disclosed the fact of Alexis' arrest and other charges, the specific details were missing. For many subjects, FBI and state-wide databases are missing criminal record information altogether that would be accessible through local agency checks. Most records of charges, arrests, dispositions, detention, and court proceedings can only be obtained through queries or site visits to individual local agencies.

Federal statute requires cooperation in background investigations for certain records providers.[15] [16] However, investigative service providers may not have adequate access to local criminal arrest records due to lack of cooperation by local authorities, or they may be overly relying on centralized electronic checks without conducting in-person leads to view or obtain actual arrest reports. These may preclude investigators and adjudicators from accurately documenting and evaluating circumstances surrounding criminal conduct, as is required by the National Adjudicative Guidelines. As a result, investigators and adjudicators are sometimes forced to rely on the subject's account of the "facts" during his or her interview to evaluate the circumstances and the extent to which issues have been mitigated.

Overall, OPM does not provide to adjudicators copies of many of the records they review in the course of investigations. For example, OPM is not required by Federal investigative standards to collect and provide copies of personnel, enlistment, and other records that are generated or obtained as part of applications for employment or military enlistment. If these documents are provided with the ROI, however, adjudicators can easily cross-reference them with SF-86 information to help identify discrepancies. Too often, investigators conducting subject interviews and adjudicators evaluating results must rely on subject self-reporting and second-hand summaries of information. An added benefit of providing adjudicators with all information used in employment applicant and military enlistment processing is they can notify human resource or military personnel when they become aware that applicants provided false or fraudulent information to gain entry.

15 Title 5, United States Code Section 9101, "Access to criminal history records for national security and other purposes," effective October 30, 2000

16 The 1985 Security Clearance Information Act requires Federal, State, and local criminal justice agencies to release criminal history record information to Federal agencies for purposes of national security clearance investigations. (Public Law 99-169, Title VIII, codified in part at 5 U.S.C. §9101).

Recommendations:

- OPM should provide copies of all records reviewed in the course of investigations to the DoD CAF, including arrest records or other documentation associated with criminal conduct. This will ensure investigators and adjudicators have the information they need to adequately detect and resolve discrepancies, enabling a more informed adjudicative process.
- OPM should report to the Department of Defense and Office of the Director of National Intelligence those agencies that do not comply with the Security Clearance Information Act by failing to provide relevant records and the reasons why. This data would inform proposed legislation to strengthen criminal history record information sharing.

Undetected Discrepancies in Self-reported Information

Upon enlisting in the Navy, Alexis received the minimum level of investigation required for military service, the National Agency Check with Local Agency Checks and Credit Check (NACLC). OPM identified Alexis' unreported delinquent debts and the 2004 arrest in Seattle but failed to detect other invalid and inconsistent information Alexis provided. Alexis' credit report provided further evidence of unlisted education, residences, and possible employment that was not identified or addressed in the investigation.

Investigators (and later adjudicators) may have missed the discrepancies in Alexis' SF-86 because NACLC investigative standards do not include employment, education, residence, and reference checks. In most instances, investigators and adjudicators are not currently required to assess whether education information provided by applicants is accurate and complete.

This should be partially mitigated once the December 2012 Federal Investigative Standards are implemented. The new standards require verifying employment and education for military enlistment and Secret-level investigations. They also articulate thresholds that require expanded investigation, including "discrepancies" in personal history information. However, the thresholds could be strengthened with additional language to specifically draw attention to logical inconsistencies between one or more pieces of information provided on standard forms and identified in the course of investigations (e.g., evidence of student loans on credit reports but no college education listed on the standard form).

Inconsistent and invalid applicant data often remain undetected partly because standard form data and reports of investigation are not provided in organized, sortable formats that allow adjudicators to detect anomalies quickly. The Department adjudicates more than half a million Secret-level clearance and military enlistment investigations and a quarter-million Top Secret-level investigations each year. This volume, coupled with an emphasis on meeting IRTPA timelines, does not allow adjudicators time to restructure the data manually and conduct a detailed review of every application and investigation.[17]

Some discrepancies won't be detected because many investigations are incomplete. Overall, at least 31 percent of the investigations forwarded to the DoD CAF are incomplete, although incomplete cases are not necessarily deficient. For example, OPM may forward an incomplete investigation where the investigator has exhausted all reasonable avenues to satisfy a lead requirement. In such cases, adjudicators have the latitude to accept some incomplete investigations. In some cases, adjudicative facilities have found ways to work with or supplement incomplete investigative products. In response to the April 2009 Government Accountability Office audit of the DoD personnel security clearance process, the Under Secretary of Defense for Intelligence published guidance in March 2010 clarifying how adjudicators should handle such incomplete investigations.

Recommendations:

- OPM should establish and enforce higher standards for the completeness of subject interviews, in part by ensuring that investigators have all documentation to formulate relevant and effective questions, and address all occurrences of omission, falsification, inconsistencies, or any other concealment of information or issues.
- OPM and DoD should accelerate and expand efforts to reformat SF-86 data and reports of investigation to support more automated, efficient, consistent, and reliable detection of potential security concerns.
- Adjudicator training should reinforce their ability and responsibility to request additional information to resolve issues as needed so they can make an informed adjudicative determination. Accelerate efforts to use publicly-available electronic information as an investigative source for initial eligibility determinations, reinvestigations, and continuous evaluation.[18]
- Expand and fund the use of polygraphs for issue resolution to obtain information from subjects that would otherwise not be known through other sources.

17 The Review Team spent about 2 hours manually reorganizing and analyzing Alexis' case file. The team identified numerous inconsistencies missed by both investigators and adjudicators. However, given the size of the Secret-level population alone and the current number of adjudicators (460 at the DoD CAF), detailed analysis of every case is impossible. Each adjudicator has about 20 minutes to process a case.

Security Clearance Adjudication

DONCAF adjudicators identified potentially disqualifying conditions for Alexis' security clearance eligibility but found them to be mitigated in accordance with existing adjudicative guidelines. DONCAF did find the issues to be of enough concern to issue a warning letter to Alexis via his commanding officer specifying certain conditions Alexis was required to meet to retain his clearance eligibility. There is no evidence to suggest the commanding officer followed up on this requirement or ensured Alexis took the appropriate steps to meet the conditions.[19]

The current 13 National Adjudicative Guidelines contain a general guideline called "Personal Conduct." This guideline is a "catch-all" of sorts and contains a wide range of issues and behaviors that are not specifically covered elsewhere in the Guidelines. It is rarely used by itself to initiate an unfavorable adjudication, but rather is used in conjunction with issues covered under other guidelines. Consequently, the Guidelines may not sufficiently articulate the importance of subjects' honesty in applications and interviews.

Recommendations:

- Require DoD CAF oversight of conditional clearance eligibility determinations. DoD CAF should create a mechanism to track and monitor all conditional clearances and waivers to adjudicative standards,

18 Preliminary results from the Army G2/ODNI's Assessment of Emerging Technologies for use in Continuous Evaluation Phase 2 show that social media checks identify evidence about illegal drug and alcohol use, arrests, images and text that may suggest an underlying psychological condition to include thoughts of despair or hopelessness, a desire to die by suicide, and more. In Alexis' case, a check of publicly available information on the internet may have surfaced mug shots from his Texas 2010 firearm-related arrest.

19 The warning letter required that Alexis maintain financial solvency and ensure any future personnel security questionnaires are complete and accurate prior to submission.

and take action to revoke or deny eligibility for non-compliance after a specified period (no more than 12 months).

- Clearances granted with warnings should be monitored through continuous evaluation to ensure the issues do not recur.[20]
- Consider revising the National Adjudicative Guidelines to list an applicant's deliberate omission or falsification of reportable information on the SF-86 as a behavior that will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility.
- Revise adjudicator training to support decisions of denial/revocation in instances of intentional misrepresentation or omission of facts on forms or during interviews.

Incident Reporting and Continuous Evaluation

After DONCAF's favorable Secret eligibility determination in 2008, neither the Navy nor Alexis' cleared employer reported any adverse information about Alexis' conduct in JPAS. During Alexis' Navy career, there were two arrests and one instance of non-judicial punishment that should have been reported. Alexis' command at the time did not consider reporting his misconduct in any security system of record, because Alexis did not need to access classified information in the course of his regular duties.

During the final weeks of his employment with The Experts, Alexis displayed behavior and made statements that indicated psychological problems of security concern. Following an August 4 incident at the Norfolk airport and subsequent incidents August 6-7 in Newport, Rhode Island, The Experts was sufficiently concerned to remove Alexis from access in JPAS and send him home to rest. Based on the information available to The Experts at the time (which included none of Alexis' misconduct prior to and during his employment in the Navy), The Experts determined he was fit to return to work, restoring his access in JPAS on August 9. At the time, The Experts also considered whether reporting this incident in JPAS was appropriate and believed it was not reportable because the incident did not involve criminal activity, nor had Alexis been referred to a medical facility for psychiatric evaluation.

20 A condition denotes action on the part of the subject. A warning usually directs the subject not to do something. At a minimum, clearances with conditions should receive oversight to ensure that the conditions are met. Subjects of warnings could be monitored through continuous evaluation record checks, once available.

The above indicates that DoD and industry personnel do not have a consistent understanding of incident reporting and security oversight requirements and procedures, particularly for individuals who are eligible but not actually granted access. To illustrate the scope of this issue, there are more than 2.5 million personnel with current access to classified information, and another 2.1 million personnel who are eligible but not currently in access. Many security personnel believe that continuous evaluation and periodic reinvestigation requirements don't apply to personnel who are simply "eligible" for access. Consequently, they may not report issues potentially affecting an individual's eligibility.

In hindsight, members of the review team and those contacted in the course of the review agreed that Alexis displayed behavior and made statements that indicated psychological problems of security concern. However, neither training that pertains to National Adjudicative Guideline I (Emotional, mental, and personality disorders) nor Question 21 on the SF-86 provides any specificity or guidance regarding those psychological conditions that are associated with the greatest risk that an individual may pose a security or safety concern. Greater specificity about clinical conditions of greatest security concern might:

- reduce ambiguity on what individuals must self-report;
- appropriately reduce the number of individuals required to report mental health counseling, by eliminating low-risk psychological conditions (thereby reducing stigma and investigation costs);
- clarify this area of reporting requirements for co-workers, supervisors, human resources and security personnel, and;
- clarify when psychological assessments should be ordered and how the results should be used.

The value of greater specificity, however, must be weighed against the potential vulnerability created by focusing too much on a narrow set of risks. Additionally, many people with psychological conditions lack the insight into the fact that they are ill; and very often, clinicians disagree about diagnoses.

The Department does not have a single, consolidated repository of security incident information. JPAS is the official system of record for reporting issues of personnel security concern; however, the DOD CAF receives incident reports using methods other than just JPAS. The Intelligence Community relies on its own system for issue reporting. It is also likely that there are component-specific records containing adverse information that could bear on an individual's continuing eligibility for access to classified information.

The process for identifying and acting on security incidents and behaviors of a national security concern relies heavily on individuals, co-workers, managers, supervisors, and commanders to report information to their security managers or FSOs. An enterprise-wide continuous evaluation capability would help mitigate gaps in information obtained through self-reporting and would complement a threat management capability. The Department has existing capability to conduct continuous evaluation checks between regularly scheduled investigations and is developing a robust continuous evaluation system that would enable real-time automatic notifications of issues of security concern.

Recommendations:

- Implement and invest in an enterprise-level continuous evaluation system to augment and enable audits of reporting by individuals, co-workers, supervisors, and security professionals. An effective continuous evaluation program may increase the number of self-reports, as personnel may decide to report rather than have their behavior discovered. It may also serve as a deterrent to unacceptable behavior if there is a greater risk of being caught.
- Update policy and issue specific DoD-wide procedures for reporting security incidents and behaviors of security concern so that all personnel, regardless of their roles and responsibilities and location in the organization, know what to report, how to report, and to whom.[21] Clarify that reporting requirements apply to all clearance-eligible individuals as well as non-cleared individuals with unsupervised access to DoD installations and facilities.
- Implement and enforce policy that holds security managers and supervisors accountable for failures to file incident reports on events that meet clearly defined reporting thresholds.
- Require annual certification by supervisors, commanders, security managers, and other personnel that they understand, have complied with, and will continue to comply with incident reporting policy.[22]

21 Policy on security incident and reportable behavior reporting are dispersed across security disciplines. For example, policy is contained in personnel security issuances like DoD 5200.2-R, industrial security issuances like DoD 5220.22-M, National Industrial Security Program Manual (NISPOM), Defense Security Service Industrial Security Letters, and information security issuances like DoDI 5200.01.

22 For example, a recent PERSEREC report (TR 13-02) provides background information and a concept of operations for a simple procedure called the Personal Acknowledgment of Staff Security (PASS). The purpose of the proposed procedure is to increase supervisor awareness, felt responsibility, accountability, and reporting of behaviors related to foreign intelligence entity threats in accordance with DoD Directive 5240.06, Counterintelligence Awareness and Reporting (CIAR), May 17, 2011. The defining feature of PASS is the requirement of a signed certification by supervisors that they understand and intend to comply with reporting policy.

- Evaluate, update, and standardize security education and training on identifying reportable behaviors and events, how they should be reported, and to whom. Establish recurring training requirements to ensure that all personnel — including supervisors, commanders, and security managers — are continuously reminded and demonstrate knowledge of their responsibility to report incidents of security concern.
- Update Question 21 on the SF-86 to specify standardized clinical conditions associated with heightened security, safety, and reliability risk.

Suitability and Fitness Determinations for Personnel who do not Require Access to Classified Information

Investigations for suitability evaluations (and contractor fitness) are comparable to investigations for security clearances and will be further aligned with implementation of the Revised Federal Investigative Standards. Under the current investigative standards, all suitability investigations require employment, education, residence, and reference checks or inquiries, whereas security investigations for military and contractor Secret-level clearances do not.

Historically, adjudications for investigations of personnel in positions that do not require access to classified information have been decentralized and of unknown consistency. Effective October 1, 2013, the DoD CAF became responsible for favorable suitability adjudications of DoD and contractor personnel in positions that do not require access to classified information. Under current policy, adverse suitability[23] adjudications are retained by the individual DoD Components. The community is divided on whether the DoD CAF should also adjudicate applicants under HSPD-12 for Common Access Cards (CACs). Some in the community feel that risk management for installation and information access can only be done effectively at the Component level. Others believe that the decentralization of potentially adverse suitability determinations reduces oversight and consistent standards for adjudicating what is likely the highest risk group of personnel based on issues identified in their background investigations.

Overall, the Review Team found insufficient oversight of suitability determinations. DoD Components either do not consistently report all adjudication actions for suitability determinations into OPM's Clearance

23 The term "suitability" is used to refer to HSPD-12 eligibility, suitability for employment in the competitive and senior executive service, fitness for employment in the excepted service, and fitness for employment as a contract employee.

Verification System (CVS), or OPM does not enter all adjudication actions received into CVS. Additionally, as of October 2013, the Department had nearly 185,000 active personnel in JPAS with eligibility reported as "No Determination Made."[24] For these latter cases, it is not known whether anyone ever reviewed the results of the investigations or whether the adjudicators simply did not have a JPAS code available to indicate a favorable suitability determination (separate from eligibility for access to classified information). Regardless, incomplete adjudications and missing adjudicative data undermine effective oversight, reciprocity, and accountability.

Recommendations:

- Expand consolidation of adjudications for DoD background investigations to include all HSPD-12 determinations in addition to security clearance determinations, and direct the required resources to the DoD CAF.[25]
- Improve accountability for, and remove barriers to, reporting of suitability adjudications and HSPD-12 determinations.

Investigation and Adjudication Verification Databases

Data pertaining to Alexis' initial investigation and adjudication status were recorded in JPAS. As discussed, however, JPAS did not contain incident reports pertaining to criminal arrests, military non-judicial punishments, and aberrant behavior that would have warranted incident reports.

Additionally, although Alexis' enlistment, separation, and employment data were entered correctly in JPAS, the Internal Review Team learned that DoD security managers do not reliably update data with respect to the status of their current

24 Alexis' initial adjudication of his background investigation was reported as "No Determination Made." In his case, however, the Navy requested his investigation be adjudicated for eligibility for access to classified information.

25 As of October 1, 2013, the DoD CAF assumed responsibility for favorable adjudications for suitability, public trust, and HSPD-12 determinations. In FY 2014, these are projected to total approximately 160,000 cases. DoD CAF leadership estimates that favorable adjudications can be made for approximately 90% of cases, which would mean that about 16,000 adjudications on the highest risk cases will be made by security personnel in the field. Effectively, this means that the DoD is assigning the adjudications of its highest risk subjects to the personnel who have the least amount of experience and training to adjudicate background investigations. Additionally, most of these field personnel will be doing adjudications in very small quantities, which contributes to lack of consistency in rendering credentialing determinations.

or departing personnel. One reason is that the Department does not have policy addressing roles, responsibilities, and standards for security managers to ensure the upkeep of data in JPAS. However, the Defense Manpower Data Center has developed numerous data quality initiatives to identify incomplete and inconsistent information in JPAS and either administratively remove associated personnel from access to classified information or administratively separate them from the Department.[26] Additionally, in August 2013, the Office of the Under Secretary of Defense for Intelligence directed DoD Components to validate that personnel identified as having overdue reinvestigations in JPAS still require them. The Department is issuing a memorandum reminding security managers, supervisors, and commanders of their responsibilities to ensure that JPAS accurately reflects the status of their personnel and whether they have engaged in behaviors of security concern.

Recommendations:

- Establish, reinforce, and enforce roles and responsibilities for updates to JPAS/Joint Verification System by security managers within specific time frames to ensure completeness, accuracy, and accessibility of information about current employment status and access to classified information.
- Revise DoD policy to define procedures for adverse information reporting and clarify the kinds of behaviors that indicate issues of security concern and must be reported.

Process for Determining Whether Security Clearances are Required

The number of clearances issued and deficiencies in the process for identifying positions and responsibilities that require security clearances were not direct factors in the Navy Yard incident. Alexis was subject to the minimum background investigation for military service, which is also the minimum background investigation for access to classified information. A few months after enlisting, he was assigned to Navy training that required eligibility for access to classified information, which led to a request for a re-adjudication of his investigation based on national security standards (i.e., the National Adjudicative Guidelines). He was not indoctrinated for access, however, until he was hired by

26 For more information on DMDC's Data Quality Initiative to administratively debrief persons with active access who do not meet business rules and policy requirements for that level of access, see: https://www.dmdc.osd.mil/psawebdocs/docRequest//filePathNm=PSA/appId=560/app_key_id=1559jsow24d/siteId=7/ediPnId=0/userId=public/fileNm=DQI+597+Slides.pdf

a cleared industry employer. In his industry position, he was assigned to support a classified contract and required a Secret security clearance in the performance of his duties.

Indirectly, one could argue that the sheer volume of security clearance eligibility and access determinations processed by the Department has the consequence of reducing the amount of time that investigators and adjudicators can spend on cases to ensure that reports of investigation are complete and all issues are adequately identified and resolved. Regardless of whether this was pertinent or indirectly affected Alexis' investigation and adjudication, the workload challenge will not be eliminated by reducing the number of security clearances because of the pending impacts of the alignment of suitability and security investigations and reinvestigations required by Executive Order 13467 and the 2012 Revised Federal Investigative Standards. The net effect of the new standards will be to increase the Department's investigative and adjudicative workload, regardless of the number of security clearances. For example, all military and contractor personnel who currently require NACLC investigations will instead require an investigation that is more similar to the ANACI required for civilian employees, which includes employment and education checks not required for NACLC investigations.

Recommendation:

- At least annually, require DoD Component and agency heads to validate and certify the need for all personnel security clearances under their cognizance.

Adequacy and Effectiveness of DoD Personnel Security Clearance and Background Reinvestigation Policies

When the 2012 Revised Federal Investigative Standards are implemented in the Department, reinvestigations for personnel will be required for all national security positions (regardless of classification level) every 5 years. Security managers may continue to apply differing reinvestigation requirements for individuals with eligibility for access but who are not indoctrinated for access unless the Department makes a concerted effort to clarify expectations. If reinvestigation requirements remain subject to interpretation, the Department will remain vulnerable to a policy gap that contributed to Alexis gaining access to classified information without having been subjected to security requirements and oversight for several years.

When Alexis was honorably released from active duty in the Navy and transitioned to the Individual Ready Reserve, he retained his active eligibility for access to classified information as recorded in JPAS. When he found employment as a DoD contractor 20 months later, his employer complied with current DoD policy that allowed him to be indoctrinated for access to classified information based on the Navy's eligibility determination and without any reinvestigation. In practical terms, Alexis was indoctrinated for access to classified information by The Experts after nearly 5 years without being subjected to security oversight. This gap in existing policy, moreover, could allow someone like him to be indoctrinated without any reinvestigation based on an existing Secret-level eligibility after 10 years without security oversight.

Numerous policy-related findings and recommendations have been presented in the previous sections of this review. The policy-making process itself, however, presents very difficult challenges to the DoD's ability to keep policies up-to-date and responsive to emerging needs. DoD Personnel Security Program policies generally take years to go through both DoD and OMB coordination processes. The current formal policy issuance process for DoD Personnel Security Program instruction and procedures as well as Common Access Credential investigation and adjudication instructions and procedures is too long and undermines the ability of the Department to provide timely direction and guidance to components.

Recommendations:

- Establish requirements for eligible personnel and transitioning personnel to more frequently update standard forms that are required for their type of eligibility. For example, the Department could revise policy to require individuals who have a break in access of 12 consecutive months or more to complete the SF-86C, Standard Form 86 Certification, to ensure SF-86 information is current and correct.
- Convene a follow-up working group to determine how to mitigate risk regarding individuals who have a break in access and extended periods with no security oversight and recommend the appropriate duration for restoration of access.
- Develop strategies for streamlining the DoD issuance process where possible to ensure policies keep pace with changes in national policies and the Department's needs (e.g., restoring USD(I)'s ability to issue interim direction and policy to DoD Components via a policy memorandum).

Installation Access Control Process

Access to DoD Facilities and Identity Vetting

The Naval Criminal Investigative Service (NCIS) and FBI published in their findings that Alexis arrived at the Washington Navy Yard on the morning of September 16 having legitimate access as a DoD contractor employee and that he used his valid building pass to gain entry to Building 197. However, the Review Team found some DoD components are not compliant with implementing policy requirements for identity proofing, vetting, and authentication of visitors seeking unescorted access to DoD installations. Implementation, execution, and oversight of DoD policies and procedures related to physical security and antiterrorism is inconsistent. Leadership awareness of policy requirements and implementation challenges is critically important in setting the tone for a strong overall security posture.

Although DoD processes and procedures related to access to facilities by cleared personnel appear to be adequate, the review revealed that some DoD Components are not in compliance with DoD policy on visitor access control. DoD Instruction 2000.16, "DoD Antiterrorism (AT) Standards," requires DoD Components in Force Protection Condition Bravo to verify the identity of visitors seeking access to DoD installations and randomly inspect their suitcases, parcels, and other containers. Likewise, Directive-type Memorandum (DTM) 09-012, "Interim Policy Guidance for DoD Physical Access Control," directs non-federal government and non-DoD-issued card holders who are provided unescorted access to DoD installations to be identity proofed and vetted to determine fitness and eligibility for access. DTM 09-012 also requires personnel to be vetted against government authoritative data sources, including the National Crime Information Center (NCIC) and Terrorist Screening Database (TSDB).

Not all visitors are being vetted before gaining unescorted access to DoD installations. In some cases, visitors can show a driver's license to gain access to DoD installations without being vetted. In other cases, local vendors may be given a base pass without being vetted against the NCIC or TSDB. As resources allow, the Military Departments actively pursue compliance with installation access control, but fiscal pressures prevent installations from having NCIC capability at their visitor centers. Some DoD installations have purchased commercial access control vetting systems (such as MOBILISA) that do not check against U.S. Government authoritative data sources (NCIC and TSDB). These systems do not meet the intent of DTM 09-012, as they use only a public records check and are not interoperable, nor do they support a DoD-wide access

control capability. A recently issued DoD Inspector General report[27] noted a key finding that numerous contractor employees were enrolled in a commercial access control system and received interim installation access and a local access credential without having their claimed identities vetted through mandatory databases such as NCIC and TSDB. This occurred in attempts to reduce access costs. OMB memorandum 05-24 directs that government employees and contractor personnel requiring routine physical access to an installation for more than 6 months must receive a personal identity verification credential, such as a DoD CAC, and successfully complete a National Agency Check with Written Inquiries (or higher) investigation.

Although it appears physical security policies at the Washington Navy Yard were aligned and nested with Department of the Navy and DoD policies, there were some shortcomings in the implementation and execution of these policies. The review revealed that random antiterrorism measures (RAM) and vehicle inspections were not being conducted regularly as required under DoDI 2000.16, "DoD Antiterrorism (AT) Standards." Installation antiterrorism plans and local vulnerability assessments were not completed in accordance with DoD antiterrorism policy. Further, visitors were not properly vetted in accordance with DoD physical security policy. We do not believe these concerns are isolated to the Navy Yard. Common observations from Joint Staff Integrated Vulnerability Assessments (JSIVAs) identified:

- Deficiencies in commercial delivery inspection processes, employment of RAM and final denial barriers; and
- Insufficient explosive detection equipment, working dogs, and communications equipment.

Implementation and enforcement of physical security and antiterrorism procedures and policies require senior leadership emphasis and oversight.

Recommendations:

- Ensure all visitors entering DoD installations are properly vetted against U.S. Government authoritative data sources (NCIC and TSDB).
- Maintain current physical security standards of physical and visual inspection of identification credentials for access control.

27 DoD Inspector General Report #DODIG-2013-134, "Navy Commercial Access Control System Did Not Effectively Mitigate Access Control Risks," September 16, 2013

- Issue policy prohibiting use of commercial access control vetting systems that do not check against U.S. Government authoritative data sources and support a DoD-wide and federally interoperable access control capability.
- Ensure Military Department and installation compliance with DoD AT and physical security policies, and examine Military Department oversight of these policies.

Not all DoD installations are using authoritative databases to vet visitors to determine fitness to enter DoD installations as specified in DTM 09-012. While most DoD installations have access to law enforcement databases like the NCIC for law enforcement and investigative purposes, not all installations have access to NCIC for the purpose of vetting for access control. DTM 09-012 mandates that unescorted visitors entering DoD installations be queried against government authoritative data sources to vet the claimed identity to determine fitness: "Installation government representatives shall query the following government authoritative data sources to vet the claimed identity and to determine fitness, using biographical information including, but not limited to, the person's name, date of birth, and social security number: NCIC, TSDB, other sources as determined by DoD component, local commander or director."

Not all installations are compliant; this is primarily a funding and personnel staffing issue. Vetting visitors against NCIC requires a trained security clerk to send individual queries to NCIC, which is a manual and labor intensive process; it also requires investment in equipment, infrastructure, and licenses to access the databases. Although workarounds exist, such as conducting NCIC checks by phone, they are not practical for installations with large visitor populations. As a result, some installations are not vetting visitors against required law enforcement databases.

Currently, Military Department-level law enforcement databases are not interoperable. Because of this, an individual barred from an Army installation can gain access to an Air Force or Navy installation. The Fort Hood Follow-on Review recommended establishing a consolidated law enforcement database to enable organizations across the Department to query, retrieve, and post criminal investigation and law enforcement data into a single repository. The report recommended acceleration of efforts to automate access control that would authenticate various identification media (e.g., passports, CAC, drivers' licenses, license plates) against authoritative databases. DoD has implemented the Law Enforcement Defense Data Exchange (LE D-DEx), an automated information

management system designed to share criminal justice information between DoD LE agencies for LE and investigative purposes. However, LE D-DEx is not currently integrated with physical access control systems.

The DIAC Working Group, under the auspices of the DoD Physical Security Equipment Action Group, is establishing IMESA to provide the capability to vet individuals seeking access to a DoD installation against DoD, Federal, state, and local authoritative data sources. This architecture will provide the capability for fitness determination of non-Federal Government and non-DoD issued card holders and visitors requesting unescorted access to DoD installations using biographical name checks. Secure information will enable installations' physical access control systems (PACS) to authenticate individuals' credentials, authorization, and fitness to enter, vastly enhancing the security of DoD personnel and resources worldwide.

Recommendations:

- Establish an efficient process or system for DoD Components to gain access to law enforcement and other authoritative databases to vet personnel for access control.
- Accelerate implementation of IMESA. Explore integrating LE D-DEx with physical access control systems via IMESA.

Suspicious Activity Reporting

DoD Instruction 2000.26, "Suspicious Activity Reporting," is the capstone DoD policy governing how the Department reports suspicious activities. Although the Department is not mandated by Federal law or other statutes to use eGuardian, DoDI 2000.26 requires DoD components with law enforcement agencies or activities to use eGuardian exclusively for reporting, storing, and sharing unclassified suspicious activity reports dealing with information regarding a potential threat or suspicious activity related to DoD personnel, facilities, or forces in transit.

Although the DoD Components and the Washington Navy Yard are compliant with suspicious activity reporting policy and have established procedures for eGuardian, they need to ensure the law enforcement community is aware of the means and methods for reporting suspicious activities through eGuardian.

In addition, law enforcement and eGuardian users must report suspicious behaviors, activities, and other reportable information and ensure this information populates within eGuardian so it can be seen and accessed.

Recommendations:

- Develop and implement suspicious activity reporting awareness campaigns for all DoD Components. Ensure all personnel (military, civilian, contractor, vendor, and visitors) on DoD installations know how to report suspicious activities.
- Ensure suspicious activities as reported through other "tip" systems, such as Eagle Eyes, are recorded in eGuardian.
- Monitor and track eGuardian reporting through the DoD eGuardian Working Group.
- Emphasize the sharing of all suspicious activities and other LE reporting through the local threat working group and other LE channels.

Privately-owned Weapons on DoD Installations

Although DoD policy regarding privately owned weapons is adequate, enforcement and verification is difficult. It is impractical to search every vehicle entering an installation for illegal weapons. Additionally, without conducting exhaustive searches of facilities and residences, it is impossible to verify illegal weapons have not been smuggled onto DoD installations. Commanders must balance security with access and privacy concerns.

Title 18 U.S.C., Section 930, prohibits any individual from knowingly possessing or presenting a firearm or dangerous weapon in a Federal facility. The December 3, 2010, Secretary of Defense message on privately owned firearms (POF) directed all DoD components to require mandatory registration of POF for all personnel who store POF on an installation (whether or not they live on the installation). U.S. Navy policy for POF aligns with this DoD policy, requiring any weapon brought onto a Navy installation to be registered with base security forces.

Recommendations:

- Installation commanders develop strategies to check vehicles and personnel entering DoD installations and facilities for POF.
- Conduct a follow-on review to examine installation security and law enforcement resource requirements to implement an adequate personnel, property, and vehicle inspection program.
- Ensure notices of provisions are posted conspicuously at each DoD installation in public entrance in accordance with subsections (a) and (b) of Title 18, United States Code, Section 930 (Possession of firearms and dangerous weapons in Federal facilities).

DoD Vulnerability Assessment Capabilities to Identify and Mitigate Physical Security Gaps

Vulnerability assessments are critical to commanders' ability to identify vulnerabilities and mitigate risk. DoDI 2000.16, Standard 6, directs heads of DoD components to conduct and update terrorism vulnerability assessments at least annually or more frequently if the terrorist threat assessment or mission requirements dictate. Vulnerability assessments are conducted, at a minimum, for any facility populated daily by 300 or more DoD personnel, any DoD facility bearing responsibility for emergency response or physical security plans and programs, or determined to host critical infrastructure.

JSIVAs evaluate an installation's ability to deter and/or respond to a terrorist incident. The Defense Threat Reduction Agency (DTRA) conducts between 80-100 JSIVAs per year. Due to fiscal concerns, the Military Departments have reduced their vulnerability assessment teams and have become more reliant upon JSIVAs. However, beginning in FY 2015, DTRA will reduce the number of JSIVAs it conducts by approximately 70 percent to about 30 per year, placing greater pressure on the Military Departments to conduct higher headquarters vulnerability assessments. Given the constrained fiscal environment, it is unlikely the Military Departments will be able to make up the difference and some installations may go without a higher headquarters vulnerability assessment. Although the vulnerabilities identified in the JSIVA and CNO integrated vulnerability assessment of the Washington Navy Yard had no direct bearing on the specific events of September 16, 2013, the identified shortcomings in the implementation and execution of DoD physical security policies introduces risk and could be a factor in the future.

Recommendation:

- Fund the JSIVA program in FY 2015 and beyond until the Department transitions to a broader Mission Assurance Assessment Capability in order to in order to retain the Chairman's critical independent vulnerability assessment capability.

Programming, Budgeting and Resourcing for Physical Security Infrastructure

Due to current budget constraints, DoD Components are encountering significant challenges with procuring technological capabilities that support physical security infrastructure. DoD programming, budgeting, and resourcing for physical security encounters significant challenges with competing requirements.

Although programming, budgeting, and resourcing of physical security infrastructure had no direct impact on the WNY shooting incident, further reductions in physical security funding could put installations at risk for preventing and responding to future active shooter incidents. Not all installations are compliant with physical security requirements due to budget constraints that impact the Military Departments' ability to procure equipment, integrate law enforcement and physical security databases, and manpower.

EQUIPMENT. DTM 09-12 directs "When funding becomes available, installations will procure an electronic Physical Access Control System (PACS) that provides capability to rapidly and electronically authenticate credentials and individuals authorized to enter an installation." Not all of the Military Departments have physical access control systems and the current capability is not interoperable for access control. Not all installations have NCIC at their visitor centers. Some installations have purchased commercial access control vetting systems that do not check against U.S. Government authoritative data sources (NCIC and TSDB); thus, they fail to meet the intent of DTM 09-12. Although the Military Departments implement "work-arounds" with telephonic NCIC background checks to offset a lack of technological equipment, this process is not operationally conducive for rapid identity vetting to determine fitness of personnel entering installations at the access control point.

INTEGRATION OF LAW ENFORCEMENT AND PHYSICAL SECURITY DATABASES. The Department implemented the Law Enforcement Defense Data Exchange (LE D-DEx), an automated information management system designed to share criminal justice information between DoD law enforcement agencies. LE D-DEx is not currently integrated with existing law enforcement databases and physical access control systems.

MANPOWER. Beginning in FY15, the Defense Threat Reduction Agency and the Military Departments will reduce the number of JSIVAs from 80 or more per year to about 30. Reduction of JSIVAs will limit commanders' ability to identify vulnerabilities and mitigate risk.

ASSESSMENTS. Observations from JSIVAs identified deficiencies in commercial delivery inspection process; RAM; final denial barriers; explosive detection equipment and dogs; and communication deficiencies. These are reoccurring deficiencies that can be rectified with additional manpower and funding. DoD Components need to procure PACS that are HSPD-12 compliant and possess capabilities now that share law enforcement information from integrated databases to rapidly vet and screen personnel entering our installations. Physical security programming, budgeting, and resourcing varies within the Military Departments. Each Service prioritizes and budgets for physical security and AT programs differently. In this austere budget environment, competing requirements are difficult for physical security and antiterrorism programs to overcome.

GOVERNANCE. Also, at the Department level, there is no single Principal Staff Assistant in OSD with oversight of law enforcement, physical security, and antiterrorism, inhibiting the Department from directing and integrating policy, assessing compliance and recommending resource priorities. Governance of these programs and their execution is diffused within the Department, and security programs sometimes do not receive appropriate priority at the strategic level.

Recommendations:

- DoD Components must continue to conduct risk-based programming to support physical security and antiterrorism capabilities and JSIVA programs during austere budget environments.

- Conduct a follow-on review to examine physical security programming, budgeting, and resourcing. DoD should review how physical security, antiterrorism, and law enforcement activities are governed within the Department to improve synergy. Currently, these functions are decentralized in the Department.
- Highlight security programs in the Defense Planning Guidance and other strategic prioritization documents.

Impact of Changes in Information Technology on Security Programs

The Department has limited capability to electronically vet and identify personnel entering its installations.

Section 1069 of the Fiscal Year 2008 National Defense Authorization Act for Fiscal Year 2008 states: "(1) Access Standards for Visitors: Secretary of Defense shall develop access standards applicable to all military installations in the United States ... to include to determine the fitness and verifying the identity. Secretary of Defense is encouraged to procure and field existing identification screening technology and to develop additional technology only to the extent necessary to assist commanders of military installations in implementing the standards developed under this section at points of entry for such installations."

DTM 09-12 directs, "When funding becomes available, installations will procure an electronic physical access control systems that provides the capability to rapidly and electronically authenticate credentials and individuals authorized to enter an installation. The PACS must support a DoD-wide and federally interoperable access control capability."

Current DoD physical access control systems are governed and implemented under Military Department-unique guidance and are not interoperable among military installations. No enterprise capability exists for linking DoD installations using electronic authentication of credentials. Funding of physical access control systems is inconsistent across the Military Departments.

The DIAC Working Group is developing IMESA to serve as the overarching architecture. This architecture consists of: 1) Interoperability Layer Service (IoLS) that will allow DoD Components' physical access control systems to share information with one another; and 2) Continuous Information Management Engine capability, which continuously updates information in the authoritative databases. IMESA will not only tie the DoD Components together, but benefit them by:

- Providing real-time continuous identity vetting with periodic updates/ alerts;
- Enabling installations to identify "bad actors;"
- Providing minimal impact on how Military Department physical access control systems are further developed and maintained;
- Providing Military Departments' physical access control systems near real-time access to authoritative source data; and
- Including additional capabilities, as the architecture evolves, leveraged from linkages to a biometric component.

The DIAC Joint Capability Technology Demonstration is currently on hold pending approval of an exception to DoDD 5200.27, which prohibits storing of information on non-DoD affiliated personnel. DoDD 5200.27 specifies all information on non-DoD affiliated personnel that the Department is not otherwise authorized by law or by direction of the Secretary of Defense to retain must be destroyed within 90 days.

Recommendations:

- Continue Defense Manpower Data Center's development of IMESA and IoLS to enable DoD components to share access control information and vet individuals continuously against U.S. Government authoritative databases before allowing access to DoD installations.
- Approve exemption to DoDD 5200.27 to collect and store NCIC and TSDB information on non-DoD personnel.
- Fund procurement of electronic physical access control systems that provide the capability to rapidly and electronically authenticate credentials and individuals authorized to enter an installation.

DEPARTMENT OF DEFENSE

Internal Review of the Washington Navy Yard Shooting

A Report to the Secretary of Defense

Appendices

Appendix A. Internal Review Team Composition, Contributing Organizations, and Terms of Reference

A-1. Internal Review Team Composition

The Internal Review Team membership was derived primarily from an existing DoD team of subject matter experts focused on threats from trusted insiders: the DoD Insider Threat Working Group, which was established under the auspices of the Under Secretary of Defense for Intelligence in August 2013. The team organized into two primary areas of focus: personnel security clearance and installation access control processes. Using those principal areas as points of departure for the review, the team received briefings and conducted interviews with subject matter experts and senior officials across the Department. The team included representatives from the following original and augmenting organizations:

The Joint Staff
Department of the Army
Department of the Navy
Department of the Air Force
U.S. Cyber Command
U.S. Northern Command
Office of the Under Secretary of Defense (Acquisition, Technology and Logistics)
Office of the Under Secretary of Defense for Intelligence
Office of the Under Secretary of Defense for Personnel and Readiness
Office of the Under Secretary of Defense for Policy
Office of the Assistant Secretary of Defense for Health Affairs
Office of the General Counsel of the Department of Defense
DoD Chief Information Officer
Director, Administration and Management
Defense Intelligence Agency
Defense Security Service
Defense Privacy and Civil Liberties Office

A-2. Briefings and Supporting Organizations

The Internal Review Team received briefings from stakeholder organizations across the Department and conducted extensive interviews with subject matter experts. The following organizations contributed to the review:

Subject	Organization
Continuous Evaluation Concept Demonstration	Department of the Army
Fort Hood Update	Office of the Under Secretary of Defense for Policy
Overview of Security Executive Agent Roles and Responsibilities; Status of Continuous Evaluation Initiative	Office of the Director of National Intelligence
DoD Adjudications	DoD Consolidated Adjudications Facility
National Industrial Security Program	Defense Security Service
Security Vulnerability Assessment Overview	Defense Security Service
Insider Threat Prediction and Prevention; MOSAIC Threat Assessment Systems	Gavin de Becker & Associates
DoD Privacy and Civil Liberties Programs	Defense Privacy and Civil Liberties Office
Navy Threat Management Unit	Naval Criminal Investigative Service
HSPD-12: DoD Common Access Card (CAC) and Other Emerging Physical Security Activities	Defense Manpower Data Center
Overview of the Washington Navy Yard Criminal Investigation	Federal Bureau of Investigation
Naval Criminal Investigative Service	
Overview of Secretary of the Navy Rapid Reviews	Department of the Navy
Overview of the Health Insurance Portability and Accountability Act (HIPAA)	Office of the Assistant Secretary of Defense for Health Affairs
Joint Lessons Learned Program	Joint Staff
Office of the Assistant Secretary of Defense for Homeland Defense & Americas' Security Affairs	

A-3. Terms of Reference

Department of Defense Review of the Washington Navy Yard Shooting

These Terms of Reference (TOR) set forth the objectives for the Secretary of Defense-directed internal and independent reviews (hereafter referred to as "the Reviews") to examine the security programs, policies, processes, and procedures related to the shooting at the Washington Navy Yard on September 16,2013. The purpose of the Reviews is to identify and address vulnerabilities or weaknesses that may have alerted the Department of Defense (DoD) to the potential threat before the incident occurred. The Reviews will be conducted on a separate but paraJlel track, with a consolidated list of recommendations provided to the Secretary of Defense.

Finally, the Department of Navy (DoN) is conducting its own review of security at Navy and Marine Corps installations, as well as other security, contractor, and personnel issues stemming from this tragedy. The DeN's findings will be incorporated into the final report to the Secretary of Defense.

BACKGROUND

On September 16, 2013, Aaron Alexis, a Navy contractor, shot and killed 12 U.S. Navy civilian and contractor employees and wounded several others at the Washington Navy Yard. The shooter was also killed. The Federal Bureau of Investigation is leading a criminal investigation into the incident. The Reviews should in no way interfere with that investigation or suggest culpability for the events of September 16, 2013.

OBJECTIVES AND SCOPE

The Reviews are to determine whether there are DoD program, policy, or procedural weaknesses in the security procedures for access to DoD installations worldwide (outside areas ofhostilities) or related to the security clearance and reinvestigation process for DoD personnel and contractors. The Reviews will examine the Washington Navy Yard shooting to identify issues that may present Department-wide vulnerabilities.

The Reviews will:

- Assess the adequacy and effectiveness of DoD policies related to personnel security clearances and background reinvestigations;

- Assess the adequacy and effectiveness of DoD processes and procedures related to access to DoD facilities by cleared personnel;
- Evaluate information-sharing processes and procedures among federal, state, and local law enforcement agencies regarding security clearance and background reinvestigations;
- Assess the accuracy and completeness of DoD investigation and adjudication verification databases;
- Evaluate DoD procedures for initiating and using background investigations for personnel security clearances, suitability determinations, and Homeland Security Presidential Directive-12 compliance, including:
  - Depth, quality, and thoroughness of investigations conducted by the Office of Personnel Management for DoD;
  - Access to relevant information, including law enforcement databases, financial data, and health and personnel records; and
  - Continuous evaluation ofDoD personnel and contractors between investigation periods;
- Assess DoD implementation and effectiveness of suitability evaluations and determinations · for those DoD and contractor personnel in positions that do not require access to classified information;
- Assess the process by which DoD determines whether security clearances are required for military, civilian, and contractor personnel;
- Review DoD self-reporting, suspicious activity reporting, and security incident reporting programs and procedures;
- Review DoD policy and procedures regarding privately-owned weapons on DoD installations;
- Review current and planned DoD vulnerability assessment capabilities used to identify and mitigate gaps in physical security procedures and resources;
- Assess the adequacy and effectiveness of programming, budgeting, and resourcing for physical security infrastructure;
- Analyze changes in information technology that may facilitate improved security programs or pose emerging challenges;

- Evaluate the roles and responsibilities of military and civilian leadership for suspension or revocation of facility access credentials, or for initiating a security clearance reinvestigation; and
- Examine whether and how changes in "insider threats" to DoD installations may alter security requirements or necessitate changes in security programs, policies, processes and procedures.

METHODOLOGY

- The Reviews should consider find ings and recommendations from previous relevant reports and studies.
- The Reviews will examine all applicable laws, policies, and regulations, including DoD directives, instructions, and manuals.
- The Reviews may include interviews with appropriate senior officials (health affairs, law enforcement and force protection, first responders, intelligence), and other pe11inent individuals.
- The Reviews will formulate recommendations for correcting problems and enhancing internal controls to prevent similar incidents in the future and mitigate associated risk.

PROCESS

- The Under Secretary of Defense for Intelligence (USD(I)) will lead the internal review, in coordination with senior representatives from each of the Military Departments, the Joint Staff, and the Office of the Secretary of Defense.
- Dr. Paul Stockton (former Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs) and Admiral Eric Olson, USN (Ret), will lead the Independent Review.
- The Deputy Secretary of Defense will oversee the internal review as well as the consolidation and drafting of the final report.
- The Secretary of Defense has given the Independent Review the authority to submit their findings directly to him, should it deem such a step necessary.

TIMELINE AND DELIVERABLES:

The Reviews will begin on September 30, 2013. A final report with key findings and recommendations from the internal and independent reviews will be provided separately to the Secretary and Deputy Secretary ofDefense by November 15,201 3. Under supervision ofthe Deputy Secretary of Defense, a consolidated report synthesizing the findings and recommendations of both reviews will be provided to the Secretary of Defense by December 20, 2013, unless the Independent Review exercises the aforementioned authority to submit their findings directly to the Secretary of Defense. Implementation plans will be developed at the direction of the Secretary of Defense.

SUPPORT:

- The Under Secretary of Defense (Comptroller)/Chief Financial Officer will ensure adequate funding is provided for the Reviews.
- The Director of Administration & Management, through Washington Headquarters Services, will coordinate with other DoD Components on behalf of the Reviews and provide human resources, office facilities, and other support, as required, to ensure the success of theseefforts.
- The Reviews will be able to draw upon the full support of the Military Departments and other DoD Components for support, personnel, information (including, but not limited to, documents and personnel to be interviewed), and analytical and investigative capacity as determined necessary by the USD(I) and the Co-chairs of the independent review.

Appendix B. Seattle Police Department Incident Report

SEATTLE POLICE DEPARTMENT — INCIDENT REPORT

☒ INCIDENT ☐ INCIDENT AND ARREST ☐ ARREST ONLY — INCIDENT NUMBER: 04-181918

☐ DO NOT DISCLOSE ☒ NOT DISCUSSED ☐ DISCLOSE

THE PERSON MAKING THIS REPORT HEREBY DECLARES THE FACTS HEREIN ARE TRUE AND CORRECT, AND UNDERSTANDS THAT BY FILING A FALSE REPORT, THEY MAY BE SUBJECT TO CRIMINAL PROSECUTION. X

☐ HAZARD TO OFFICER ☐ DOMESTIC VIOLENCE ☐ BIAS CRIME

INCIDENT CLASSIFICATION	TOOL/WEAPON USED	METHOD OF TOOL/WEAPON USE
Weapon	gun	shoot tires
Property Damage		

LOCATION: [redacted] | FIRM NAME: | CENSUS: 104 | BEAT: R3

TYPE OF PREMISE(FOR VEHICLES STATE TYPE AND WHERE PARKED): 1986 Honda Accord WA plate [redacted] (see below) | POINT OF ENTRY:

DATE/TIME REPORTED	DAY OF WEEK	DATE(S) / TIME(S) OCCURRED	DAY(S) OF WEEK
05/06/04 @ 1004	Thursday	05/06/04 @ 0800	Thursday

☐ PROPERTY STOLEN / RECOVERED (PROPERTY FORM 5.37.1 MUST BE ATTACHED) ☐ NOTHING TAKEN ☐ UNKNOWN AT TIME OF REPORT ☐ VICTIM FOLLOW-UP LEFT

☒ EVIDENCE SUBMITTED ☐ FINGERPRINT SEARCH MADE ☐ FINGERPRINTS FOUND ☐ LAB EXAM REQUESTED

INJURED - 1 HAS USABLE TESTIMONY - 2 DO NOT DISCLOSE - 3

CODE C (PERSON REPORTING, COMPLAINANT) V (VICTIM) W (WITNESS)

PERSON/BUSINESS INVOLVED	CODE	NAME (LAST, FIRST, MIDDLE)	RACE/SEX/D.O.B.(OPTIONAL)	HOME PHONE	HOURS	
	CV	[redacted]	HM [redacted]/80	[redacted]	any	1 ☐ 2 ☐ 3 ☐
	ADDRESS	ZIP CODE	OCCUPATION(OPTIONAL)	WORK PHONE	HOURS	
	[redacted]	[redacted]	[redacted]	[redacted]	eves	
	CODE	NAME (LAST, FIRST, MIDDLE)	RACE/SEX/D.O.B.(OPTIONAL)	HOME PHONE	HOURS	
	W	[redacted]	AM [redacted]/63	[redacted]	vary	1 ☐ 2 ☐ 3 ☐
	ADDRESS	ZIP CODE	OCCUPATION(OPTIONAL)	WORK PHONE	HOURS	
	[redacted]	[redacted]	[redacted]			

SUSPECT(S)	NAME (LAST, FIRST, MIDDLE)	RACE/SEX/D.O.B	HEIGHT	WEIGHT	HAIR	EYES	SKIN TONE	BUILD
	ALEXIS, Aaron	BM 05/[redacted]/79	6-02	175	BLK			Thin
	ADDRESS	HOME PHONE	WORK PHONE	WORK HOURS	OCCUPATION	EMPLOYER/SCHOOL		
	[redacted]							

CLOTHING, SCARS, MARKS, TATTOOS, PECULIARITIES, A.K.A.: Black jacket, white shirt, blue pants, clean shaven

ITS ENTERED-CAN-RVW

RELATIONSHIP TO VICTIM: NONE

BA/CIT. NO. | CHARGE DETAILS (INCLUDE ORDINANCE OR R.C.W. NUMBER AND LARGEST PENALTY): At Large | ☐ BOOKED ☐ YSC ☐ CITED ☐ KCJ

1. ADDITIONAL PERSONS - CODE, NAME, RACE, SEX, D.O.B., ADDRESS, INJURY, HOSPITALIZATION, HOME AND WORK PHONES, HOURS, AND IF DISCLOSURE OF NAME IS PERMITTED.
2. ADDITIONAL SUSPECTS - DETAIL INFORMATION IN SAME ORDER AS SUSPECT BLOCK.
3. VICTIM'S INJURIES - DETAILS AND WHERE MEDICAL EXAM OCCURRED.
4. PROPERTY DAMAGED - DESCRIBE AND INDICATE AMOUNT OF LOSS.
5. PHYSICAL EVIDENCE - DETAIL WHAT AND WHERE FOUND, BY WHOM, AND DISPOSITION.
6. VEHICLE USED BY SUSPECT AND DISPOSITION.
7. NAME, ADDRESS, PHONE NUMBER OF JUVENILE'S PARENT(S)/GUARDIAN(S). NOTE IF CONTACTED AND IF INCIDENT ADJUSTED.
8. LIST STATEMENTS TAKEN AND DISPOSITION.
9. RECONSTRUCT INCIDENT AND DESCRIBE INVESTIGATION.
10. OUTLINE TESTIMONY OF PERSONS MARKED "HAS USABLE TESTIMONY" ON FRONT.

ITEM # 1

The above listed car belongs to [redacted]. Suspect shot the rear tires causing them to flatten, rendering the tires unusable. The wheels that held the tires appeared to be damaged. Total damage was estimated to be at least $800.00.

TM1 - I placed one roll of 35mm film into evidence.
TM2 – I placed three .45 caliber shell casings, which I found at the scene, into evidence.

On the above date and time, [redacted] and [redacted], both construction workers, were building a house at [redacted]. [redacted]ar (see above) was parked in the driveway of the work site. It was legally parked on the worksite's property. [redacted] saw the black male suspect, wearing the above listed clothing and matching the description, standing behind his car. [redacted] saw the suspect remove what appeared to be a gun from his waistband, chamber a round and shoot [redacted]cars rear left tire. The suspect then walked to the right side of

I HEREBY CERTIFY (DECLARE) UNDER PENALTY OF PERJURY UNDER THE LAWS OF THE STATE OF WASHINGTON THAT THIS REPORT IS TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE AND BELIEF (RCW 9A.72.085)

PRIMARY OFFICER'S SIGNATURE	SERIAL #	UNIT #	DATE SIGNED	PLACE SIGNED
	6663	652	05-06-04	SEATTLE, WA

PRIMARY OFFICER'S PRINTED NAME	SECONDARY OFFICER	SERIAL	UNIT	APPROVING OFFICER / SERIAL
T. MANSOUR				[redacted]276

Incident Number: 04-181918

DISTRIBUTION: PRECINCT (S) ☒ CRIMES AGAINST PERSONS ☐N ☐S ☐C JUV ☒ COURT UNIT ☐ K-9 UNIT PAGE 1 OF 2
Form 5.37A CS 21.924 Rev. 9/01 ☐E ☐W ☒S ☐N CRIMES/ PROPERTY ☐ VICE/NARC ☒CRIME ANALYSIS ☒OTHER H/R UNIT

SEATTLE POLICE DEPARTMENT

CONTINUATION SHEET

INCIDENT NUMBER: 04-181918
UNIT FILE NUMBER:

ITEM OR ENTRY | ☒ INCIDENT ☐ INCIDENT AND ARREST ☐ ARREST ONLY | ☐ FOLLOW-UP ☐ TRAFFIC / COLLISION ☐ SUPERFORM | ☐ OTHER: (specify)

PAGE 2 OF 2

[redacted]'s car and shot the rear right tire. The suspect returned to the left side of the car and shot one round into the air. [redacted] who was working on the second floor of the house, had a clear and unobstructed view of the shooting. The suspect "walked slowly" northbound and into the blue house [redacted] stated he could not see the gun's color or make.

Ofc. B. Hanson and I tried to contact the suspect at [redacted] No one answered the door. I did not see any movement within the house. I ran a records check of the house and found the suspects name. A continuing records check (CCW) found suspect to have a Glock .45 caliber [redacted] registered to him. The physicals from the records check and suspect's New York DMV record match the description given to me by [redacted]

I gave [redacted] a business card.

At the time of report, officers were unable to contact suspect for identification purposes.

INVESTIGATING OFFICER	SERIAL	UNIT	INVESTIGATING OFFICER	SERIAL	UNIT	APPROVING OFFICER	SERIAL
T. MANSOUR	6663	652					5336

Form 5.7.2 CSS 21.866 Rev. 8/01

SEATTLE POLICE DEPARTMENT

FOLLOW-UP REPORT

INCIDENT NUMBER: 04-181918
UNIT FILE NUMBER: B/TS 04-179

TYPE OF INCIDENT	DATE OF INCIDENT	PRESENT DATE
Property Damage	5/6/2004	5/7/2004

ORIGINALLY REPORTED AS: Same
LOCATION OF INCIDENT: [redacted]
VICTIM: [redacted] ADDRESS: [redacted] PHONE: [redacted]

CASE DISPOSITION: CLEARED (ARREST-UNFOUNDED-REFERRAL JUVENILE COURT,-EXCEPTIONAL CLEARANCE); AT LARGE WARRANT; ETC.
Referred to Seattle Municipal Court

PROPERTY: RECOVERED ☐ ADDITIONAL STOLEN ☐ FURTHER DESCRIPTION ☐ (INDICATE ID MARKS,—COLORS—SIZES—SERIAL NUMBERS—DISPOSITION—VALUE, ETC. AS FIRST ENTRY BELOW)

ENTRY — COMMENCE EACH ENTRY WITH A NUMBER AND THE DATE AND TIME
SUSPECTS: INCLUDE NAMES, B/A NUMBERS, DESCRIPTIONS, DISPOSITION, CAN VICTIM IDENTIFY, ETC
GENERAL: SUMMARIZE STEPS OF INVESTIGATION; INCLUDE PERSONS INTERVIEWED, ADDITIONAL WITNESSES, RESULTS OF INTERROGATIONS, EVIDENCE, BUSINESS ADDRESSES AND PHONES, ETC.
CASE M.O.: INDICATE ADDTIONAL M.O. FACTORS NOT INCLUDED ON OFFENSE REPORT

PROCESSED BY [redacted]

D/C

Index as Verified Suspect:

ITS/FNT/MOD/CLR/RVW
ID 070904 0259 1084

Alexis, Aaron
B/M DOB/05/[redacted]79
6'2" 175 lbs. Bld head, Brn eyes
LKA [redacted]
CCN: 1808233
PCN: 213369083
B/A : 204022684

Charge:

Referred to
Seattle Municipal Court
Property Destruction
SMC 12A.08.020

&

Discharge of a Firearm
SMC 12A.14.071

I CERTIFY (DECLARE) UNDER PENALTY OF PERJURY UNDER THE LAWS OF THE STATE OF WASHINGTON THAT THIS REPORT IS TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE AND BELIEF (RCW 9A.72.085)

PRIMARY OFFICER'S SIGNATURE	SERIAL #	UNIT #	DATE SIGNED	PLACE SIGNED
[redacted]	5670	658	5/15/04	SEATTLE, WA

PRIMARY OFFICER'S PRINTED NAME	SECONDARY OFFICER	SERIAL	UNIT	APPROVING OFFICER	SERIAL
Detective R. Bourns				[redacted]	3367

DISTRIBUTION: RECORDS DETECTIVES PRECINCT ( ) COURT UNIT ID JUVENILE OTHER:

Form 5.8.2 CS 21.865 Rev 5/03

SEATTLE POLICE DEPARTMENT

CONTINUATION SHEET

INCIDENT NUMBER 04-181918
UNIT FILE NUMBER B/TS 04-179

ITEM OR ENTRY | INCIDENT / INCIDENT AND ARREST ARREST ONLY | FOLLOW-UP / TRAFFIC / COLLISION SUPPEROFM | OTHER: (specify)

1 05-07-04 1300 Case assigned by Sgt. Mike Nelson for follow-up. ***CASE SUMMARY***: On May 6th, 2004 at 0800 hours, **Aaron Alexis** exited his home located at [redacted] 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 worke[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**.

Officer T. Mansour responded to investigate the complaint and subsequently collected three spent .45 caliber casings from the ground near the victim's 1986 Honda Accord. He attempted to make contact with **Alexis** but no one answered the door at his residence. Mansour researched the RMS database for the residence and located a DOL record that documented a Concealed Pistol License and a registered .45 caliber Glock associated with **Aaron Alexis**.

On June 3rd, 2004 Detective S. Berg and I arrested **Alexis** outside of his residence. His grandmother and owner of the residence granted us written consent to search his bedroom where the Glock pistol and ammunition were recovered. During post-Miranda questioning **Alexis** confessed to the crime of discharging his weapon for the purpose of shooting out the tires on the car owned b[redacted]. **Alexis** also stated that he perceived the victim had mocked him earlier that morning after he discovered his own vehicle had been tampered with. The suspect was booked into the King Co. jail and his weapon and ammunition was entered as evidence. [redacted] later reported it cost him $200 to repair his vehicle.

2 05-20-04 1420 I conducted an RMS database search and located a phone number [redacted] associated with the suspect address. I called the number and left a message for **Aaron Alexis** to call me. I did not indicate the reason I needed to speak to him.

3 05-20-04 1430 I printed a copy of Alexis' CPL and gun registration.

4 05-20-04 1435 P/C t[redacted] He used his girlfriend [redacted] as an interpreter. He explained that the black male suspect stared at the construction workers every morning for about 30 days prior to the shooting. He displayed his gun when he walked to his car but the suspect never spoke [redacted] his workers. He provided the phone number to his employe[redacted] 46). [redacted] told me that it could cost him about $500 to replace his tires and wheels but was not sure if he wanted to prosecute the suspect. However he did want to be repaid for damages. He said he would call me back with his decision to prosecute.

5 05-21-04 0935 I contacted [redacted]. He told me that he believed the suspect was angered over the parking problem outside the construction site. He added that neither he nor his crew had seen the suspect for at least one-week.

6 05-25-04 1415 Second P/C to **Aaron Alexis**. I left another message for him to call me back.

INVESTIGATING OFFICER	SERIAL	UNIT	INVESTIGATING OFFICER	SERIAL	UNIT	APPROVING OFFICER	SERIAL
Detective R. Bourns	5670	658				[redacted]	3365

Form 5.7.2 CS 21.866 Rev. 4/97

SEATTLE POLICE DEPARTMENT

CONTINUATION SHEET

INCIDENT NUMBER 04-181918
UNIT FILE NUMBER B/TS 04-179

ITEM OR ENTRY | INCIDENT / INCIDENT AND ARREST ARREST ONLY | FOLLOW-UP / TRAFFIC / COLLISION SUPPEROFM | OTHER: (specify)

7 05-26-04 0900 P/C to SPD Identification Section. I requested that they research **Alexis'** application for CPL then learned that the suspect provided only a New York D/L for photo ID. I questioned as to why there was an associated WA State ID number attached to the CPL record. I was informed that DOL often adds WA State ID to the record if it is not initially available to them. It should be noted that the WA ID listed on the record was not valid.

8 06-01-04 0900 Detective Berg and I responded to [redacted] to attempt contact with Alexis. He was not home but I spoke with his grandmother [redacted] who is the homeowner [redacted] (who is his cousin) [redacted] was aware that her grandson owned a handgun and kept it in the house but Weeks was not aware of it. Neither of them knew about the shooting that occurred on May 6th. Both confirmed that **Aaron Alexis** was the only male that lived in the house and that there had been no known male guests. Mrs. Alexis stated that **Aaron** did not pay her rent and that he did not have an exclusive access to his bedroom. She gave us a written consent to search **Aaron's** room for the weapon. The search proved negative [redacted] said that her cousin drove a black Mitsubishi Eclipse and believed he worked in Kirkland for a company known [redacted]

9 06-01-04 1130 Detective Berg and I arrived in Kirkland at the offices o[redacted] We discovered that the offices had moved to Bellevue. We then responded to their new location but did not spot the suspect's black Mitsubishi in the parking lot. I then called the company's Human Resources Dept. who indicated that **Alexis** was not listed on their employee roster.

10 06-03-04 0630 Detective Berg and I arrived in the area of Alexis' residence. We maintained surveillance on his vehicle for about twenty minutes.

11 06-03-04 0650 We arrested **Alexis** just as he climbed into his vehicle. I advised him of his rights and he stated he understood. He stated that his gun was in his bedroom but would not tell us exactly where. I then contacted Dorothy Alexis, and once again she agreed to sign a consent to search. Detective Berg eventually located the Glock 30 handgun wrapped in a paper sack.

12 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.

13 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.

14 06-11-04 1200 P/C to victim [redacted] but his cell phone had been disconnected.

15 06-11-04 1205 [redacted]. He told me that he too was trying to reach [redacted] for work and experienced the disconnected phone number. He indicated he would find another method of contacting [redacted] then have him call me.

INVESTIGATING OFFICER	SERIAL	UNIT	INVESTIGATING OFFICER	SERIAL	UNIT	APPROVING OFFICER	SERIAL
Detective R. Bourns	5670	658				[redacted]	3365

Form 5.7.2 CS 21.866 Rev. 4/97

SEATTLE POLICE DEPARTMENT

CONTINUATION SHEET

INCIDENT NUMBER: 04-181918
UNIT FILE NUMBER: B/TS 04-179

ITEM OR ENTRY | INCIDENT | INCIDENT AND ARREST | ARREST ONLY | FOLLOW-UP | TRAFFIC / COLLISION | SUPERFORM | OTHER: (specify)

PAGE 4 OF 4

16 06-14-04 1045 P/C to [redacted] again. He stated that [redacted] was present at a job site and would allow him to speak with me at about 1055 hours.

17 06-14-04 1058 I called [redacted] then obtained his statement with the aid of the Qwest Spanish Interpreter [redacted] agreed to cooperate with the prosecution then told me that he spent $200 cash to repair the damages to his vehicle. He obtained the tires from an acquaintance then repaired the holes in the wheels by himself. He believed that **Alexis** should be responsible to repay him the amount he spent for repairs.

18 06-15-04 1100 Case prepared then referred to the Seattle Municipal Court for charges of Property Damage (over $50) as well as Discharge of a firearm.

INVESTIGATING OFFICER	SERIAL	UNIT	INVESTIGATING OFFICER	SERIAL	UNIT	APPROVING OFFICER	SERIAL
Detective R. Bourns	5670	658				[redacted]	3345

Form 5.7.2 CS 21.868 Rev. 4/97

Appendix C. References

Personnel Security

U.S. LAW, NATIONAL POLICY AND FEDERAL REGULATIONS

Part 732 of title 5, Code of Federal Regulations

Public Law 108-458, "Intelligence Reform and Terrorism Prevention Act of 2004," December 17, 2004

Executive Order 10450, "Security Requirements for Government Employment," April 27, 1953, as amended

Executive Order 10865, "Safeguarding Classified Information within Industry," February 20, 1960, as amended

Executive Order 12829, "National Industrial Security Program," January 6, 1993, as amended

Executive Order 12968, "Access to Classified Information," August 2, 1995, as amended

Executive Order 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information," June 30, 2008

Executive Order 13488, "Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust," January 16, 2009

White House Memorandum, "Adjudicative Guidelines," December 29, 2005

White House Memorandum, "Implementation of Executive Order 12968," March 24, 1997

Executive Order 13526, "Classified National Security Information," December 29, 2009

U.S. Office of Personnel Management Booklet, "Requesting OPM Personnel Investigations," December, 2010 (also known as "INV 15")

U.S. Office of Personnel Management Federal Investigations Notice 97-02, "Executive Order 12968 and Investigative Standards for Background Investigations for Access to Classified Information," July 29, 1997

Office of Management and Budget Memorandum, "Reciprocal Recognition of Existing Personnel Security Clearances," December 12, 2005

Office of Management and Budget Memorandum M-06-21, "Reciprocal Recognition of Existing Personnel Security Clearances," July 17, 2006

Office of Management and Budget Memorandum, "Reciprocal Recognition of Existing Personnel Security Clearances," November 14, 2007

Director of National Intelligence and U.S. Office of Personnel Management Memorandum, "Approval of the Federal Investigative Standards," December 13, 2009

INTELLIGENCE COMMUNITY POLICY

Office of the Director of National Intelligence and the U.S. Office of Personnel Management, "Approval of the Federal Investigative Standards," December 13, 2008

Intelligence Community Directive 704, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information," October 2, 2008

Intelligence Community Policy Guidance 704.2, "Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information," October 2, 2008

Intelligence Community Policy Guidance 704.3, "Denial or Revocation of Access to Sensitive Compartmented Information, Other Controlled Access Program Information, and Appeals Processes," October 2, 2008

Director of National Intelligence Memorandum, "Delegation of Authority for the Director of Administration and Management to Determine Sensitive Compartmented Information Eligibility at the Department of Defense Consolidated Central Adjudication Facility," October 22, 2012

Director of National Intelligence Memorandum, "Clarification of Conflicting Personnel Security Investigative Standards," E/S 00388, July 29, 2011

DEPARTMENT OF DEFENSE POLICY

DoD Directive O-5240.02, "Counterintelligence," December 20, 2007, as amended

DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," November 23, 2005

DoD Directive 5200.02, "DoD Personnel Security Program," April 9, 1999

DoD Directive 5220.6, "Defense Industrial Personnel Security Clearance Review Program," January 2, 1992

DoD Instruction 3305.13, "DoD Security Training," December 18, 2007

DoD Directive 5145.01, "General Counsel of the Department of Defense," May 2, 2001

DoD 5200.2-R, "Personnel Security Program," January 1987

DoD 5220.22-R, "Industrial Security Regulation," December 4, 1985

DoD 5220.22-M, National Industrial Security Program Operating Manual, February 28, 2006

DoD 5400.11-R, "DoD Privacy Program," May 14, 2007

DoD Instruction 5210.91, "Polygraph and Credibility Assessment (PCA) Procedures," August 12, 2010

DoD Directive 5210.48, "Polygraph and Credibility Assessment Program," January 25, 2007

DoD Directive 5105.42, "Defense Security Service (DSS)," August 3, 2010

DoD Instruction 5145.03, "Oversight of the DoD Personnel Security Programs," January 10, 2013

DoD Directive 5240.06, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011, as amended

DoD Instruction 5220.22, "National Industrial Security Program (NISP)," March 13, 2011

DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998

DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007

DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012

DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended

DoD Manual 3305.13, "DoD Security Accreditation and Certification," March 14, 2011

Secretary of Defense Memorandum, "Final Recommendations of the Defense Science Board Report on Predicting Violent Behavior," March 26, 2013

Office of the Assistant Secretary of Defense, C3I Memorandum, "Clearance and Access Reciprocity in the Department of Defense," July 16, 1998

Office of the Assistant Secretary of Defense, C3I Memorandum, "Personnel Security Investigations and Adjudications," November 10, 1998

Assistant Secretary of Defense, C3I Memorandum, "Personnel Security Clearance Investigations," August 22, 2000

Assistant Secretary of Defense, C3I Memorandum, "Transfer of Additional Personnel Security Investigation Workload to the Office of Personnel Management (OPM)," April 30, 2001

Deputy Under Secretary of Defense (Counterintelligence and Security) Memorandum, "Personnel Security Issues," January 8, 2004

Office of the Under Secretary of Defense for Intelligence letter to U.S. Office of Personnel Management, re: Presidential approval of Single-Scope Background Investigation – Periodic Reinvestigation, known as the Phased PR, February 22, 2005

Office of the Under Secretary of Defense for Intelligence Memorandum, "Facilitating Classified Visits within the Department of Defense," April 01, 2005

Under Secretary of Defense for Intelligence Memorandum, "Implementation of Adjudicative Guidelines for Determining Eligibility For Access to Classified Information (December 29, 2005)", August 30, 2006

Deputy Secretary of Defense Memorandum, "Defense Security Service (DSS) Future Options Study Recommendations," January 15, 2009

Under Secretary of Defense for Intelligence Memorandum, "Designation of the DoD Case Management and Adjudication Systems," April 10, 2009

Office of the Secretary of Defense Memorandum, "Department of Defense (DoD) Implementation and Transition to the Office of Personnel Management (OPM) Electronic Questionnaires for Investigations Processing (e-QIP)," May 18, 2009

Under Secretary of Defense for Intelligence Memorandum, "Personnel Security Clearance Adjudication Documentation," November 8, 2009

Under Secretary of Defense for Intelligence Memorandum, "DoD Personnel Security Adjudicator Certification Program," July 1, 2010

Under Secretary of Defense for Intelligence Memorandum, "Implementation of the Rapid Assessment of Incomplete Security Evaluations (RAISE)," July 13, 2010

Under Secretary of Defense for Intelligence Memorandum, "DoD Transition to Electronic Fingerprint Capture and Submission in Support of Background Investigations," July 29, 2010

Under Secretary of Defense for Intelligence Memorandum, "Review of the Adjudication Documentation, Accuracy and Rationales (RADAR) Assessments," August 31, 2010

Deputy Secretary of Defense Memorandum, "DoD Central Adjudications Facilities (CAF) Consolidation," October 20, 2010

Office of the Under Secretary of Defense for Intelligence Memorandum, "Approval of the Defense Security Service Industry Implementation Plan in Support of the DoD Transition to Electronic Fingerprint Capture," April 12, 2011

Deputy Secretary of Defense Memorandum, "DoD Central Adjudications Facilities (CAF) Consolidation, May 3, 2012

Office of the Under Secretary of Defense for Intelligence Memorandum, "Transition to Electronic Fingerprint Capture and Submission in Support of Background Investigations," June 7, 2012

Secretary of Defense Memorandum, "Department of Defense Guidance on Question 21, Standard Form 86, Questionnaire for National Security Positions," September 4, 2012

Deputy Secretary of Defense Memorandum, "Appointment of the DoD Senior Official Charged with Overseeing Insider Threat Efforts," September 25, 2013

Note: Memoranda without a corresponding hyperlink are available from the Security Policy and Oversight Directorate, Office of the Deputy Under Secretary of Defense (Intelligence & Security)

OTHER

Memorandum of Agreement among Defense Security Service, Defense Human Resources Activity's Defense Manpower Data Center, Deputy Under Secretary of Defense (HUMINT, Counterintelligence and Security) and Deputy Under Secretary of Defense (Program Integration), February 2, 2010

Memorandum of Understanding between U.S. Office of Personnel Management, Federal Investigative Services and DoD Office of the Under Secretary of Defense for Intelligence for the Expansion of Electronic Delivery (eDelivery), June 21, 2010

Physical Security and Installation Access

U.S. LAW, NATIONAL POLICY AND FEDERAL REGULATIONS

10 U.S.C. Subtitle C, "Authority, Law Enforcement, Security of Naval Installations, Security of DoD Installations."

Title 18, U.S.C. Section 930, "Possession of firearms and dangerous weapons in Federal facilities"

PRESIDENTIAL DOCUMENTS

Presidential Memorandum, "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs. (limited public link)

Homeland Security Presidential Directive 12, "Policies for a Common Identification Standard for Federal Employees and Contractors"

DEPARTMENT OF DEFENSE POLICY

DTM 09-012, "Interim Policy Guidance for DoD Physical Access Control," with chg 3, March 19, 2013

DTM 13-005, "Deviations from the DoD Physical Security Program," April 25, 2013

Deputy Secretary of Defense Memorandum, "Antiterrorism Building Standards for Leased Space," December 7, 2012

DoDI 2000.12, "DoD Antiterrorism Program," September 9, 2013

DoDI 2000.16, "DOD Antiterrorism Standards," December 8, 2006

DoDI 2000.26, "Suspicious Activity Reporting," November 1, 2011

DoD 5200.08-R, " Physical Security Program," April 2007

DoDI 5200.08, "Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)," December I 0, 2005

DoDD 3000.3, "Policy for Non-Lethal Weapons," July 9, 1996

FIPS 201, "Federal Information Processing Standards Publication Personal Identity Verification of Federal Employees and Contractors," June 23, 2006

Unified Facilities Criteria 4-010-01, "DoD Minimum Antiterrorism Standards for Buildings," February 9, 2012

DEPARTMENT OF HOMELAND SECURITY POLICY

DHS Interagency Security Committee (ISC) Standard, "Facility Security Level Determinations for Federal Facilities," 2008 (FOUO – requires an HSIN account for access)

DHS ISC Standard, "Items Prohibited from Federal Facilities," February 2013

DHS ISC, "Use of Physical Security Performance Measures," 2009

DHS ISC Standard, "Physical Security Criteria for Federal Facilities," April 7, 2010 (FOUO – requires an HSIN account for access)

DEPARTMENT OF THE NAVY POLICY

SECNAV M-5510.30, "DoN Personnel Security Program," June 2006

SECNAV M-5510.36, "DoN Information Security Program," June 2006

SECNAVINST 5510.37, "DoN Insider Threat Program," August 8, 2013

SECNAV Directed Installation Security Posture Assessment, September 17, 20 13

CNO Antiterrorism Strategic Guidance, September 2010

OPNAVINST 3400.12, "Navy Required Operational Capability Levels for Navy Installations and Activities," October 6, 2008

OPNAVINST 3300.53C, "Navy Antiterrorism Program," May 26, 2009 (FOUO – on SIPRNET)

OPNAVINST 5530.14E, "Navy Physical Security and Law Enforcement Program," January 28,2009

OPNAVINST 3591.1F, "Small Arms Training and Qualification," August 12, 2009

Navy-wide OPTASK Antiterrorism, March 18, 2013

U.S. Fleet Forces, Antiterrorism Operations Order 3300-13, January 2013

U.S. Pacific Fleet Operations Order 201, September 2007

U.S Naval Forces Southern Command, Operations Order 4000-07, October 2007

U.S. Naval Forces Europe, Operations Order 4000-05, April 2006

U.S. Naval Forces Central Command, Operations Order 09-1, December 2009

DEPARTMENT OF THE ARMY POLICY

Army pamphlet, "Tips for Commanders on Suspicious Activity Reporting"

Army Regulation 600-20, "Army Command Policy," September 20, 2012

Army Regulation 525-13, "Antiterrorism," September 11, 2008 (FOUO – requires AKO account for access)

All Army Activities (ALARACT) message 145/11, EXORD 171-11, "Law Enforcement Suspicious Activity Reporting (eGuardian)," 131536Z April, 2011

All CID message, 015-10, "Implementation of the eGuardian Reporting System," October 26, 2010

HQ, US Army Installation Management Command, OPORD 12-116, "Requirement to Establish and Report eGuardian Accounts," (DTG not available)

CHAIRMAN OF THE JOINT CHIEFS OF STAFF POLICY

CJCS EXORD for Standup of USNORTHCOM AT-FP Responsibility, 011710Z May 2004

GEOGRAPHIC COMBATANT COMMAND POLICY

USNORTHCOM Antiterrorism Instruction 10-222

USNORTHCOM Force Protection Directive (Information Reporting Requirements) 11-100, 102100Z April, 2011

USNORTHCOM Force Protection Level messages, 242245Z May 2012

USNORTHCOM Force Protection Directive 11-356 (NCI 10-222 interim revision 3), 221745Z December 2011

USNORTHCOM Force Protection Directive 12-241 (NCI 10-222 interim revision 4), 292215Z August 2012

USNORTHCOM FP Advisory 13-231, 291935 August 2013

USEUCOM Antiterrorism Operations Order 11-05

USCENTCOM Antiterrorism Operations Order 05-02

USPACOM Antiterrorism/CIP Operations Order 5050-08

USSOUTHCOM SC Regulation 380.16

USAFRICOM AT-CIP Operations Order 10-06

OTHER

Memorandum of Understanding between The Federal Bureau of Investigation, Criminal Justice Information Services Division and the United States Department of Defense, December 5, 2012

Appendix D. Bibliography

Ainslie, F.M., Helton-Fauth, W.B., Chandler, C.J. (2012). Department of Defense/Director of National Intelligence automated continuing evaluation system (ACES)—pilot evaluation.

Working paper 12-02. Monterey, CA: Defense Personnel Security Research Center. FOUO.

Ainslie, F.M., Neal, M.M., & Buck, K.R. Comparison of government and commercial criminal history record sources. Unpublished manuscript. Monterey, CA: Defense Personnel Security Research Center

Buck, K.R. & Neal, M.M. (2008). Military accession and security clearance screening impact on early and adverse separation. Tech. rep. 08-09. Monterey, CA: Defense Personnel Security Research Center

Buck, K.R. & Rose, A.E. (2005). Crime self-reporting study: Phase I. Tech. rep. 05-1. Monterey, CA: Defense Personnel Security Research Center

Buck, K.R. (2005). Comparative productivity of criminal record checks by federal investigations and contractors. Tech rep. 05-3. Monterey, CA: Defense Personnel Security Research Center

Buck, K.R., Rose, A.E., Wiskoff, M.F., & Liverpool, K.M. (2005). Screening for potential terrorists in the enlisted military accessions process. Tech. rep. 05-07. Monterey, CA: Defense Personnel Security Research Center. FOUO.

Chandler, C.J. (2013, July 24). Automated record check pilot status update: Briefing to DADSIWG. Unpublished manuscript. Monterey, CA: Defense Personnel Security Research Center

Chandler, C.J. (2013, October). ACES checks on Aaron Alexis. Unpublished manuscript. Monterey, CA: Defense Personnel Security Research Center. FOUO

Defense Personnel Security Research Center & Office of the Director of National Intelligence—Special Security Directorate (ODNI-SSD). (2012: August 15). Security clearance reciprocity within the Department of Defense: Evaluation of reciprocity practices. Unpublished manuscript. Monterey, CA: Author. FOUO

Defense Personnel Security Research Center. (2010). PERSEREC crosswalk of adjudicative guidelines, HSPD-12 credentialing, and suitability. Monterey, CA: Author

Executive Order 13488, Granting reciprocity on excepted service and federal contractor employee fitness and reinvestigating individuals in positions of public trust, January 16, 2009

Godes, O. & Lang, E.L. (2009). Identifying personality disorders that are security risks: Phase I results. Tech rep. 09-01. Monterey, CA: Defense Personnel Security Research Center. FOUO

Helton-Fauth, W.B. (2013). Evaluating health information technology for use in accession screening. DRAFT. Unpublished manuscript. Monterey, CA: Defense Personnel Security Research Center

Helton-Fauth, W.B. Analysis of decision thresholds articulated in Defense Office of Hearings and appeals (DOHA) Statements of Fact: 2002 – 2007 DRAFT. Unpublished manuscript. Monterey, CA: Defense Personnel Security Research Center

Helton-Fauth, W.B., Ainslie, F.M., Chandler, C.J. (2013). Department of Defense/automated continuing evaluation system continuing evaluation: Pilot study results. Tech rep. 13-03. Monterey, CA: Defense Personnel Security Research Center. FOUO

Helton-Fauth, W.B., Ainslie, F.M., Chandler, C.J., Harris, D.B. (2012). Department of Defense and Office of Personnel Management (OPM) Automated Continuing Evaluation System (ACES)

Automated Record Check (ARC) Pilot: Final Report. DRAFT. Unpublished manuscript: raw data. Monterey, CA: Defense Personnel Security Research Center

Herbig, K.L. & Nelson, P. R. (2004). Reciprocity: A progress report. Tech rep. 04-2. Monterey, CA: Defense Personnel Security Research Center

Lang, E.L. & Shedler, J. (2013). Relevant risk approach to Q21. DRAFT. Unpublished manuscript. Monterey, CA: Defense Personnel Security Research Center

Leggitt, J.S., Leather, J.E., & Lang, E.L. (2010). Using hand-held computers when conducting national security background interviews: Utility test results. Tech. rep. 10-01. Monterey, CA: Defense Personnel Security Research Center

Neal, M.M., Buck, K.R., & Chandler, C.J. (2006). Comparison of criminal history record detection methods to meet NACLC requirements: LAC, NCIC/III, and NLETS. Unpublished manuscript. Monterey, CA: Defense Personnel Security Research Center

Neal, M.M., Leather, J.E., Buck, K.R. OPM, ANACI, NACI, and NACLC investigations: Developing baseline information. Unpublished manuscript. Monterey, CA: Defense Personnel Security Research Center

Neal, M.M. & Buck, K.R. (2008). Greater information sharing needed between screening systems for military accessions and national security clearances. Tech. rep. 08-08. Monterey, CA: Defense Personnel Security Research Center

Nelson, L.C. & Smith-Pritchard, S.A. (2013). Baseline suitability analysis. Tech rep. 13-05. (Monterey, CA: Defense Personnel Security Research Center

Nelson, L.C. & Tadle, D.L. (2013). 2012 RADAR adjudication quality evaluation. DRAFT. Unpublished manuscript. Monterey, CA: Defense Personnel Security Research Center

Nelson, L.C., Crawford, K.S., Richmond, D.A., Lang, E.L., Leather, J.E., Nicewander, P.P., & Godes, O. (2009). DoD personnel security program performance measures. Management rep. 09-01. Monterey, CA: Defense Personnel Security Research Center

Office of Personnel Management. (2009, September 24). Guidance on implementing executive order 13488, "Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and

Reinvestigating Individuals in Positions of Public Trust." Washington, DC: Author. Retrieved October 14, 2013 at http://www.chcoc.gov/Transmittals/TransmittalDetails.aspx?TransmittalId=2518

Rose, A.E. & Buck, K.R. (2004). Crime self-reporting: Phase II. Management rep. 05-3. Monterey, CA: Defense Personnel Security Research Center. FOUO

Rose, A.E. (2005). Compact Council user fee survey. Unpublished manuscript. Monterey, CA: Defense Personnel Security Research Center

Rose, A.E. (2007). Options for using military waiver information in personnel security clearance investigations. Tech. rep. 07-03. Monterey, CA: Defense Personnel Security Research Center

Rose, A.E., Timm, H.W., Pogson, C.E., Gonzalez, J.L., Appel, E.J., Kolb, N. (2011). Guidance for developing a cybervetting strategy for national security positions. Management rep. 11-02. Monterey, CA: Defense Personnel Security Research Center. FOUO

Shechter, O.G. & Lang, E.L. (2011). Identifying personality disorders that are security risks: Field test results. Tech. rep. 11-05. Monterey, CA: Defense Personnel Security Research Center.

United States Army G2 & Office of Director of National Intelligence (ODNI). Assessment of emerging technologies for use in continuous evaluation phase 2. DRAFT. Unpublished manuscript. Washington, DC: Author

Youpa, D.G. & Smith-Pritchard, S.A. (2013). Development of a procedure to increase awareness and reporting of counterintelligence and terrorism indicators: Personal acknowledgment of staff security (PASS). Tech. rep. 13-02. Monterey, CA: Defense Personnel Security Research Center.

Appendix E. Glossary of Terms

Personnel security clearance. An administrative determination by competent authority that an individual is eligible for access to classified information.

Access to classified information. The ability and opportunity to obtain knowledge of classified information by persons with the proper security clearance and a need to know of specified classified information.

Insider. Any person with authorized access to any United States Government resource, to include personnel, facilities, information, equipment, networks or systems.[28]

Insider threat. The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.[29]

Physical security. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

Targeted violence. Pre-conceived violence focused on individuals, groups, or locations where perpetrators are engaged in behaviors that precede and are related to their attacks. These perpetrators consider, plan and prepare before engaging in acts of violence and are often detectable, providing an opportunity for disruption of the intended violence.[30]

28 National Insider Threat Policy, November 21, 2012

29 Ibid.

30 Defense Science Board Task Force Report: Predicting Violent Behavior, August 2012

Appendix F. Abbreviations and Acronyms

ACES	Automated Continuous Evaluation System
ANACI	Access National Agency Check plus Written Inquiries
CAC	Common Access Card
DIAC	Defense Installation Access Control
DITMAC	DoD Insider Threat Management and Analysis Center
DONCAF	Department of the Navy Central Adjudication Facility
DISS	Defense Information System for Security
e-QIP	Electronic Questionnaires for Investigations Processing system
FIS	Federal Investigative Standards
FSO	facility security officer
HSPD-12	Homeland Security Presidential Directive 12
IMESA	Identity Management Enterprise Services Architecture
IRTPA	Intelligence Reform and Terrorism Prevention Act
JPAS	Joint Personnel Adjudication System
JSIVA	Joint Staff Integrated Vulnerability Assessment
NACLC	National Agency Check with Local Agency Checks and Credit Check/
	National Agency Check with Law Check and Credit Search/
NCIC	National Crime Information Center
NCIS	Naval Criminal Investigative Service
NJP	non-judicial punishment
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
OPM	Office of Personnel Management
PERSEREC	Defense Personnel Security Research Center
PCL	personnel security clearance

PR	periodic reinvestigation
PSI	personnel security investigation
PSP	Personnel Security Program
RAM	random antiterrorism measures
SCI	sensitive compartmented information
SF-86	Standard Form 86, Questionnaire for National Security Positions
SPIN	subject personal interview
TSDB	Terrorist Screening Database
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
WNY	Washington Navy Yard