SECURITY FROM WITHIN

Independent Review of the Washington Navy Yard Shooting

NOVEMBER 2013

Report of the Independent Review

TABLE OF CONTENTS

INTRODUCTION

SCOPE

EXECUTIVE SUMMARY

FINDINGS AND RECOMMENDATIONS

1 **Cut the number of DoD employees and contractors holding Secret clearances, and adopt a "just in time" clearance system more tightly linked to need to know.**

2 **Use more and better data to investigate clearance seekers.**

3 **Implement "continuous evaluation" as part of DoD's personnel security program.**

4 **Establish Threat Management Units to decrease the risk of workplace violence.**

5 **Strengthen mental health care.**

6 **Centralize authority, accountability, and programmatic integration.**

APPENDICIES

1 - 6 **Information supporting findings and recommendations**

7 **Letter of Appointment and Terms of Reference**

8 **A timeline of the events leading to September 16, 2013**

9 **The Evolving Insider Threat**

GLOSSARY

ACRONYMS

ENDNOTES

INDEPENDENT REVIEW TEAM MEMBERS

REPORT OF THE DoD INDEPENDENT REVIEW

INTRODUCTION

Our Independent Review of the Washington Navy Yard Shooting has identified structural gaps and weaknesses in Department of Defense (DoD) security programs, policies and procedures. Fixing these flaws is essential to prevent future tragedies, and to ensure that those who died on September 16, 2013 did not perish in vain.

The changes we recommend are fundamental and far-reaching, and reflect the need to replace the underlying premise of installation and personnel security. For decades, DoD has framed installation security as a perimeter problem: Defend the perimeter, and installations can keep threats at bay.

This paradigm is outdated. Threats to our personnel and classified information increasingly lie within our installations, and come from DoD employees and contractors who are trusted insiders. The Department of Defense needs to strengthen security *from within*, and reframe its policies and programs to counter insider threats.

The current official definition of insider threats focuses on those who use their "authorized access, wittingly or unwittingly, to do harm to the security of the United States." The definition goes on to include "espionage, terrorism, or unauthorized disclosure" as examples. Although acts of workplace violence are not specifically mentioned, we found that many security gaps and weaknesses are common to all such insider challenges. Our report seeks to improve security against the full range of threats within DoD facilities, from severely troubled employees to those who knowingly serve America's adversaries.

Our analysis assumes that defense budgets will remain constrained. Therefore, we emphasize risk-based recommendations that would reallocate scarce resources to achieve the greatest improvements in security. Our recommendations also leverage the many promising but under-recognized pilot programs underway across DoD, the federal government, and the private sector.

Entirely eliminating the risk of attacks on DoD facilities and personnel is impossible. Taken too far, measures to tighten security can also impose unreasonable burdens on DoD employees and their families, and disrupt the ability of defense installations to execute their missions. Yet, there is much the Department can and should do to meet the challenges posed by insider threats, and to use the tragedy at the Washington Navy Yard as the starting point for transformational change in installation and personnel security.

Paul N. Stockton, PhD
Co-Chair
Secretary of Defense Independent Review
of the Washington Navy Yard Shooting

Admiral Eric T. Olson, U.S. Navy (Retired)
Co-Chair
Secretary of Defense Independent Review
of the Washington Navy Yard Shooting

THE SCOPE OF THIS INDEPENDENT REVIEW

Secretary of Defense Chuck Hagel established the DoD Independent Review of the Washington Navy Yard Shooting "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."

The Secretary specified that the review's "primary objective is to determine whether there are weaknesses in DoD programs, policies, or procedures regarding physical security at DoD installations and the security clearance and reinvestigation process that can be strengthened to prevent a similar tragedy in the future."

Mindful that the catalyst for this Independent Review was the Washington Navy Yard shooting of September 16, 2013, we focused on the factors that permitted the gunman – a Navy contract worker with a history of troubling behavior – to gain routine access to the guarded site where he shot his victims.

This shooting was, at its core, an incident of workplace violence perpetrated by an individual who had been investigated, adjudicated and credentialed to be exactly where he was on that morning. Aaron Alexis's armed presence in Building 197 at the Navy Yard did not require him to breach any physical barriers, because he had already been granted permission to enter.

In accordance with the Terms of Reference for the Independent Review, we considered all relevant aspects of this incident, including the physical security measures in place at the Navy Yard's entry gates. We did not focus our efforts on the issues related to "gates, guns and guards," however, because they have been comprehensively addressed by other investigations and panels.

Separately, the response by law enforcement authorities to this "active shooter" situation is the subject of a thorough review by the Federal Bureau of Investigation, and is therefore a matter that is outside the scope of our review. On the other hand, the Alexis case drew us to many issues related to mental health diagnosis and treatment, and we address these in some detail.

While our review focuses on security measures that might have prevented the September 16 shooting, we also identify underlying flaws in security policies, programs and procedures that put DoD personnel and installations at risk to a broad range of insider threats.

Wherever possible, we identify the specific legal or regulatory provisions that need to be either adopted or enforced to bring about the necessary policy improvements. We also specify whether the Secretary of Defense already has sufficient authority to direct the implementation of our recommendations – or whether changes in law, Executive Orders or interagency agreements will be necessary to go forward.

To keep the report brief, we focused its text on our recommendations and supporting analysis. Details of our findings (both those specific to Alexis and also our broader analysis of security policies and programs) can be found in the report's appendices and endnotes.

EXECUTIVE SUMMARY

SECTION ONE: Cut the number of DoD employees and contractors holding Secret clearances, and adopt a "just in time" clearance system more tightly linked to need to know.

Since 9/11, the number of clearances annually approved by DoD has tripled, and continues to grow. This growth magnifies the challenge of investigating clearance seekers, judging their applications, and periodically reviewing them after they are approved. A deeper problem helps fuel this growth: DoD fails to adequately apply the mandate that the Department grant clearances only those who require them (i.e., those whose positions and responsibilities give them a "need to know" classified information). We recommend that the Secretary Defense use his authority to direct a DoD-wide review to determine which positions actually require cleared personnel. As a starting point, DoD should seek to make a 10 percent cut in the number of positions that require access to material classified as Secret. DoD should also adopt a "just in time" clearance system that gets the Department back into compliance with need to know, and concentrates our resources on vetting and monitoring a smaller cleared population. In addition, we recommend measures by which the Defense Security Service can provide stricter oversight of Defense contractors.

SECTION TWO: Use more and better data to investigate clearance seekers.

DoD and the Office of Personnel Management (which investigates clearance applicants for DoD) should use additional sources of data, especially social media, financial data, and more detailed criminal records. DoD should collaborate with the Director of National Intelligence to establish standards for the use of these additional data, and fully comply with requirements to protect privacy and civil liberties.

SECTION THREE: Implement "continuous evaluation" as part of DoD's personnel security program.

Individuals with Secret clearances are subject to periodic reinvestigations (every 10 years at present, and every five years starting in 2016). As seen in the case of Aaron Alexis, the current system does not provide the opportunity to discover dangerous behavior between evaluations. The system also wastes resources; all cleared individuals get the same periodic reinvestigation, regardless of the risks they present. DoD should adopt a continuous evaluation system that provides for automated reviews of cleared personnel, and focuses follow-up investigations on those who trigger "red flags" under that system. DoD must apply Fair Information Practice Principles to continuous evaluation, including the need to regularly review whether these practices are actually protecting privacy and civil liberties as intended.

SECTION FOUR: Establish Threat Management Units to decrease the risk of workplace violence.

DoD lacks adequate mechanisms and training to protect personnel from workplace violence. Threat management units are multidisciplinary teams that assess the danger that individuals pose to their colleagues, and advise commanders and supervisors on measures to mitigate that danger. Borrowing from best practices in the Navy, the National Geospatial-Intelligence Agency, and the private sector, DoD should establish its own TMU system, educate its workforce about the risk factors of violence and how to report on potential workplace dangers.

SECTION FIVE: Strengthen mental health care.

Question 21 on Standard Form-86 is the primary means used to screen prospective DoD employees and cleared contractors for mental health concerns. That question risks stigmatizing mental health treatment, often fails to provide reliable information, and requires some respondents to lie. We propose substantial revisions to the question. We also recommend more effective measures to screen recruits, separate the unfit, further destigmatize treatment, and ensure the quality of mental health care within DoD. We propose initiatives to help commanders gain greater awareness of the mental health challenges facing their subordinates. Doing so is essential to help commanders meet their dual requirements to ensure mission readiness and care for their troops. To help strengthen that awareness, we recommend measures to improve communications between DoD and civilian health care providers (including those in the Department of Veterans Affairs), and bridge the cultural gaps between them on treatment of military patients.

SECTION SIX: Centralize authority, accountability, and programmatic integration.

Authorities and accountability for physical and personnel security matters are fractured within DoD and across many government agencies. DoD should assume responsibility for personnel security investigations from the Office of Personnel Management, and consolidate a single authority within the Department for security policies, budgets and implementation.

FINDINGS AND RECOMMENDATIONS

SECTION ONE
Cut the number of Department of Defense employees and contractors holding Secret clearances, and adopt a "just in time" clearance system more tightly linked to need to know.

Finding: Aaron Alexis was granted eligibility for access to Secret material even though he never needed it while on active duty with the Navy. This eligibility, valid for 10 years, allowed him to later gain employment at a DoD contracting firm that then granted him access to Secret-level information systems at the Washington Navy Yard.

Alexis was an example of a security clearance system that is flawed in two significant ways. First, it assumes that every service member will eventually need a clearance, and therefore grants eligibility "just in case." Second, initially as a service member and then as a contractor, Alexis represents the rapid growth of DoD personnel who are eligible for access to Secret material.

Prior to September 11, 2001, DoD processed approximately 200,000 security clearances annually. Since 9/11, DoD has approved approximately three times as many each year, with more than 630,000 clearances approved in Fiscal Year 2008.[1] As a result, DoD's Central Adjudication Facility (DoD CAF) reports that there are approximately 3.5 million cleared eligible personnel Department-wide.[2] This growth magnifies the challenge of investigating clearance seekers, judging their applications, and periodically reviewing them after they are approved.

An unknown (but we believe substantial) number of DoD personnel holding security clearances do not need them. Repeated Government Accountability Office (GAO) reports have determined that there are major inconsistencies in how DoD determines which positions require clearances, and little oversight of the process.[3] At the Top Secret level, this "need to know" sensibility still largely prevails through the designation of "compartments" of material to which the clearance holder is granted access.[4] At the far more prevalent Secret level, however, this ethos has broken down. Too many people are granted security clearances without a "need to know."[5] These multiple reports lead us to a broader finding: the continuing expansion of the cleared population has created a culture in which once-rare security clearances are now too often granted by default, which needlessly adds to the challenge of investigating and monitoring the cleared DoD workforce.

One reason why DoD so often defaults to submitting personnel for Secret clearances (rather than determine whether their positions actually require them) is that the clearance process is so slow. The current standard to complete the personnel security clearance process is 60 days. Because commanders may need to quickly assign personnel to cleared positions than this process permits, the Department has increasingly adopted the practice of providing for Secret-level eligibility "just in case" they may someday need access to such classified material in their duties.[6]

A related problem is that adjudications are often "stale," owing to elapsed time since the original determination was made. Currently, once individuals are granted security clearance eligibility, they are not monitored or reinvestigated when they are submitted for access until their periodic reinvestigations.[7] Alexis was granted Secret eligibility upon entering the U.S. Navy, and despite behavior that was of concern during the five years he maintained Secret eligibility, he was hired by The Experts, Inc. (TEI), and granted Secret access based on the adjudication and background investigation done five years earlier at the time of his enlistment.

Alexis was part of a "pool" of cleared personnel at TEI much larger than the company needed to execute its contracts at the time. TEI had 444 cleared personnel as of September 16, 2013. The 16 classified contracts under which TEI was performing work for the government required a total of 260 cleared personnel.[8] As was the case at TEI, this pooling of cleared personnel on the rosters of defense contractors is convenient to the contractor, because the practice helps them rapidly access personnel who are eligible to perform classified work. DoD Manual 5220.22 requires that companies determine the number of classified positions and the level of clearance on the basis of contract requirements. The Federal Acquisition Regulation requires that a government official approve such classified contracts. However, there is little coordination between acquisition and security functions once the contract is approved.[9] The cost of maintaining personnel in a cleared status is borne by DoD, not by the contractor.

Recommendation 1.1: Reestablish "need to know" as the basis for determining which positions and personnel require access to Secret material, through a one-time review of all military and civilian positions.

Currently, in accord with Department of Defense Instruction (DoDI) 1400.25, an "authorized management official" determines the sensitivity level of a position which, in turn, determines the level of clearance required by the military or civilian employee who is assigned to that position.[10]

An Office of Personnel Management (OPM) Position Designation Tool is available to support this effort, but the actual practices vary widely across DoD components.[11] As of 2013, DoD policy provides oversight of all stages of clearance investigation, but not on position designation.[12]

Executive Order 13467 authorized the Director of National Intelligence (DNI) to issue guidelines to agency heads, including the Secretary of Defense, on how to determine eligibility for to classified information.[13] The DNI and OPM are currently updating 5 Code of Federal Regulations (CFR) Part 732 (§ 1400) to do so, calling for a government-wide two-year review of all position description and requirements.[14]

Even before this guidance is issued, however, the Secretary can conduct a review of military and civilian position descriptions and requirements. The authority to do this resides in the combined authorities of Executive Orders 10450 and 12968 as amended, which make the heads of agencies responsible for establishing and maintaining effective programs to ensure that access to classified information is clearly consistent with the interests of national security.[15]

We recommend that the Secretary initiate such a review immediately, with an interim goal of achieving a 10 percent reduction in the number of positions designated at the Secret level. This goal admittedly has little analytical basis because of a lack of useful data owing to disregard of existing position designation guidance, but we think it is both achievable and meaningful. As soon as this reduction is attained, a follow-on review should determine whether further reductions can be realized.

Two related issues - a growing culture of over-classification[16] of information and the recent rapid proliferation of work spaces designated as "open storage" areas - merit additional focused study. In the meantime, implementing the recommendations of this section will help DoD make progress toward resolving both of these emerging challenges.

Finally, all DoD positions are currently coded as "national security positions." We recommend that the Secretary address this by requiring a report on whether the lower threshold of "public trust positions" is a suitable alternative in some cases, including for non-U.S. citizens who are serving within DoD.[17]

Recommendation 1.2: Within the above reduced levels, shorten the timeline required to investigate and adjudicate security clearances at the Secret level. Shift to a "just in time" approach to Secret-level investigations and adjudications.

We recommend that the "just in case" approach to granting Secret-level clearances be replaced by a "just in time" method.

Currently, all personnel applying for national security positions at DoD – whether military or civilian – are already subject to completing a personnel security investigation (PSI), which includes the Standard Form-86 (SF-86) and National Agency Check with Local Agency and Credit Checks (NACLC) investigations.[18] This SF-86/NACLC process accomplishes everything that is normally required to permit adjudication for access to Secret material.[19]

Under a "just in time" approach, this process would not change – every military and civilian employee would still have an SF-86 and NACLC in their file. However, the requirement to submit everyone for a Secret-level clearance upon entry to government service would disappear. Instead, personnel would be subject to an eligibility determination when they are actually designated for a position that requires access to Secret material.

When implemented, this would essentially eliminate the status of "eligible for Secret," an often confusing and ambiguous condition in any case. Personnel who went through the initial SF-86/NACLC process and were hired or enlisted/inducted would be in a "national security" status, cleared for access to official (but not classified) information. They would elevate to "Secret access" status as needed, and only upon adjudication.

A "just in time" approach would offer several benefits. First, it would provide commanders and supervisors increased flexibility in shifting personnel into and out of Secret access. Second, it would support DoD's efforts to base security clearance on a "need to know." Third, it would

eliminate the expense of unnecessary investigations and adjudications. Fourth, and most important, it would ensure that Secret-level access, when granted, is based on up-to-date information.

We recommend that DoD set an aggressive goal in this regard; 90 percent of Secret adjudications accomplished within seven days. When the seven-day timeline is impossible for normal administrative reasons, an interim clearance can be issued if it is urgently required.

Although the Intelligence and Reform and Terrorism Prevention Act (IRTPA) requires that 90 percent of adjudications be completed within 60 days, there is no legal prohibition against allowing the Secretary to request a more compressed timeline. Close coordination with the DNI, as the Security Executive Agent under Executive Order 13467, would be required.

Recommendation 1.3: DoD should review and adjudicate clearances using an event-driven model that captures when eligible individuals are submitted for Secret access or change status.

All personnel should undergo a status-change review at key junctures in their career, rather than waiting for the next scheduled periodic reinvestigation. Events that would require a review might include transitioning to a position in the reserves from active duty, or taking a contractor position in the private sector.

Implementation of this recommendation would require permission from the DNI to implement an event-driven adjudication system and potentially legislative change. For the sake of reciprocity, current law prohibits re-adjudication "except when an agency has substantial information indicating that an employee may not satisfy the standards," required for eligibility.[20]

Executive Order 13467 and the IRTPA go further to state that agencies may not establish additional investigative or adjudicative requirements without the approval of the Security Executive Agent (SecEA), the DNI.

Recommendation 1.4: Improve oversight and enforcement of the clearance process for contractors.

We recommend that the Secretary direct the Under Secretary of Defense for Acquisition, Technology and Logistics (USD[AT&L]) and the Under Secretary of Defense for Intelligence (USD[I]) to issue new guidance that will ensure alignment between the acquisition and security functions related to defense contracting, and that the number of cleared personnel maintained on contractor rosters remains within established guidelines. As the manager of the Industrial Security Program under DoD Manual 5200.22, the Secretary has the authority to implement this recommendation.

We recommend that the Secretary direct the Defense Security Service (DSS) to establish a method of monitoring the number of cleared contractor personnel in the Joint Personnel

Adjudication System (JPAS) database, and of comparing that figure to the number called for under current contracts.

This should include a consistent procedure to respond to instances where the number of cleared personnel is deemed to be excessive. DoD Manual 5200.22 and DoD 5105.42 grant the Secretary and DSS the authority to implement this recommendation. DSS oversight of contractors that conduct classified work is also addressed in Section Six of this report.

SECTION TWO
Use more and better data to investigate clearance seekers.

Finding: The OPM-contracted investigators did not discover that Aaron Alexis had shot out the tires of a car in a 2004 Seattle incident, because they had accepted as adequate a court record that described the circumstances of his malicious mischief charge, in accordance with Federal Investigative Standards (FIS). The Navy adjudicators granted Alexis eligibility for a Secret clearance (despite the fact that they knew he had misled them on his SF-86), on the grounds that he had no prior arrests.[21]

These facts reflect five critical problems in the security clearance investigation and adjudication processes:

- OPM investigators are not required to pursue all information that is available and relevant, under existing Federal Investigative Standards.[22]
- OPM investigators may not have access to relevant information.
- The majority of investigative reports that OPM provides for DoD adjudication are incomplete.[23]
- Data integration systems, such as they exist, employ archaic technologies.
- DoD lacks qualitative metrics for OPM investigations or for its own clearance adjudications.

Recommendation 2.1: Expand access to data sources not currently used in personnel security investigations.

OPM currently uses a limited number of government and commercial records databases. These include credit report information, the National Crime Information Center, and local law enforcement databases, among others. Pilot programs such as the Army G-2 continuous evaluation (CE) system are exploring access to additional databases. For a more extensive discussion of continuous evaluation, see Section Three.

We recommend that DoD explore additional sources of relevant information, including the use of social media in security clearance investigations.

Currently there is no legislation or government-wide policy addressing the use of social media as part of a personnel security investigation. Executive Order 13467 allows for the use of commercial databases in CE. However, the absence of any guidance for federal agencies on the use of social media as part of a personnel security program inhibits the use of it. To ensure the reciprocity of security clearances, agencies involved in the granting of a security clearance must obtain SecEA approval in order to establish additional investigative requirements.

In the absence of a government-wide policy, an agency head must seek approval from the SecEA to pilot the use of social media as part of any personnel security program. Then the SecEA must evaluate the results, requiring additional time.

However, a clearly stated policy that establishes standards for the use of social media in personnel security investigations would significantly advance the role of social media in CE for the U.S. government.

Social media sites can include information of relevance in assessing suitability for clearances – and anyone who seeks to be trusted with a clearance should not object to allowing an evaluation of social-media information and images that he or she may have voluntarily shared with hundreds or thousands of people worldwide. Such evaluations should be carefully tailored to include only potentially relevant material, with particular care taken to protect the "third-party data" of others.

The Army G-2 program includes social media source checks to determine if relevant data is available between reinvestigations. This program used a private company that established thresholds to identify information that may be relevant to clearance adjudications under the White House's 2005 Adjudicative Guidelines.

Using social media, the pilot program reviewed approximately 3,370 cleared Army personnel.[24] At least 20 percent of the individuals subject to the pilot have been identified as having information relevant to adjudication.[25] The DNI's preliminary analysis of the pilot reflects that while none of the issues identified were disqualifying by themselves, there is value in collecting information from social media sources. DoD should advance the Army's G-2 CE pilot program for rapid fielding, as a means of further developing CE for evaluating cleared personnel.

Information derived from social media presents some unique challenges. It can be difficult to substantiate, and its sheer abundance makes it hard to filter for relevant material. Additional research is needed, but the potential value of social media for clearance assessment cannot be ignored, and should be evaluated further. [26]

Recommendation 2.1.1: Improve information-sharing with state and local law enforcement agencies to ensure better data for clearance investigation and adjudication processes.

At the time of Alexis's tire-shooting incident, Seattle Police Department practice had been to release only conviction information to OPM investigators – not incident reports on arrests that did not result in a conviction.[27] Therefore, no data on the 2004 shooting was provided, and the arrest record was missing from Alexis's NACLC report.

In coordination with the FBI, DoD should work with organizations like the International Association of Chiefs of Police, Major Cities Chiefs Association, the National Sheriffs' Association, and other state and local law enforcement associations to strengthen DoD access to law enforcement information that might be relevant to determining an individual's eligibility for a clearance.

Many police departments provide this information. In early 2011, the Seattle Police Department changed its policies to permit the release of incident reports on arrests – including those that do not lead to conviction – to OPM background investigators.[28]

However, many cities and some states still have ordinances that limit the release of data other than convictions. Rather than review these constraints on a jurisdiction-by-jurisdiction basis, we recommend initiating dialogue with key associations to build consensus on improved access, while fully respecting state and local laws and ordinances – as well as constitutional considerations – related to such issues.

Access to juvenile violent-felony records could also reveal useful information, and might be particularly relevant in the case of security clearance candidates who are right out of high school and do not have an extensive personal history to report.

However, given the various ways in which state and local jurisdictions deal with the treatment of maintenance of juvenile felony records, the use of such material for clearance investigations will require an intensive and cooperative effort between federal, state and local authorities.

Recommendation 2.1.2: Require DoD adjudicators[29] to reject as incomplete any investigation report that does not include a copy of local police arrest records, if such records are available.

In May 2009, GAO found that "about 87% of about 3,500 investigative reports that adjudicators used to make clearance decisions were missing at least one type of documentation required by the federal investigative standards and OPM's internal guidance. …"[30]

In June 2013 testimony, GAO reported that OPM had not taken any action to measure the completeness of its investigative reports and further stated, "OPM continues to assess the quality of investigations based on voluntary reporting from customer agencies," either from returned reports or from adjudicator feedback submitted via an OPM website or hotline.[31]

In accordance with the Federal Investigative Standards, the USD(I) should issue guidance for DoD adjudicators clarifying when investigative reports should be returned to OPM as insufficient.

Recommendation 2.1.3: Improve the use of financial data.

Cleared personnel who have severe debts may be vulnerable to bribery or blackmail. A recent GAO study highlighted that "about 8,400 individuals adjudicated as eligible for a security clearance from April 2006 to December 2011 owed approximately $85 million" in federal taxes.[32] Access to debt information is needed to better position federal agencies to assess security clearance applicants.

After the Navy Yard Shooting, the issue of reforming security clearances has received increased attention from Congress. A bipartisan group of senators introduced legislation in the last week of October 2013 requiring frequent records checks of an increased number of government, public, and commercial databases – including those of the major consumer reporting agencies.[33]

In addition to expanding the range of databases used for investigations, those sources of information need to be better integrated. This would provide the holistic view needed to identify trends and patterns during the security clearance process. To bring about such integration, DoD needs to work in active cooperation with the DNI.

Recommendation 2.2: DoD must adjudicate more restrictively when granting eligibility for access using the 2005 Adjudicative Standards.

The current Federal Adjudicative Standards state, "Each case must be judged on its own merits. … Any doubt concerning personnel being considered for access to classified information will be resolved in favor of national security."[34] DoD policy states that the omission, concealment, or falsification of relevant facts from the personnel security questionnaire "*could* raise a security concern and *may* be disqualifying."[35] (Emphasis added.)

DoD guidance should be revised to standardize adjudication decisions involving the omission, concealment, or falsification of information provided in the personnel security questionnaire. This would require revisions to the adjudication training program as well as metrics to assess the application of the revised guidance.

Furthermore, DoD should introduce a quality assurance program that randomly audits adjudications for quality. Such a program ensures the integrity of the adjudicative process and is consistent with the Secretary's responsibility for maintaining an effective personnel security program.[36] Finally, DoD must continue to be a lead player in interagency working groups to establish standards for the quality and comprehensiveness of a background investigation.

SECTION THREE
Implement "continuous evaluation" as part of DoD's personnel security program.

Finding: Determining how our security clearances should be organized, and who should hold them, is just the beginning. An equally important question is how we should evaluate the people who receive these clearances.

Potentially useful security-related information often goes unnoticed during the long periods between reinvestigations of cleared individuals. For example, over a month before the Navy Yard shooting, Alexis displayed psychotic behavior to active duty police force members at Naval Station Newport, to civilian police officers in the town adjacent to the base, and to coworkers. Even earlier, Alexis did not sufficiently self-report his contact with law enforcement during his service in the Navy. These incidents affecting his continued eligibility were not investigated or were missed altogether.

In order to ensure retention of a security clearance, DoD should work with DNI to move toward a system of "continuous evaluation" (CE) of employees. The definition of CE as established by EO 13467 is "reviewing the background of an individual who has been determined to be eligible for access to classified information or eligible to hold a sensitive position (including additional or new checks of commercial databases, government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements of eligibility."[37]

Individuals seeking eligibility for access to classified information already authorize federal agencies to carry out such an evaluation.[38] DNI is the federal executive agent for CE,[39] and has granted approval for DoD to conduct CE pilot initiatives, including the ongoing Army G-2 CE pilot (see Section Two above) and a DoD Continuous Evaluation Concept Demonstration (CECD) that is expected to begin in April 2014.

The CE approach challenges the DoD "once in, always in" culture, which tends to regard its cleared personnel as a trusted population that only requires infrequent reassessments of eligibility for clearances and installation access. The current FIS require individuals with access to Secret level information to undergo periodic reinvestigation every 10 years. The revised FIS will require periodic reinvestigation every five years.[40]

Recommendation 3.1: DoD must shift from exclusive reliance on periodic reinvestigations to a risk based personnel security clearance program that includes both periodic reinvestigations and CE.

DoD must work with ODNI to aggressively accelerate CE pilot programs and to establish government-wide CE standards for all individuals eligible for access to classified information.

CE must not only have the ability to "pull" records upon request, but to have critical records automatically provided – or "pushed" – to the appropriate security authority. This allows for "red

flags" to be identified and addressed in a timely manner and provides the government with the opportunity to allocate resources using a risk management approach.

For the Army G-2 CE pilot, the Automated Continuous Evaluation System (ACES) runs checks of 38 government and commercial data sources.[41] ACES does not provide access to all possible records in making an eligibility determination, but it does provide the capability to conduct pertinent records checks in a timely manner. ACES has also demonstrated that obtaining even a limited number of records yields relevant information; DoD must seek approval from SecEA to use ACES more than it presently does.

Additionally, the FBI has the ability, through its Rap Back Service, to continuously inform authorized agencies of reported activities – such as arrests and convictions – by individuals in positions of trust, which includes individuals eligible for access to classified information.

The Rap Back Service is flexible and can notify an authorized agency as appropriate. Rap Back is a fee-based service, but the potential to obtain pertinent data in a timely manner – and the utility of such data given limited personnel security resources – is reason enough to explore its use as part of a robust CE program.[42]

Recommendation 3.2: DoD must immediately institute an aperiodic reinvestigation program as an interim step toward establishing CE.

DoD gains little to no insight into its cleared workforce between periodic reinvestigations. As DoD incorporates CE into its personnel security program, it must take an approach that accounts for this risk.

Executive Order 12968, as amended, allows for the investigation of individuals granted access to classified information at any time during their period of access to determine whether or not they continue to meet the requirements for access.[43] The SecEA recently established criteria for a risk based approach to update overdue reinvestigations, and this guidance can be used by DoD to accelerate reinvestigations as part of an aperiodic program. This approach would be an effective interim step as DoD shifts to CE.[44]

Recommendation 3.3: DoD should request that the DNI grant it the authority to conduct CE.

While the DNI will establish the standards and thresholds for additional investigation using CE, the fact remains that an agency head is the one responsible for ensuring that access to classified information by his or her own employees is consistent with the interests of national security,[45]

Consistent with this principle, DoD must manage its own CE program to ensure the continued eligibility of military members, civilian employees, and contractors. To achieve this, DoD must seek approval from the DNI as the SecEA for continuous evaluation.

Recommendation 3.4: Ensure that privacy and civil liberties are protected.

As DoD uses additional sources of data for continuous evaluation, it is essential that the Department only does so in full compliance with laws, regulations, and policies protecting individual privacy and civil liberties.

In particular, CE will likely increase the volume of personally identifying information (PII) maintained by DoD about cleared personnel. To match this drive for more comprehensive data to support CE – and any other collection of personal information recommended by this report – DoD programs must satisfy established privacy and civil liberties protections.

These cannot simply be initiatives to be added on later, after the need for them becomes all too apparent. They must be woven into CE as it is first established so that potential problems can be averted.

DoD should use the Fair Information Practice Principles (FIPP) framework to help scale up its privacy protections for CE.[46] In doing so, compliance with the Privacy Act of 1974, as amended, DoD Directive 5400.11, *DoD Privacy Program*, and DoD 5400.11-R, *DoD Privacy Program*, and DoD Instruction 1000.29, *DoD Civil Liberties Program*, will be essential.

This framework should reflect the following values and considerations:

- **Transparency.** Individuals must be clearly and fully informed in plain language that before they can be determined eligible for access to classified information, they will need to consent to continuous evaluation. Individuals should also be given a detailed understanding of what that evaluation will include, such as the use of non-governmental databases, as well as an understanding of how PII will be collected and maintained.
- **Individual Participation.** Access to classified information is a privilege and not a right. Therefore, in completing the SF-86, personnel sign a release authorizing the use of CE, and new DoD CE pilots should obtain explicit consent from evaluated personnel. DoD must also ensure reasonable individual access to records maintained about them; the ability to request amendment to those records; and an appropriate process for seeking redress regarding the use of employee PII. We recommend that DoD build a culture that embraces individual participation, including a willingness to be challenged by cleared personnel. Ultimately, such employee participation will strengthen the effectiveness of CE.
- **Purpose Specification.** In every use of CE, DoD will identify authorities for the use of CE and the collection of PII. Authorities will be clearly identified in notices provided to personnel under investigation. The purpose of any CE collection must be specifically tied to clear legal authority.
- **Data Minimization.** DoD will collect only PII that is relevant and necessary to fulfill the purposes listed in notices to personnel. Proposed CE pilots must detail how data will be minimized, and should explicitly state how long such data will be retained by the Department. Of special consideration is how DoD will deal with the collection of third

party data in conducting CE. We recommend that DoD take every precaution to avoid maintaining information about individuals who are not subjects of CE.

- **Use Limitation.** DoD will not use PII collected through CE for any purpose other than those listed in the notices provided to personnel who are investigated.
- **Data Quality and Integrity.** In carrying out CE, DoD should develop adequate safeguards and controls to ensure that the information collected about an individual is accurate; that the information is relevant to the purposes listed in the notices; that the information is current and timely; and that the PII collected is complete as it relates to the individual.
- **Security.** Personnel security programs must ensure appropriate safeguards and controls are used to ensure the constant security of any PII that is collected as a result of CE. Safeguards and controls must provide a high level of security to ensure personal information is not inappropriately disclosed or modified. DoD must ensure that an efficient process is in place to notify individuals if their PII is breached, and to help the mitigate the harm caused by such a breach.
- **Accountability and Auditing.** Systems maintaining information collected as a result of CE must be auditable. An oversight mechanism must be implemented to ensure accountability for systems maintaining CE data. Auditing the actual use of PII to demonstrate compliance with the FIPPs will help to ensure all applicable privacy protection requirements are met. The Department must be prepared to complete privacy and civil liberties based assessments of their programs, and periodically reassess the uses of maintained information to ensure that initiatives comply with privacy and civil liberties protections.
- **First Amendment Rights.** The overall CE enterprise must be structured so as to prevent its implementation from chilling the exercise of First Amendment rights and freedoms.

SECTION FOUR
Establish Threat Management Units (TMUs) to decrease the risk of workplace violence.

Finding: In August 2013, about five weeks prior to the Navy Yard shooting, Aaron Alexis displayed psychotic behavior. This was reported to supervisors and police, but DoD lacked a system to assess the potential threat Alexis posed to himself and others around him.

DoD does not adequately address the potential for workplace violence. Dangerous behavior and warning signs often go unrecognized and unreported. Mechanisms to report and prevent potential workplace violence are inadequate. DoD does not know how much violence occurs on its installations annually, or how many employees are victimized by it. [47]

Recommendation 4.1: DoD must establish a strong Threat Management capability.

In its August 2012 report, the Defense Science Board (DSB) Task Force reviewing the Fort Hood shooting recommended "a threat management approach employing multidisciplinary professionals in support of local commanders/supervisors provides the best practical solution" to the problem of addressing workplace violence.[48]

The Navy, unique among the armed services, has established a TMU – a unit established within the Naval Criminal Investigative Service (NCIS). It consists of a small group of full-time NCIS agents, part-time analysts, and a staff psychologist as well as a larger group of agents and investigators who handle TMU-related matters in the field. Legal, medical, human-resources, and other officials assist on an ad-hoc basis.[49]

The emphasis is on prevention, and much of the unit's activity focuses on responding to activity that may be a precursor to violence down the line, such as stalking, threatening communications, and domestic disputes. The TMU assesses the situation and refers the case to local NCIS colleagues or to the relevant commanders as required.[50]

A threat management capability, if implemented, would assess risk and recommend action before events escalate to violence. It would ensure that trained, responsible professionals are available to validate, investigate, and evaluate concerns about individuals based on established standards. The range of possible responses is broad and incorporates constructive interventions to help a troubled employee, not just punitive actions.

DoD should evaluate existing military and agency efforts, such as the NCIS TMU,[51] the National Geospatial-Intelligence Agency's Threat Management Unit,[52] and the VA's Employee Threat Assessment Team (ETAT),[53] as well as private sector and academia[54] in creating its threat management infrastructure. The field of threat assessment provides further insights into the scientific and technical issues, approaches and best practices for risk assessment.

We recommend an approach that uses localized threat management teams for assessment and management of specific threats. We also recommend that DoD move forward as rapidly as possible to adopt the DSB Task Force's recommendation to establish Department-wide TMU

capability and that it do so by establishing a centralized Joint Threat Management Unit (JTMU) to oversee component-level TMU functions. A JTMU would empower decentralized local teams, which can then in turn work with supervisors and commanders.

Recommendation 4.2: Educate the workforce.

Workplace violence prevention requires consistent policy,[55] comprehensive training, and effective reporting structures, in addition to threat management teams. As with efforts to prevent sexual assault, suicide, and domestic violence, a better understanding by employees and workmates of what behaviors indicate potential violent behavior will improve awareness and reporting.

We recommend that DoD assess best practices in workplace violence prevention training and institute a training program for employees and supervisors. Training should emphasize the role of the TMUs in managing workplace risk.

Recommendation 4.3: Emphasize "peer reporting" as more reliable than "self-reporting." Make reporting safe, easy, and accessible.

Threat management efforts cannot work if troubling behavior is not identified or reported. Comprehensive, easily accessible reporting mechanisms are needed across DoD to ensure potentially troubling behavior receives quick attention and potential resolution.

Relying on self-reporting alone is insufficient. Existing policies and culture rely on individuals to self-report derogatory and other significant personal information, such as law enforcement involvement, financial problems, or mental health issues. In general, workplace violence is significantly underreported[56] and, in particular, DoD culture tends to shun reporting of concerns about co-workers. Further, it may serve to penalize those who are candid or self-aware enough to report truthfully, while giving a free pass to the deceitful or the unaware.[57]

Supervisor and peer observation offer two complementary, often superior mechanisms to self-reporting risk behaviors relating to personnel reliability, including mental health problems that pose a risk of violence. Peer reporting can work. For example, a critical DoD program, the Nuclear Personnel Reliability Program, relies heavily on peer reporting.[58] DoD must shift from a system largely reliant on self-reporting to one that encourages co-workers, supervisors, and even family members, to communicate their concerns.

A robust threat management approach both relies on and supports a culture in which it is acceptable to report concerns about colleagues who are showing signs of disturbance or violent tendencies. It ensures that trained, responsible professionals are available to validate, investigate, and evaluate these concerns based on established standards.

DoD must provide mechanisms for parties to report concerns without exposing their identities. Employees who report on their workmates must feel safe from both violence and any negative

consequences of reporting, such as reprisal. Since not all troubling behavior occurs in front of coworkers, the TMU must also be accessible to – and able to interact with – members of the community outside of DoD. Friends and family, outside care providers, and other threat management teams (such as those established at educational institutions in some states),[59] may provide key pieces of the puzzle in assessing threats.

DoD must create policy and procedures to enable employees, family members, or the general public to report on troubling behavior. Availability of multiple reporting channels may encourage active employee participation.[60] These could include anonymous tip lines and increased awareness campaigns to spread the word that early reporting of suspect behavior could prevent a potential terrible and violent act. DoD must establish training programs to educate the work force that peer reporting is critical and that no stigma should attach to the act of reporting a serious concern. Our consultations with private sector security experts support this approach to foster employee awareness and to empower people to report problems as soon as they arise.

Recommendation 4.4: Collect, store, and report data about violence in the DoD workplace.

DoD does not sufficiently collect or share data on violence-related incidents at its installations, making it difficult to identify and act upon emerging threats, determine baselines, or assess outcomes of efforts to reduce violent behavior. DoD needs to track and maintain information on violence and other criminal incidents.

DoD should implement the recommendation from the DoD Independent Review of the Fort Hood shooting and the DSB Task Force calling upon the Department to "[e]stablish a consolidated criminal investigation and law enforcement database such as the Defense Law Enforcement Exchange."[61] DoD should reexamine its policies on the collection and sharing of crime and workplace-violence data and ensure that mechanisms are in place to report such data as required.

SECTION FIVE
Strengthen mental health care.

Finding: Aaron Alexis demonstrated increasingly severe behavioral and impulse control problems as he left active duty and served in the Navy Individual Ready Reserve. Supervisors and public safety officers witnessed these problems.[62] Yet, he was never separated during active duty, never referred to definitive care, and never received treatment that might have prevented the tragedy of September 16, 2013.[63]

Establishing Threat Management Units across the Department will increase the likelihood that service members who need mental health care will be identified. However, we have also identified broader policy and programmatic changes needed to improve the way DoD provides for such care. In developing our recommendations, two factors were paramount in our analysis.

First, from the perspective of predicting violence,[64] mental illness[65] (in isolation from other risk factors[66]) is an *exceedingly* weak indicator of future violence, including workplace violence.[67] Improved diagnosis of mental health problems cannot be the sole focus of violence-prevention efforts.[68]

Second, it is imperative that DoD continue its work to assist individuals who have acquired mental health problems during their service, and avoid stigmatizing those who are receiving the care they need. Significant increases in Department of Veterans Affairs (VA) and DoD resources[69] have improved the availability of health care. A range of policy changes could maximize the effective use of these resources, from the moment military applicants seek to join the DoD workforce (accession) through their transition to reserve or retired status.

We focus much of our analysis below on the active duty military. However, many of the measures we propose will ultimately benefit the broader DoD workforce, since nearly half of DoD's civilian employees (and many of its contractors) previously served in active duty status. [70]

Recommendation 5.1: Revise SF-86 Question 21

Self-reporting provides the primary means by which individuals seeking DoD employment are screened for mental health problems. Question 21 on the SF-86 (Questionnaire for National Security Positions) requires all individuals seeking employment to self-report their mental health treatment histories. The current version of Question 21 reads as follows:

> Mental health counseling in and of itself is not a reason to revoke or deny eligibility for access to classified information or for a sensitive position, suitability or fitness to obtain or retain Federal employment, fitness to obtain or retain contract employment, or eligibility for physical or logical access to federally controlled facilities or information systems.
>
> In the last seven years, have you consulted with a health care professional regarding an emotional or mental health condition or were you hospitalized for such a condition?

> Answer 'No' if the counseling was for any of the following reasons and was not court ordered:
> - Strictly marital, family, grief not related to violence by you; or
> - Strictly related to adjustments from service in a military combat environment.
>
> Please respond to this question with the following additional instruction: Victims of sexual assault who have consulted with the health care professional regarding an emotional or mental health condition during this period strictly in relation to the sexual assault are instructed to answer No.

Such self-reporting is inherently problematic. There are *no* data showing that the answers to Question 21 are generally truthful and accurate. On the contrary: during our research on this issue, we gathered strong anecdotal evidence that individuals frequently prevaricate in their responses. In fact, the way the question is worded, individuals are actually instructed to lie if they have received treatment for any one of these very different types of difficulties.

We recommend that DoD and its interagency partners gather data on response veracity to determine whether Question 21 should be eliminated from SF-86, except for individuals slated for follow-on polygraph testing. Additionally, we recommend that DoD propose to ODNI that Question 21 be revised so that it does not inadvertently discourage individuals from seeking care.

Despite recurrent edits, current wording of Question 21 *still* risks stigmatizing mental health treatment.[71] We propose to revise the question to make it less likely to discourage treatment, and help individuals understand that effective care is available.

For the introduction section of Question 21, we recommend adding the following text to improve respondents' understanding of the importance of seeking mental health care if they need it:

> Mental health counseling in and of itself is not a reason to revoke or deny eligibility for access to classified information or for a sensitive position, suitability or fitness to obtain or retain Federal employment, fitness to obtain or retain contract employment, or eligibility for physical or logical access to federally controlled facilities or information systems. *Failure to seek care for mental health issues is of much greater concern than seeking help. Seeking professional care for mental health issues will not necessarily jeopardize an individual's security clearance.*

For the wording of Question 21 itself, we recommend the following:

- 21.1: In the last seven (7) years, have you consulted with a health care professional regarding an emotional or mental health condition or were you hospitalized for such a condition? Yes No
  - If Yes, was your treatment the result of traumatic experiences, marital or family stress, grief or in connection with having been a victim of sexual assault? Yes No
- 21.2 Are you currently experiencing any mental health concerns which for which you believe it would be beneficial to see a mental health professional? Yes No.

At the end of the SF-86 Questionnaire in the Authorization for Health Insurance Portability and Accountability Act (HIPAA) release, we recommend addition of the following text under the section "For Use by Practitioner(s) Only":

- Was the treatment sought by this person focused on traumatic experiences, marital or family stress, grief or in connection with having been the victim of sexual assault?
- In your judgment, does the person under investigation have a condition that could impair his or her judgment, reliability, or ability to properly safeguard classified national security information?"

Recommendation 5.2: Help commanders better assess and respond to mental health challenges.

There was a 65 percent increase in the incidence of mental health diagnoses in the military between 2000 and 2011.[72] In part, that growth reflects congressionally-mandated changes to ensure that those who suffer from post-traumatic stress disorder, traumatic brain injury, and other invisible wounds of war are not unfairly discharged from the Armed Forces. We strongly support the fair treatment of those who have served and acquired mental health problems during honorable service.

Nevertheless, DoD must effectively use health care resources to balance this population's growing need for necessary care with needs of the military mission. The recommendations below will help DoD achieve greater efficiencies and effectiveness in its mental health care system.

Recommendation 5.3: Strengthen mental health standards for induction.

One way to better use scarce mental health resources is to tighten the standards applied to individuals seeking to enter the military, and reduce the number of entrants who already have mental health problems. Tightening these standards is especially appropriate at a time when DoD is reducing the number of personnel in the workforce.

Measures to reduce the burden on DoD's mental health system through tighter induction screening will have important downstream benefits. Individuals with mental health diagnoses conferred as recruits are at increased risk for early attrition and are 77 percent less likely to deploy.[73]

Current recruiting and accession procedures are poorly suited to screening out the mentally unfit.[74] In particular, induction procedures rely heavily on previous diagnoses of mental health problems, and the assumption that individuals who do have mental illness or concerning histories will report these during military processing[75] or apply for waivers to be inducted.[76] We recommend that DoD move away from exhaustive lists of disqualifying diagnoses and go beyond cognitive assessment toward evaluation of dimensions such as personality and motivation, for two reasons:

First, because of changes in the diagnosis of mental illness in children and adolescents, diagnosis alone provides an inadequate proxy for screening inductees. Diagnoses of mental illness in childhood and adolescence have increased markedly in the last two decades, and the connection between a particular illness and functional problems can be limited by confounding factors and evolving trends in diagnosis.[77] Accession standards based on diagnoses also promote deceit among many applicants who ultimately do enlist and ship to recruit training. Given the obvious incentive to withhold information, it is not surprising that pre-existing mental health conditions are found at recruit training.[78]

Second, evaluating domains such as personality and motivation in candidates provides a stronger basis for screening. Non-cognitive measures, such as the Assessment for Individual Motivation (AIM) and Tailored Adaptive Personality Assessment System (TAPAS) could offer potential to predict mental health fitness for duty. The AIM composite score predicted mental disorder diagnoses in the first year of service. Certain TAPAS subscale scores were also associated with a mental disorder diagnosis within six months of entering service.

After adjustments for confounding factors (such as age, sex, race, and body mass index in both groups), scorers in the lowest quintile of AIM and TAPAS had, respectively, 56 percent and 100 percent higher rates of attrition and 44 percent and 41 percent higher odds of being diagnosed with a mental disorder than those in the highest quintile. Because AIM/TAPAS are already operationalized for use at all Military Entrance Processing Stations (MEPS), we recommend that medical officers at MEPS use these measures to determine whether an applicant requires a mental health consultation.[79]

Recommendation 5.3.1: Use the first 180 days of service to better identify mental health and conduct problems, and increase administrative separations for recruits.

At present, DoD underuses the 180-day entry period to cull candidates for reasons of mental health and conduct.[80] Entry-level separations for issues of mental health, performance, and conduct[81] are considerably lower than the rates of psychopathology in the adolescent population,[82] despite an expectation that mental health problems in recruit trainees would reflect trends in this population.[83]

Of course, the need to discharge problematic new service members does not stem solely from the impetus to reduce DoD workplace violence. Mental health issues in isolation, as discussed above, cannot be used to predict violent behavior with validity and reliability. As the military shrinks, separating those with mental health problems that significantly impact their performance will ensure that those in the military are most capable of executing the mission.

Appropriately separating recruits out during their first 180 days will also reduce the burden of downstream mental health care requirements, and free up mental health resources for those already in the military who most need such care.[84] Naturally, DoD must continue to ensure that transitions to community mental health care are arranged for individuals who are separated under these circumstances.

To make separation processes more effective during this initial period, DoD should increase the presence of uniformed or other qualified mental health professionals in training commands, and ensure these personnel have expertise in administrative behavioral health, the demands of contingency operations, and recruit management and evaluation procedures, across the services.[85] These personnel would assist local commanders to do a better job identifying and separating recruits and first term enlistees on a mental health[86] and behavioral[87] basis.

Finally, to reduce the risk that this process will separate personnel who might ultimately have become effective members of the workforce, DoD should conduct further research to prospectively identify factors that can be identified during recruit training which predict long term outcomes among service members. Outcomes of interest would include duration of service, discharge status, promotion trajectory, and legal, behavioral and mental health outcomes.

Recommendation 5.4: Accelerate evaluation of mental health care program effectiveness, and improve monitoring of care across DoD.

Even with the major increases in DoD and VA mental health care spending over the past years, there is a persistent gap between in the number of individuals receiving mental health care and the number of individuals suffering.[88] Hence, it is vital to assess the effectiveness of treatment programs, including those that could have most benefited Aaron Alexis.

DoD has recently increased its program evaluation efforts. In an inferential assessment mandated by DoD's Cost Analysis and Program Evaluation Office (CAPE), several such programs were found to have substandard documentation procedures and minimal evidence for their effectiveness – which raises concerns about the system's ability to identify, manage, or refer clients with mental health or behavioral concerns, including substance abuse.[89]

We recommend that DoD further accelerate evaluation efforts mandated by presidential Executive Order 13625,[90] as well as by NDAA 2013 Section 739 and the CAPE initiative to eliminate behavioral-health programs that are ineffective.

Monitoring Quality of Care is one of six strategic initiatives in DoD's Psychological Health and Traumatic Brain Injury portfolio. Quality of care includes training and certification programs across DoD and development of clinical practice guidelines to better inform evidence-based care.[91]

Across the Military Health System, DoD has begun comprehensive efforts[92] to establish standardized quality and outcome measures for mental health care.[93] We recognize the incipient nature of this effort as it is among the first undertakings of its type in mental health care nationwide. We encourage its completion and full implementation.

We are more concerned about the proliferation of service-administered programs that are often billed as essential supports for the community of service members and their families. We understand that base assets for case management, family support, and counseling have always been needed and existed well before the current round of expansions.

In some cases, however, there is potential for a *de facto* mental-health system to be created that does not have reliable tools, such as provider credentialing and peer-review among colleagues, to reliably monitor providers and the flow of Service members into and out of care.

Most troubling is the situation where a patient who presents a safety or security issue is in front of an inadequately trained provider who may not know when a referral to the Military Health System is indicated.[94] DoD must ensure that only mental health providers, trained in their specialties, are entrusted with providing mental health care to Service members.

Recommendation 5.5: Increase commanders' awareness of mental health issues arising within their units, and enhance their ability to help subordinates get the care they need.

Service members frequently seek care for behavioral and mental health issues outside the awareness of their commanders through service-administered programs, VA, community providers, or other sources of treatment outside the Military Health System (MHS).

Some individuals do so to avoid the stigmatizing effect of seeking care, and the potential negative impact on their military careers. Others seek non-MHS treatment options because MHS services are not readily available in their area. In either case, the non-MHS care providers often provide little or no awareness to commanders that their subordinates are being treated, even when those subordinates are engaging in or at serious risk for dangerous behavior.

This problem is exacerbated by a cultural gap between military and civilian providers (at VA and in the community). Whereas military providers have a dual focus on the military mission and the health of patients, providers outside DoD often do not have awareness of these complexities.

We recommend that DoD seek to strengthen commanders' awareness of heath care issues in subordinates, and at the same address the underlying causes of this situation. The initiatives in Recommendations 5.5.1 would help achieve both ends.

Recommendation 5.5.1: Strengthen VA-DoD communication and integration of clinical leadership.

VA and community providers and DoD commanders often do not communicate in a manner that gives commanders sufficient awareness of the challenges facing their subordinates. VA and community providers are obligated to abide by ethics standards that apply to civilian medicine, which are patient-centered while DoD providers have a split fiduciary role that takes the mission into account. This difference manifests in regard to obligations for patient confidentiality, especially when confidentiality might affect the military disposition of an active-duty or reserve service member, or subsequent security risks that member might present.

There are opportunities for better communication with VA providers already available but they are not consistently used. VA and DoD are legally permitted but not required to share health care

information. In reality the problem is multifaceted, with differences manifested on a case-by-case basis, and fundamentally complicated by differing healthcare responsibilities for VA, under Title 38, and DoD, under Title 10.[95]

When service members seek mental health care outside of the MHS, DoD needs to establish better mechanisms and procedures for communications with commanders. Commanders and supervisors need greater awareness of the challenges facing their subordinates and help ensure that those subordinates are getting the care they need.

In conjunction with VA, DoD must ensure broader understanding of policies that allow for sharing of clinical information between DoD and VA.[96] In particular, it must address the execution of the sharing of that information for the ends of continuity of care and fitness for duty in active duty, guard, and reserve personnel.

To address the cultural gap between DoD and non-DoD providers, DoD and VA have jointly developed a course on military culture and mental health.[97] DoD should disseminate this course to the widest possible audience, including civilian providers who treat military patients.

Finally, DoD must review the integration of medical leadership structures in joint DoD/VA facilities and other settings where mental health care is rendered jointly with non-DoD care providers to better address security imperatives related to the health of personnel who work for DoD.

Recommendation 5.6: Further de-stigmatize mental health care treatment within DoD.

While most service members are psychologically healthy, some need help. It is DoD's responsibility to ensure that mental health procedures are implemented in a manner that reduces stigma associated with obtaining care for those who need it, while ensuring fitness for duty in the force and managing medical conditions that might endanger service members.[98]

In the past decade, DoD experienced some procedural difficulties in managing emotionally distressed service members, including in addressing the rare but important need for commanders to compel psychologically impaired service members to mental health evaluation or cases where inpatient hospitalization needed to be pursued involuntarily.[99]

Current law,[100] changed in 2012, mandates that the use of mental health services is considered, whenever possible, to be comparable to the use of other medical and health services. Implicit in this change is the assumption that commanders will act in service members' best interests.

Anecdotally, there is a growing awareness at the unit level of the importance of seeking mental health care without the perception that it will result in negative consequences. An increasing number of commanders and supervisors are setting a positive example by consulting with mental health professionals after deployments or stressful incidents and then discussing the value of their experience with their Service members and employees. The trend in this regard is in the right direction and should be further encouraged and supported.

We recommend that DoD insert specific training about de-stigmatization of mental health visits into leadership courses at every level for NCOs, officers and civilian supervisors. We further recommend that DoD develop policies and programs that recognize leaders and units that are high performers in this area and hold accountable those that fail to meet expectations.

Recommendation 5.7: Speed the transfer of research findings to clinical practice.

DoD and other federal agencies have commissioned multiple lines of research on predicting violence in military populations,[101] as well as extensive studies and surveillance of sexual violence underwritten by DoD's Sexual Assault Prevention and Response Office, comprehensive surveillance of suicide in DoD and VA complemented by numerous lines of study and a joint VA/DoD Suicide Practice Guideline.[102]

DoD should establish mechanisms and infrastructure to help translate the findings of research into practice, so that Service members benefit from care informed by the latest mental health research. A preliminary framework is in place to do so. Under the auspices of the DoD/VA Integrated Mental Health Strategy (Strategic Action #26), DoD and VA are developing and pilot testing a coordinated approach to facilitate the rapid translation of mental health research findings into clinical practice.[103]

The field of implementation science offers several models for establishing and supporting the necessary infrastructure, one of which is currently being jointly pilot tested by DoD and VA through a Joint Incentive Fund (JIF) project.[104]

SECTION SIX
Centralize authority, accountability, and programmatic integration.

Finding: The Department lacks a single office responsible for protecting its workforce and missions from internal and external threats.[105] DoD's security enterprise is a fractured array of organizations, protocols, databases, and directives resulting in inconsistent and sometimes incomplete policy compliance.[106]

Recommendation 6.1: Establish a single authority within DoD for security policy, funding, and accountability. Create a program of record for DoD security.

The Defense Security Enterprise (DSE) 2013 Strategic Plan correctly observed, "The absence of an overarching Department-wide security strategy results in inefficiencies and wasted resources, which in turn leaves DoD's mission vulnerable to internal and external threats."[107]

DoD security is not a "program of record," formally included for funding the Future Years Defense Program (FYDP). Both the Under Secretary of Defense for Policy (USD[P]) and Under Secretary of Defense for Intelligence (USD[I]) make security policy for the Department – but the armed services and other DoD components are separately responsible for funding and executing that policy.

Within the United States, U.S. Northern Command sets force protection levels that guide overall base security postures, but each military service has considerable autonomy in setting specific procedures for access to installations under their purview.[108] Still greater variation in installation access policies, programs and procedures exists across State National Guard facilities, particularly for Army National Guard armories and other assets.

The complex and dispersed nature of DoD security responsibilities suggests the need for a dedicated security office to oversee DoD security programs and funding for issues such as insider threats; installation security; force protection; personnel security; and behavioral security issues such as workplace violence and sexual assault.

Recommendation 6.2: Commission an external review of Defense Security Service (DSS) oversight of the National Industrial Security Program (NISP).

The Defense Security Service (DSS) is the agency that evaluates the offices, factories, and other facilities of the companies that handle classified material in the course of their contract work with the Department of Defense. DSS's work is vital to ensuring that the appropriate protections of classified material are in place throughout the far-flung network of DoD contractors.[109]

Site visits are the primary tool by which DSS carries out its oversight responsibilities.[110] Prior to Alexis's attack, DSS had last conducted a Security Vulnerability Assessment of TEI headquarters in Fort Lauderdale, Florida on December 13, 2011.[111] After the shooting, DSS

conducted a site visit of TEI headquarters and identified several vulnerabilities that resulted in TEI's Facility Security Clearance being invalidated.[112]

DSS's approach is based on a traditional model in which contractors hold classified information at a limited number of facilities. Unfortunately, this model has not kept pace with today's distributed workforce environment, technology proliferation, and continuous-service contracts.

The DSS facility-clearance process needs to be strengthened. It needs to go beyond the security certification of facilities handling classified information. It must include more rigorous oversight of a contracting organization's ability to find and prevent security violations – no matter where they might occur.

DSS needs to make active inquiries into the accountability of supervisors and security officials at contracting organizations. It should have the authority and resources to better evaluate the risks associated with a contracting organization's ability[113] to keep classified material secure.[114]

One crucial weakness in the DSS system is the lack of sufficient consistency or rigor in defining the role of the Facility Security Officer, or FSO. This is the individual who is supposed to be directly responsible for upholding classification standards at each contractor site.

In practice, FSO qualifications vary enormously. Anyone who is a U.S. citizen, an employee at the site, and holds requisite clearance may qualify as an FSO; nothing is needed beyond this. An FSO does not even have to be physically present at the site he or she is supposed to monitor. This can lead to a diluted sense of responsibility for a contractor's security practices.[115]

The clarification and strengthening of the FSO role is an important practical step that would help DSS carry out its mission – a mission that is only becoming more important and more challenging over time.

Recommendation 6.3: The Department of Defense is the adjudicative authority, but not the investigative authority, for granting clearances to DoD personnel. OPM, which conducts personnel security investigations, lacks transparency regarding its systems, processes, quality control programs, and costs.

In 2005, in light of the Intelligence Reform and Terrorism Prevention Act (IRTPA), DoD transferred its investigative responsibilities to OPM. The IRTPA called for security investigations to be consolidated to the greatest extent possible and also introduced strict timelines for the completion of background investigations.[116]

At the time, DSS – which had been handling the investigations for DoD – had an investigative backlog of approximately 270,000 people.[117] OPM now conducts DoD's background investigations, which DoD then adjudicates through a Central Adjudication Facility (CAF).

GAO and DoD have both cited concerns regarding the quality and cost of OPM's background investigations.[118] DoD's primary concern is that in seeking to meet timeliness standards, OPM's

contract investigators reduce investigations to checklists, and provide incomplete investigations for adjudication. DoD pays OPM an estimated $800 million per year for investigative services.

Contributing to OPM's inefficiency is that its information technology systems are underutilized and dated. OPM has elected not to use available tools for monitoring its own quality and is still converting electronic submissions to paper. This prevents automatic cross-checking of information, which may miss inaccuracies or omissions.[119]

Additionally, OPM does not have a way to audit its program, because background investigations are paid for by client agencies, and the current rules bar OPM's inspector general from using any of that money for performance audits.[120] Those rules should be changed. In addition, OPM has not been transparent with DoD about its specific costs transparency for its services.[121]

In June 2013, the Senate Armed Services Committee called on the Secretary of Defense to develop a plan to acquire investigative authority.[122] Conducting investigations in-house will improve synergy between investigation and adjudication to provide a more comprehensive process to grant clearances.[123] It should be noted that all of the information that is normally required for Secret-level clearances is available on computer networks, and fieldwork is not required unless derogatory or questionable information surfaces.

We strongly recommend that DoD determine how to regain the responsibility for its own background investigations. While DoD failed previously to conduct timely investigations, it now has the benefit of learning from that experience and building on OPM's efforts. ODNI has the authority to allow DoD to take back all or part of the investigation process from OPM. DoD will face significant objections from OPM because DoD is by far OPM's largest provider of funds. If DoD receives this responsibility, then it should be prepared to take on this role for all federal organizations.

We recommend that, during the transition period, DoD put pressure on OPM to be more responsive to its demands for quality investigations and more transparency on costs. DoD should immediately deploy case managers and adjudicators to work alongside OPM's Federal Investigative Service to build synergy between investigators and adjudicators to improve the quality of investigations and adjudications.

Recommendation 6.4: The systems and processes for admitting cleared and uncleared personnel through the gates to DoD facilities are insufficient to ensure on-base security.

The Independent Review of the Fort Hood shooting identified practical and necessary improvements to installation security. We recommend timely implementation of those programs.

Currently, each service is implementing its own automated system for its own facilities according to its own timetable and available resources. We recommend the joint approach of the Identity Management Enterprise Services Architecture (IMESA) effort.

The IMESA program links the services' systems with each other, and with non-DoD databases. When fully operable, IMESA will run the name of anyone visiting a DoD facility through a comprehensive check of data sources – such as the Integrated Automated Fingerprint Identification System and the Terrorist Screening Database – that would indicate past criminal behavior, outstanding warrants, and other similar information.

The increased use of automated access control points may eventually lead to a reduced reliance on manpower intensive access control regimes for DoD personnel, and the consolidation of non-DoD visitor access to a reduced number of control points. Both approaches would help the services reduce the cost of manning gates and vetting visitors, while at the same time enhancing the security of personnel working on those installations.

A related issue is the lack of a standardized approach governing access to state National Guard facilities. This challenge is due to the present state of cooperative agreements with communities regarding installation access. Access policies and enforcement protocols vary from state to state, including with regard to regulations on who receives access to National Guard facilities. We recommend that the Secretary direct the National Guard Bureau to coordinate with U.S. Northern Command, other appropriate DoD components, and each state's Adjutant General to establish appropriately standardized access policies and procedures.

APPENDICIES

APPENDIX ONE

Cut the number of Department of Defense employees and contractors holding Secret clearances, and adopt a "just in time" clearance system more tightly linked to need to know.

The challenge of an excessively large "cleared" population

The improvements we recommend to DoD's security-clearance system will initially cost money. We are very mindful, however, that the Department budget is under enormous pressure. To this end, our proposal is to reduce the number of those granted access to classified information and re-set the Department-wide concept of who specifically needs clearances in the first place, so that the system can provide greater scrutiny of those who do ultimately get them.

There are consequences to the growth of cleared personnel. Such a vast input of clearance applications, combined with an emphasis on timeliness in granting clearances, creates conditions for contracted investigators to maximize the quantity of investigations at the expense of quality. One extreme manifestation of this would be the alleged practice of "flushing" or "dumping" background investigations, meaning that case files are passed to the Office of Personnel Management (OPM) at the end of a month without thorough scrutiny.[124]

According to DoD CAF, there are now more than 3.5 million people who are "eligible for Secret access" based on SF-86/NACLC adjudications, some of which are nearly a decade old. Of these eligible individuals, about 1.8 million do not have Secret level access. A large number never will.

Shifting to a "just in time" clearance process

Granting a Secret clearance involves three basic processes – submission, investigation, and adjudication. The specific steps for our proposed "just in time" clearances are as follows:

Submission	• DoD personnel maintain a current SF-86 on Electronic Questionnaires for Investigations Processing (eQIP)[125]
	• Security managers routinely review eQIP for "flags"
	• Based on "need to know," supervisors submit "just in time" clearance request
Investigation	• Investigators complete automated NACLC and follow up as required
	• Investigators interview applicant (if required)
Adjudication	• DoD CAF makes a determination to grant, deny, suspend, or revoke clearance

When an SF-86 is submitted, automated record checks and background investigators expand the investigation.[126] The completed personnel security investigation undergoes a quality review and is then release to the adjudicative agency to render the eligibility determination.[127]

Oversight of contractor clearances

The process for contractors to obtain clearances for their employees working on classified contracts is contained in DoD Manual 5220.22-M, "National Industrial Security Program Manual (NISPOM)." Under the provisions of the NISPOM, it is the company's responsibility to determine the number of positions that require a security clearance, as well as the level of clearance required based on the duties and responsibility of each position. These determinations are made on the basis of contract requirements.

The NISPOM explicitly states, in accordance with Executive Order 12968: "The contractor shall limit requests for [personnel security clearances] to the minimal number of employees necessary for operational efficiency, consistent with contractual obligations. … Requests for PCLs shall not be made to establish 'pools' of cleared employees."[128]

Despite this requirement, pooling is prevalent in the contractor processes. This practice underscores that "just in case" clearances are being submitted to ensure contractor flexibility in meeting new contract requirements. This creates a larger number of cleared personnel than is actually needed, and adds significantly to the government's cost to maintain the system – in terms of unnecessary clearances, periodic reevaluations and more personnel to be considered for continuous evaluation.

At the Secret level, the base price of an investigation for "just in case" clearances costs approximately $260[129] as opposed to a system of "just in time" clearances that would cost only for those investigations needed to meet the contract.

According to the Department of State, which conducts its own reciprocal investigations and adjudications, the SF-86/NACLC process can be completed in about 48 hours at a cost of approximately $300. Full adjudication of a Secret clearance requires approximately five more days and an additional $900.[130]

Oversight of contractor security practices is the responsibility of the DSS, normally executed through periodic inspection visits. However, because of the volume of cleared contractors and facilities, only the largest contractors get the most frequent visits under the DSS Risk assessment strategy. Because TEI was considered a Tier 4 risk, no inspection was planned before the incident at Washington Navy Yard. The most recent inspection of TEI before the Navy Yard shooting was conducted in 2011. In a no-notice inspection visit subsequent to the shooting, conducted in October 2013, TEI was graded as unsatisfactory.

APPENDIX TWO
Use more and better data to investigate clearance seekers.

Information-sharing with state and local law-enforcement agencies

In the course of its 2007 investigation into Aaron Alexis's background to determine his suitability for a Secret clearance, USIS looked into a 2004 incident in which Alexis had been arrested by Seattle police for "malicious mischief."

The courts database indicated Alexis had been arrested, but it did not show the single document from the court record that included arrest details, such as the use of a firearm.[131]

All the Department of the Navy knew at the time it cleared Alexis to receive a Secret clearance was that the charge had been dismissed, and that Alexis had falsely stated on his SF-86 form that he had never been arrested. The 2007 OPM investigation did not reveal that the 2004 incident had involved a firearm.

This was evidently due to the fact that the Seattle Police Department did not release arrest records to background investigators unless the arrest led to a conviction; OPM's work-around procedure was to rely instead on the Washington Statewide District and Municipal Courts database.[132] Those general databases did not have the details of the Seattle Police Report. They reported only the charge for which Alexis was arrested, but did not contain details about the underlying conduct.

Lacking the more detailed police report, OPM and its contractor USIS relied upon the ensuing misleading statements by Alexis in his subject interview, in which he characterized his action as merely the "deflating" of the tires of a construction worker. The investigators never confronted Alexis with the fact that he had used a gun to shoot out a car's tires in what he claimed was a "black out"[133] fueled by anger.

OPM has the ability to compel local police departments to produce such reports. Specifically, 5 USC 9101 states:

> (b)(1) Upon request by the head of a covered agency, criminal justice agencies shall make available criminal history record information regarding individuals under investigation by that covered agency for the purpose of determining eligibility for any of the following: (A) Access to classified information. (B) Assignment to or retention in sensitive national security duties.

DoD, OPM and other relevant agencies should insist on the full enforcement of this longstanding statute, and not simply rely upon statewide databases. While this may initially lengthen the time and complexity of OPM's background investigations and stress IRTPA timeliness requirements, it will ensure that DoD adjudicators have the full range of information before they weigh risks associated with a favorable grant of access.

In March 2010, USD(I) issued a memorandum that provided guidance on adjudicating cases with incomplete investigative reports.[134] In the opening paragraph, the guidance rightly emphasizes the importance of training and experience for adjudicators. However, it also notes, "It is possible to return incomplete investigations to the provider to gather more information, but this adds to investigation costs and time requirements."

This statement illustrates a significant problem that needs to be addressed. Since IRTPA was issued in 2004, the security clearance reform effort has focused on timeliness at the expense of quality control. Adjudicators are under pressure to meet strict timelines, creating a disincentive to return incomplete investigation reports.[135]

Furthermore, the USD(I) guidance does not clearly define the cases in which incomplete or missing information can be accepted based on "sufficient explanation" in the report of investigation. This should be clarified, to include the requirement of copies of original police records.

Expanding database access

One of the strategic goals of the Office of the National Counterintelligence Executive (NCIX) is to "enhance utility of and increase access to an integrated, secure database containing security clearance and suitability investigations and adjudications information."[136]

Executive Order 13467 ("Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information")[137] established the Performance Accountability Council (PAC) chaired by the Deputy Director for Management, Office of Management and Budget. One of the authorities of the council is to establish requirements for enterprise information technology and develop tools and techniques for enhancing background investigations.

There are two systems that OMB's Performance Accountability Council (PAC) has identified in its approach to reform: eApplication and the Automated Records Check. The eApplication system has been developed and has already been fielded to "collect information required for investigations, adjudications, and continuous evaluation through the use of information technology to minimize the need for manual review for data correction, leveraging storage of data to eliminate redundant data collection and support complete, accurate, and timely initiation of requests for investigations."[138]

The Automated Records Check (ARC) will provide an "automated process to run subject data against appropriate government and validated commercial databases to collect, analyze, and validate data, and to flag potential issues, thereby providing cost, consistency, and time efficiencies."[139]

Department of Treasury has numerous databases that could strengthen the financial-investigation part of the security-clearance process. For example, the Office of Foreign Assets Control maintains lists of individuals "owned or controlled by, or acting for or on behalf of, targeted

countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific."[140]

Federal agencies are restricted from taxpayer information under 26 USC 6103, but agencies would be able to access records if the applicant provides consent. Alternatively the Department of Treasury's Offset Program (TOP) could provide an opportunity for federal agencies to perform automated checks on federal debts.[141]

Additionally, DoD has established two tools to assess the quality of investigative and adjudication reports: Rapid Assessment of Incomplete Security Evaluations (RAISE) and the Review of Adjudication Documentation Accuracy and Rationales (RADAR). RAISE was initially going to be used across the executive branch to assess background investigations, but GAO has reported that OPM has chosen not to utilize the RAISE tool and instead plans to develop a different assessment tool. [142]

DoD used RADAR to assess the quality of the adjudicative process in fiscal year 2010, but the program was cancelled in fiscal year 2011 due to funding cuts. The program was restarted in fiscal year 2012, but has yet to yield data that supports specific reforms.[143] If it is determined that these are effective assessment tools, then the Department should continue to use them.

APPENDIX THREE
Implement "continuous evaluation" as part of DoD's personnel security program.

Missed CE opportunities in Alexis's history

Had Alexis been subject to CE, his contact with law enforcement, including an August 2008 arrest for disorderly conduct in Georgia and a September 2010 arrest for unlawfully discharging a firearm in Texas, may have been discovered.

Further, non-judicial punishment (NJP) for unauthorized absence was imposed on Alexis in September 2008 relating to the August arrest in Georgia. A second NJP was imposed in 2009 following a drunk and disorderly incident, but was ultimately set aside and removed from his record. Following the 2010 arrest in Texas involving the discharge of a firearm, the Navy initiated the process to administratively separate Alexis. Instead, Alexis was separated from the Navy in December 2010 under a "reduction in force" program and received an honorable characterization of service with the most favorable re-entry code possible. He also remained eligible for access to classified information.

Without a CE program to collect and evaluate information about his arrests and NJPs, Alexis' security clearance record reflected no concerns about his eligibility for access to classified information and he was granted access to classified information as a DoD contractor.

CE authorities and pilots

EO 12968, as amended, establishes the DNI as the SecEA with the authority to establish CE standards, provides a broad definition of CE, and states that individuals determined eligible for, or who currently have access to, classified information shall be subject to CE. The DNI has begun to develop a CE tool that will provide an enterprise-wide solution across security elements of the federal government, as appropriate.[144] Recognizing CE as a critical element of a robust personnel security program, DoD requested and was granted approval by the DNI to conduct two pilots.

The Army G-2 CE pilot is a phased approach and includes checks of government and commercial databases, including social media. The second pilot is the CECD and is a broader DoD-wide effort that includes a 100,000 person sample of cleared individuals and will run from April through September 2014.

Both pilots are designed to search for information pertaining to the White House's 2005 Adjudicative Guidelines using the ACES, a system developed by the Defense Personnel and Security Research Center, to conduct record checks that dates back to 2005. The CECD pilot builds upon DoD's previous work and includes ACES checks and some additional record checks. Unlike the Army G-2 CE pilot, the CECD pilot does not include checks of social media. The CECD pilot may provide a proof of concept that will enable DoD to build a CE program with the approval of the SecEA. These pilots will provide information on: potential costs, challenges related to data collection, resources, including manpower, required to resolve issues raised by CE, data storage, and information sharing.[145]

APPENDIX FOUR
Establish Threat Management Units to decrease the risk of workplace violence.

Threat management capability

Local threat management teams that are known, trusted, and easily accessible present lower barriers to reporting and are most familiar with the culture at local installations. Using local teams to "identify risk factors, patterns of escalation, and to construct an environment that inhibits or prevents violence,"[146] emphasizes swift identification of potential problems before they result in harm.

These multidisciplinary teams[147] can leverage existing resources such as Case Management Groups (CMGs), which already have expertise in dealing with a specific type of violence, sexual assault. CMGs are mandated by DoDI 6495.02.[148] Triggers for TMU action can include text tips, hotline calls, emails, third-party referrals, or any other form of communication. The threat management team is best positioned to provide recommendations to supervisors or commanders regarding their personnel. These commanders and supervisors can then engage with the individual of concern in the manner that is appropriate to each unique situation.

The Secretary of Defense memorandum on the final recommendations of the DSB Task Force found that "The cost to establish a TMU-like capability and associated training will come from within existing resources and full time equivalent positions currently programmed within DoD Components. The approximate cost to maintain or establish DoD component TMU-like training programs, if DoD Components follow the current Navy TMU manpower and structure, is $1,000,000 per DoD Component for manpower and $100,000 per DoD Component for training and materials over the Future Years Defense Program."[149]

In that same March 2013 memorandum, the Secretary stated support for "the DSB Task Force recommendations to strengthen Departmental policies, programs, and procedures" in certain specific areas, including "[e]stablishing Departmental policy to establish threat management capability."[150]

The accompanying implementation document directs that "[t]he Department will implement a TMU-like capability," with DoD components establishing their own implementation guidance no later than March 2014.[151]

It further states: "There is consensus on the need for a TMU-like capability, however DoD Components agree that it is not necessary to assign specific responsibilities or authorities to a single organization."[152]

We do not concur. Failing to establish a JTMU dilutes responsibility and accountability, and creates unneeded complexity and redundancy in execution. It neglects the joint nature of DoD workplaces, and creates too many opportunities for critical information to fall through the cracks.

The JTMU would be a fused, multi-disciplinary team that would serve as a central clearinghouse, focal point, and reach-back support to local TMUs for commanders and supervisors in the field.

It would support administrative functions, and help manage information exchange. It could facilitate the flow of information on potential threats to the appropriate local TMU, should the threat information emerge from outside the local TMU's area of responsibility. It can also foster information sharing with CE.

While CE and threat management are distinct functions and cover different sets of individuals (those holding or seeking a clearance, and those employed by or working at DoD facilities), they have overlapping concerns. It is essential that both functions can share significant risk-related or derogatory information.

TMUs must broadly leverage available information

Given the stakes, we cannot afford to overlook information regarding indicators of potential threats to our workforce. The technological revolution that has transformed our society in the information age also offers ways to augment self-reports, peer and supervisor reports. Publicly available online information, appropriately and judiciously used, can provide evidence of troubling behavior. [153] "Leakage" of intentions or plans to commit violent acts (mass murders, school and campus shootings, and assassinations of public figures) through electronic communications has been observed. [154] Threat management teams must have access to the information they need to investigate thoroughly.

Managing and sharing crime data

The FBI's Criminal Justice Information Services Division handles the collection and publication of crime data through its Uniform Crime Reporting (UCR) Program. Federal agencies that "routinely" investigate complaints of criminal activity are required to report their data to the FBI for inclusion in the Uniform Crime Reports.[155]

The Bureau of Justice Statistics' National Crime Victimization Survey (NCVS) is a related, complementary effort, providing data on crimes not reported to law enforcement agencies.

DoD has not reported information to the FBI despite federal statutes – on the books since 1988 – requiring it to do so.[156] Moreover, DoD has never made any systematic effort to understand the full extent of unreported victimization within its workforce – even though the NCVS is capable of producing data that would offer a fuller picture of the problem. DoD needs to accelerate efforts to ensure compliance with federal law.

Peer reporting benefits

With regard to shifting from self-reporting to peer reporting, there is an acknowledgement that peer reporting may have success in recognizing warning signs. According to the FBI Behavioral Analysis Unit, "Many active shooters display pre-attack behaviors which, if recognized, can lead to the disruption of a planned attack." They further state "human bystanders generally represent the greatest opportunity for the detection and recognition of an active shooter prior to his or her attack." [157] While shifting to a system of peer reporting, CE will greatly increase the likelihood of detection of behavior or actions of concern that may allow intervention before a tragedy occurs.

APPENDIX FIVE
Strengthen mental health care.

Aaron Alexis, who engaged in an attack on the Washington Navy Yard that he may well have understood would result on his death, struggled with performance, behavior and impulse control throughout his short military career. These struggles were witnessed by commanders, supervisors and public safety officers. Alexis was not separated, nor was he referred to definitive care, on balance, for these problems. Military training about the management of imminent or potential danger by aberrantly acting individuals did not lead to action. A mental health system that had sustained double-digit growth for a decade was not called upon to provide guidance to commanders or render assistance to this troubled individual.

None of the systems that could have addressed problems were used to intervene effectively. This incident presents an opportunity to examine the resources that might have assisted Aaron Alexis and his commanders while he was on active duty. These resources can be better marshaled to serve future military personnel and leaders.

Aaron Alexis's behavioral problems predated his military service, persisted while he was an entry-level recruit, continued under the watch of two squadron commanders, and were lost to history upon discharge. Some of that behavior continued to manifest itself during his time as a DoD contractor. This includes weapons incidents that occurred before and during his military service. Alexis came to the Navy Yard on September 16 with a history of behavior suggestive of serious mental-health concerns and a propensity toward violence.

Furthermore, Alexis showed several behaviors that might have provided an impetus for him to seek mental health care or be referred to such care. Yet no such care was sought or offered. Among other issues, Alexis appears to have had an alcohol abuse problem. While he was on active-duty, Aaron Alexis also obtained line-administered Alcohol AWARE training, once while in recruit training and once after an alleged alcohol-related incident.[158]

The failure to address Alexis' mental health and conduct problems meant that subsequent commanders and supervisors knew precious little about Alexis' behavioral profile. Lacking adequate records to base decisions on, leaders made decisions regarding Alexis that did not, in the end, serve DoD or Alexis.

In the weeks leading up to the shooting, Alexis displayed psychotic behavior[159] at a government facility with active-duty employees, who are required by DoD instruction[160] to be trained in the recognition of imminent dangerousness based on behavior or mental state, to civilian police officers in the town adjacent to the base, to coworkers, and most importantly, to a supervisor in a contracting firm DoD retained for work to further DoD's mission. But he was not referred for a psychiatric evaluation and mental health treatment such as hospitalization, and stabilization was not provided. It is possible that such care could have diverted the trajectory of later events[161].

The Department of Defense had several opportunities to recognize that Alexis was a troubled individual – one who needed help and might pose a hazard to himself or others if past patterns of

behavior were allowed to continue unchecked, if his mental-health condition continued to go unrecognized and untreated, and his behavior problems remained unresolved.

DoD's failure to adequately address Alexis' difficulties is all the more notable in light of the general increase in the military's awareness and acknowledgment of psychological challenges in the broader force during the period of his military service, and much closer alignment with VA in regard to strategies pertaining to management of mental health in service members and Veterans. Alexis, like many service members and veterans, availed himself of care in the Military Health System (MHS) and in the Department of Veterans Affairs (VA) medical system.

Over the past decade, significant efforts have been focused on increasing the availability of mental health care for active-duty service members and their families, destigmatizing that care, and ensuring that care is available during transitions in their lives. These efforts were well-founded. Despite considerable efforts and policy emphasis within DoD,[162] there will always be more individuals experiencing mental health concerns than are receiving care for those difficulties. This is not a problem in America alone; it exists across Western military forces.[163]

Moreover, the high tempo of military operations since 2001 has resulted in a large increase in needed mental-health services for service members. Balances between supply and demand have at times been precarious—the need, for instance, for mission-oriented mental-health care could easily outstrip the supply of military mental-health services in certain catchment areas with a significant flux of active duty Service members stemming from deployments.

Recognizing the huge investment made in mental health services over the last decade, recent mandates from the White House[164] have sought to foster mental health and substance abuse treatment programs that produce the best impacts on quality and outcomes.

Programs designed for service members, but outside of the Military Health System (MHS) may have emerged in an effort to meet the needs of today's service members. However, they have in places supplanted the time-honored role of military providers as fiduciary agents who balance command and mission imperatives, and they may not provide the most effective care.

An embedded-care model of mental health provision allows providers to balance their treatment imperatives with their fiduciary role to serve the command,[165] particularly with regard to patient disposition, and ultimately, force protection. Leveraging the knowledge of military providers, who are already inured to the split responsibilities of operational medicine[166] best balances the ethical need to act in a patient's best interest with the needs of the mission.[167]

Commanders have a recognized "need to know" about dangerous behavior and mental health issues that have the potential to disrupt good order and discipline; personnel safety and security imperatives; or other aspects of the mission. Likewise, Commanders should always have access to providers who are well-versed in the administrative and personnel-related aspects of military mental health care, including management of risks stemming from aggression, sexual violence, and suicidal or homicidal behavior, and the nuances of separating conduct problems that stem from substance abuse or character pathology from the suffering that stems from other forms of mental illness.

APPENDIX SIX
Centralize authority, accountability, and programmatic integration.

Establish a single authority within DoD for security policy, funding and accountability.

DoD needs a single office that has the institutional authority to implement the policies that would prevent security failures. In October 2012, the Department created the Defense Security Enterprise (DSE) to provide governance for the strategic administration and policy coordination of workforce, information, and installation security.

While the DSE effort is well-intentioned, it does not adequately address the lack of centralized leadership needed to manage and advocate for a strategic, coordinated approach to DoD security.[168] Absent a program of record managed by a consolidated senior decision making authority, no one is really responsible for strategic planning for security. No one is at the table to advocate for it when the money decisions get made.

The services maintain and operate their installations, with access procedures that can vary widely from location to location. Meanwhile, personnel security, information security, and force-protection programs are managed by a spectrum of DoD offices, including the Under Secretaries of Defense for Intelligence; Policy; Personnel and Readiness; and Acquisition, Technology, and Logistics, as well as the Chief Information Officer.

This complex management structure creates untenable responsibility, management, and oversight seams and has slowed the ability of the Department to implement physical-security and access reforms. For example, the development of a draft directive on insider threat policy was reassigned from the offices of USD(P) to USD(I) and back several times.[169]

The central question here, of course, is where – and how high – to place this office in the Pentagon's organizational chart. Such a centralized security authority must reside at a level high enough to protect the security function as a program of record within DoD, and to advocate for workforce and installation security funding in the Program Objective Memorandum (POM) process that guides resource-allocation decisions every year. At a minimum, this new office would need the authority to approve the security budgets of the armed services and other DoD components.

We have identified five options for creating such an authority:

- Designate the Deputy Chief Management Officer (DCMO) as this authority, building upon the integration, process transformation, and coordination across the DoD and other government agencies inherent in the role.
- The authority could be designated within the OUSD(I), where the security functions already exist.
- Create a new military command – U.S. Security Command – along the lines of U.S. Special Operations Command or U.S Cyber Command.
- Establish a new Office of the Under Secretary of Defense for Security OUSD(S), which would require congressional action.

- The Secretary of Defense could establish a sub-unified command headed by a three-star officer within U.S. Northern Command. Each of these options and others would require further study with regard to costs and requirements for Executive or Legislative action.

Oversight by Defense Security Service (DSS)

Prior to Alexis's attack, DSS had last conducted a Security Vulnerability Assessment of TEI headquarters in Fort Lauderdale, Florida on December 13, 2011. It is not unusual that DSS would not conduct more frequent site visits as DSS only has several hundred field investigators to visit more than 13,000 facilities located nationwide.[170] TEI was an "access elsewhere" facility, meaning that TEI employees who worked with classified material only did so at other work sites including government facilities such as the Washington Navy Yard.[171] The DSS prioritization process—which must focus its site visits on facilities that face the greatest risks of vulnerabilities to classified information—ranked TEI in the lowest tier of risk.

TEI failed to recognize the seriousness of Alexis' August 7 and 8 episode in Newport, Rhode Island. Despite taking the steps of removing Alexis' access to classified information temporarily, they failed to take appropriate steps to ensure Alexis was able to resume his duties at TEI. TEI further failed to report this to DSS.[172]

After the September 16 attack, DSS conducted a site visit of TEI headquarters and identified several vulnerabilities that resulted in TEI's Facility Security Clearance being invalidated and TEI being deemed ineligible from accepting new or additional classified contract work.[173] Had the attack not occurred and the October 2013 assessment not been conducted, it is likely that DSS would not have visited TEI for as long as another year. Given the nature of the problems uncovered at an organization that is assessed to be low-risk, this level of oversight is not enough.

An assessment needs to be conducted on how DSS prioritizes its limited resources to provide effective oversight. This assessment should include outside experts and involve a top to bottom review of processes, resources, and authorities. The review needs to consider the adequacy of existing IT infrastructure and manpower and assess what is appropriate given the state of the modern national security industrial program and current threats. The review should attempt to create a new, more real-time oversight approach as opposed to enhancing capability to conduct more of the existing procedures.

We recommend that our proposed external review of DSS include an assessment of contractor compliance with National Industrial Security Program Manual (NISPOM) reporting responsibilities regarding adverse information on contractors with security clearances. This should include how adverse information is updated in JPAS.

Reverting authority and responsibility for conducting investigations back to DoD.

Currently, DoD spends approximately $800 million a year on background investigations, yet it has missed many opportunities to identify individuals – including Aaron Alexis and Edward Snowden – who have presented obvious dangers to personnel or classified information.[174]

While OPM has reduced the investigation backlog and now meets the official timeliness standards for initial clearances,[175] GAO and DoD have both cited "quality" issues with OPM's background investigations.[176]

OPM has relied heavily on U.S. Investigations Services (USIS) to carry out investigations for government agencies, including DoD. (Under the current system, DoD adjudicates the cases that OPM has investigated on its behalf.)

USIS is presently under grand-jury investigation for the alleged mishandling of this high responsibility, including through the practice of "dumping" (also sometimes referred to as "flushing"), or giving quick approvals without due scrutiny in order to cash in on incentives for completing a certain number of cases. USIS handled the screening of both Aaron Alexis and Edward Snowden as USIS provides the lion's share of background investigations on behalf of OPM.[177]

OPM asserts that it provides high-quality investigations meeting the federal investigative standards and that DoD adjudicators have not returned cases "to OPM … for quality deficiencies."[178]

This disagreement over quality is indicative of a critical problem: the failure of DoD and OPM to communicate. There is a lack of a regular dialog and clear expectations between OPM and DoD perpetuated by mutual animosity and misunderstanding.

In June 2013, the Senate Armed Services Committee issued a recommendation, "that would require major reform of the personnel security clearance investigation, adjudication, and transfer processes to improve security and reduce costs."[179] This legislation calls on the Director of Cost Assessment and Program Evaluation (CAPE) to assess OPM's personnel security investigations and calls on the Secretary to develop a plan to acquire investigative authority.[180]

The State Department and many intelligence organizations manage their own investigations and adjudicate their own clearances to avoid interagency challenges.[181]

The DoD CAF should own the investigative and adjudicative processes. Similar to the State Department, DoD CAF should hire experienced investigation case managers to oversee contract investigators. The case managers must also be trained to understand the adjudication process. This will build synergy between the investigators, case managers, and adjudicators that has proven successful at the State Department and throughout the Intelligence Community. This will also eliminate interagency challenges between OPM and DoD. Further, the new DoD chief security official recommended earlier in this Section would provide valuable unified leadership.

As discussed in Appendix Two, DoD has developed tools to measure the quality of investigations and adjudications, Rapid Assessment of Incomplete Security Evaluations (RAISE) and Review of Adjudication Documentation Accuracy and Rationales (RADAR). These tools need to be enhanced and implemented to generate consistent data capable of identifying quality trends.

As DoD resumes conducting its own personal security investigations, DoD must also consider whether or not DoD would absorb the background investigation requirements from other members of the community who currently pay OPM for this service. Given that DoD is approximately three-quarters of OPM's investigation workload it may be cost effective for DoD to provide the background investigations for the remaining quarter.[182]

Improving access control at the gates for cleared and uncleared personnel.

- DoD is taking steps to implement recommendations from the Independent Review of the Fort Hood Shootings. OUSD(P&R) is coordinating a draft DoDI 1438.ff, "DoD Workplace Violence Prevention and Response"[183] with a goal of issuance in December 2013.
- The Naval Criminal Investigative Service is enhancing the DoD Defense Law Enforcement Defense Data Exchange (D-DEx)[184] in furtherance of Fort Hood Recommendation 2.10.[185] While this effort is well advanced, budget cuts and the timely availability of funds have slowed the incorporation of all DoD law enforcement elements and the inter-connection with key local jurisdictions. A modest amount of funding, enhanced level of effort, and the increased participation of the remaining DoD law enforcement agencies could address outstanding gaps.[186]
- OUSD(I) is in the process of implementing Fort Hood Recommendations 3.7 and 3.9 concerning the consolidation of access control programs and information sharing regarding personnel and vehicles registered on installations, debarment lists, and other relevant information related to access screening.[187]

Congress required the Secretary of Defense to develop minimum access standards to all DoD installations.[188] To this end, USD(I) issued Directive-Type Memorandum (DTM) 09-012, "Interim Policy Guidance for DoD Physical Access Control." This DTM established minimum standards for controlling physical access to facilities but allowed installations to delay implementation of electronic access control measures "when funding becomes available."[189]

Thus, each Service is implementing its own automated system for its own facilities according to its own timetable and available resources.[190] Given the increasingly joint nature of DoD installations we recommend the joint approach of the Identity Management Enterprise Services Architecture (IMESA) effort.

IMESA has only been tested with DoD personnel. However, any viable access system must also be able to screen non-DoD personnel. Bringing IMESA up to this level raises both technical and policy challenges, including privacy considerations.

To make access control effective, IMESA needs to be able to sift through the relevant databases quickly – a task that becomes even more challenging with the added requirement of screening individuals from outside the Department. Quick searching in the vast repository of federal criminal information may require DoD servers to mirror certain elements of the data maintained by non-DoD sources.

APPENDIX SEVEN
Letter of Appointment and Terms of Reference for the Independent Review.

SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

SEP 30 2013

MEMORANDUM FOR THE HONORABLE PAUL STOCKTON
ADMIRAL ERIC OLSON, USN (RET)

SUBJECT: Department of Defense Independent Review of the Washington Navy Yard Shooting

Thank you for agreeing to conduct the Department of Defense (DoD) Independent Review ("Review") of the shooting at the Washington Navy Yard on September 16, 2013. I ask that you conduct the Review to identify and recommend actions that address gaps or deficiencies in DoD programs, policies, and procedures regarding security at DoD installations and the granting and renewing of security clearances for DoD employees and contractor personnel. Your work is to be conducted separately from the internal review I asked the Deputy Secretary of Defense to lead.

Your primary objective is to determine whether there are weaknesses in DoD programs, policies, or procedures regarding physical security at DoD installations and the security clearance and reinvestigation process that can be strengthened to prevent a similar tragedy in the future.

The President has directed the Office of Management and Budget, in coordination with the Office of the Director of National Intelligence and the Office of Personnel Management, to conduct a government-wide review into the oversight, nature, and implementation of security and suitability standards for federal employees and contractors. In addition, the Federal Bureau of Investigation is leading an investigation into the incident. Your Review should not interfere with either of these activities.

I hereby appoint you as employees of the DoD pursuant to title 5, U.S.C., section 9903. You are to have access to all relevant DoD investigations into this incident and other DoD information, unless prohibited by law. Should you determine the need to travel or conduct outside interviews, the Director of Administration and Management will make appropriate arrangements.

You are to begin the Review on September 30, 2013. A report, including findings and recommendations, should be provided to me and the Deputy Secretary by November 15, 2013. You may identify follow-on issues which may require further study. I have also asked the Deputy Secretary to synthesize your findings with those that emerge from the internal DoD review and to consolidate key recommendations from those two studies into a final report to be provided to me by December 20, 2013.

You shall provide a full briefing to me on the findings of your report prior to the aforementioned process by the Deputy Secretary to synthesize findings that emerge from the internal DoD review. In addition to the briefing, you may opt to present your findings in writing

OSD011576-13

directly to me. At any time in the process you may bring matters you deem appropriate directly to the attention of the Deputy Secretary or me.

Following my review of the final report, I will direct relevant Services and DoD Agencies to implement new security measures or actions, as appropriate.

All DoD Components will fully cooperate in the execution of your Review and will provide support and timely responses to all requests for relevant information, detailed personnel, or other support.

By copy of this memorandum, I direct the Director of Administration and Management to secure and coordinate the necessary technical, administrative, and legal support for your Review from DoD Components. Furthermore, the Director of Administration and Management will coordinate administrative, facilities, and other support from the Department, as required.

On behalf of the men and women of the Department and their families, thank you for your willingness to serve once again the Department, the Nation, and the American people.

Attachment:
Terms of Reference

cc:
Secretaries of the Military Departments
Chairman of the Joint Chiefs of Staff
Under Secretaries of Defense
General Counsel of the Department of Defense
Inspector General of the Department of Defense
Assistant Secretaries of Defense
Director, Administration and Management

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 parallel 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 DoN'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 of hostilities) 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 of DoD 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 findings 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 pertinent 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 of Defense by November 15, 2013. Under supervision of the 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 these efforts.

- 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 EIGHT
A timeline of the events leading to September 16, 2013

This brief summary of events helps set the context necessary to assess some of the important flaws in our security systems, and this review's recommendations for addressing them.

This timeline was developed from the following sources:

- Department of the Navy release, "Timeline of events Concerning Aaron Alexis," 20 September 2013.
- Department of Veterans Affairs, News Release, 18 September 2013.
- FBI Public Information Office, "Law Enforcement Shares Finding of the Investigation into the Washington Navy Yard Shootings," 25 September 2013.
- Newport Police Department Incident Report 13-17827-OF, 17 September, 2013.
- Associated Press: The Big Story, "Navy Timeline of Navy Yard Shooter in Reserve," 23 September 2013.
- Fox, Maggie. "VA Aaron Alexis never sought mental health treatment." NBC News, 19 September 2013.
- Lewis, Paul. "Aaron Alexis: police piece together picture of man 'as normal as you or me." The Guardian, 20 September 2013.
- Vogel, Steve, Horwitz, Sari and Fahrenthold, David A. "Navy Yard gunman Aaron Alexis told VA doctors he was not thinking of harming others." Washington Post, 18 September 18 2013.

Relevant pre-service and active duty events:

On June 3, 2004, approximately three years prior to his enlistment in the U.S. Navy, Aaron Alexis was arrested in Seattle following an incident in which he allegedly shot the tires out of a construction worker's vehicle following an argument.

On May 5, 2007, Alexis enlisted in the Navy Reserve at the New York Military Entrance Processing Station in Brooklyn.

During his personnel security investigation, OPM checked on the 2004 Seattle shooting incident with the King County court system, whose records did not include police reports of the shooting. There was no reference to gunplay in OPM's final report to the Department of Navy Central Adjudication Facility (DONCAF). Instead, the report simply states that Alexis "deflated the tires on a construction worker's vehicle."

OPM closed its security investigation of Aaron Alexis on August 4, 2007. Three months later, Alexis graduated from recruit training at Naval Station Great Lakes, Ill. On December 15, 2007, he graduated from Aviation Electrician's Mate "A" School and transferred to Fleet Logistics Support Squadron 46 in Atlanta. Alexis remained with this unit for the remainder of his brief naval career.

On March 11, 2008, DONCAF, upon review of the OPM investigation, determined Alexis was eligible for a Secret-level security clearance, with a single caution – Alexis had an unfavorable credit history.

At the time of Alexis's investigation and adjudication, a Secret-level clearance was good for a full decade. In 2012, the Directors of National Intelligence and OPM ordered Secret periodic investigations to be completed every five years, a requirement that is still not in effect and isn't expected to enter into force until 2015.

On August 10, 2008, Alexis was arrested for disorderly conduct outside a nightclub in suburban Atlanta. He spent the night in a DeKalb County jail, and a month later his commanding officer imposed non-judicial punishment (NJP) on him for unauthorized absence related to the incident, imposed a forfeiture of half his pay for two months and a pay-grade reduction; both of these disciplinary measures were suspended.

The record of this NJP appears in Alexis's service record from this date forward. However, it was never logged into the Joint Personnel Adjudication System (JPAS), a system relied upon by the Department of Defense Central Adjudicative Facilities (DODCAF) to record information affecting individual eligibility to access classified information. This was not unusual; there is no strict requirement for reporting such incidents into these databases.

On July 12, 2009, the commanding officer imposed a second NJP on Alexis for being drunk and disorderly, following an incident in which Alexis jumped from a staircase and broke his ankle while reportedly intoxicated.

There was no police involvement in the matter. Alexis appealed this NJP. The month following the incident, there was a change of command at the squadron. The appeal authority in Alexis's case, a Naval Air Force Reserve commander, reviewed the appeal and concluded that there was no physical evidence that Alexis had been drunk at the time of the stairwell incident. The reserve commander made clear that the NJP would therefore be set aside.

On December 3, 2009, the recently installed commanding officer set aside the NJP, and it was removed from Alexis's record. This is consistent with the standard Navy practice of cleansing sailors' records of any NJP that is set aside.

Due to base realignment, the squadron relocated to Fort Worth, Texas, in 2009. On September 5, 2010, Alexis was arrested in that city for having discharged a firearm in his home the previous day. According to law enforcement documents, Alexis said he had accidentally discharged the firearm while cleaning it. No charges were filed. However, following this latest incident,

Alexis's commanding officer began the official process of getting the troubled sailor out of the Navy.

Toward this end, the squadron's legal officer prepared an administrative separation document that he intended to forward to Navy Personnel Command. However, after Alexis's case was dropped without so much as a filing of charges, this paper trail stopped cold – the legal officer's letter was not signed, dated or sent. In the eventual absence of any formal charges in the Fort Worth gun incident, it was unlikely that Alexis could have been forced out of the Navy against his will.

As it turned out, Alexis would leave the military on his own volition. On December 2, 2010, he requested separation from the Navy in accordance with a "reduction in force" program allowing sailors to request an early release. Navy Personnel Command approved Alexis's request seven days later.

It's worth noting that, as of this moment in the chronology, Aaron Alexis's official record was relatively clean. The troubling string of firearms incidents and other brushes with the law had left no blemish on his dossier, aside from the single NJP arising from the Atlanta nightclub incident.

His Navy file included no record of any civilian convictions, and no security incidents involving Alexis – not even the NJP from the Atlanta incident – had been reported in JPAS or DODCAF.

On January 31, 2011, Aaron Alexis received an honorable discharge from the Navy. What is more, he garnered a Reentry Code of RE-1 – the most favorable code available, and one that would facilitate any future attempts to rejoin the Navy.

However, Alexis would not actually obtain a Secret clearance until he joined The Experts, the firm for which he was working at the time of the Navy Yard shooting.

Events subsequent to Navy active duty

The following month, Alexis received a Navy Reserve Identification and Privilege card. It was not set to expire until May 4, 2015. This card would permit access onto Navy bases, consistent with Alexis's post-discharge status as a member of the Navy's Individual Ready Reserve (IRR).

On February 1, 2011 Alexis enrolled in Veterans Affairs health care. On February 12 he was granted a 20 percent disability rating (orthopedic issues) by the VA.

In September 2012, Alexis began working on the Navy-Marine Corps computer system, on a contract held by Florida-based company, The Experts Inc.

Little is known of the following 11 months of Alexis's life. By early August 2013, however, his pattern of erratic behavior had resumed.

On August 7, Newport Police were dispatched to the Marriott Hotel, room 405 to respond to a harassment report of a resident who was making noises and disturbing patrons. Upon arrival, the

police officers spoke with Alexis, who went on to explain that "while getting onto his flight from Virginia to Rhode Island he got into a verbal altercation with an unknown party in the airport . . . believes that the individual that he got into an argument with has sent 3 people to follow him and keep him awake by talking to him and sending vibrations into his body."

He went on to explain he first heard them talking to him through a wall while at the Residence Inn in Middletown at which point he packed up and went to a hotel on the Navy base where he heard the same voices talking to him. He then moved to his third hotel and is currently staying at the Marriott. He stated that the individuals are using a "microwave machine" to send vibrations which penetrate his body so he cannot fall asleep. He clearly stated that he does not have a history of mental illness in his family and has never had a mental episode. The police officer asked him to stay away from the individuals and notify Newport Police Department if they attempt to make contact again.

Later on August 7, the responding officer made contact with on duty Naval Station Police and faxed a copy of the police report. No further action was taken.

On August 23, Alexis visited the emergency room at the VA Medical Center in Providence, R.I., complaining of insomnia. After a medical examination he was given a small amount of Trazodone, a generic anti-depressant that is widely prescribed for sleeplessness. He was also instructed to follow up with a primary-care provider.

On August 28, Alexis went to the emergency room at the VA medical Center in Washington D.C. complaining again of insomnia. He was given a small refill of Trazodone and was again asked to follow up with a primary-care provider. Alexis had been in the VA's medical records for a couple of years; he had initially enrolled in VA health care in February 2011, but either cancelled or failed to show up for scheduled primary-care appointments and claims evaluations.

On September 14, Alexis visited Sharpshooters, a gun store in an industrial park in Lorton, Va. He used a rented rifle for target practice and then purchased a pump-action Remington 870 shotgun and 24 shells for $419. At some point, he used a hacksaw to shorten the barrel of the gun and stock.

Events of September 16

On September 16, Alexis drove to the Navy Yard in a rented car and used his security pass to enter Building 197. He entered the building and proceeded to the fourth floor bathroom.

At 8:15 a.m., Alexis crossed the hallway into the 4 West area of Building 197 carrying a shotgun and immediately started "hunting people to shoot" according to James B. Comey, Director of the FBI.

At 8:16 a.m., Alexis shot the first victim in the 4 West Area of Building 197.

At 8:17 a.m., the first frantic phone calls to police were received about shots at Building 197.

The FBI now has a provisional idea of the route Alexis took. He evidently started on the fourth floor, and then moved to the third floor. Before entering the atrium, he shot a security guard and took the handgun from the guard's holster. The majority of Alexis's victims were shot on the third and fourth floors.

At approximately 8:25 a.m., the first police armed response unit entered the building within several minutes of the first 911 call. Eyewitness accounts state that there were multiple firefights, with a pause in gunfire that lasted between 10 and 25 minutes.

At 9:25 a.m., law enforcement officers shot and killed Alexis on the third floor. Alexis had slain 12 people and wounded three others.

APPENDIX NINE
The evolving insider threat

Insider Threat Defined

In October 2011, President Obama issued an executive order that defined an insider threat as a person who "use[s] his/her 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."[191]

While acts of workplace violence are not specifically mentioned in this definition, they are a part of the broader range of threats within DoD facilities, and represent a major challenge. In 2011, one in five victims of workplace homicide was a government employee, and one in 115 government employees (federal, state or local) was a victim of workplace violence.[192] As the Navy Yard shootings and other tragic events have demonstrated, DoD is not immune. DoD can and must reduce the risk of such tragedies occurring in the future.

Insiders who pose a threat may be motivated by ideological beliefs, criminal intent, or a wide range of other factors, including mental illness. As such, we recommend leveraging the Threat Management Units (TMU's discussed in Recommendation Four) to assess a broad spectrum of behavior and motivations when addressing the potential risk for violence posed by an individual. Moreover, insiders who intend or commit violence are only part of the challenge within our installations. This appendix takes take a more holistic view, and highlights several evolving threats of special concern. These specific categories of insider threats deserve attention as the Department considers new security initiatives.

Homegrown Violent Extremism (HVE) and the Evolution of Al Qaeda

The FBI has found that homegrown violent extremism represents a rapidly evolving threat in which "individuals inside the United States become radicalized and motivated to conduct attacks against the Homeland."[193] Central Intelligence Agency Director John Brennan has said the evolving al Qaeda threat now includes "individuals, sometimes with little or no direct physical contact with al Qaeda, who have succumbed to its hateful ideology and who have engaged in, or facilitated, terrorist activities here in the United States."[194] The Boston bombers Dzokhar and Tamerlan Tsarnaev offer a prime example of HVE.

While the brothers acted alone, they were not entirely without assistance. They learned how to make bombs from the *Inspire* magazine article: "Make a bomb in the kitchen of your Mom."[195] This was no accident. *Inspire* is published in an effort to recruit, motivate and remotely train HVEs. The issue published after the Boston Marathon bombings praised the Tsarnaev brothers: "The Boston Bombings have uncovered the capabilities of the Muslim youth, they have revealed the power of a Lone Jihad operation."[196] Shortly after the Navy Yard shooting began, some jihadist sympathizers took to Twitter to declare their hopes that the attack had been motivated by Islamist extremism. [197] Some of these messages used the hashtag "al Qaeda."[198]

This effort to recruit HVEs represents a broader shift in the al Qaeda strategy. As the United States continues to destroy and disrupt al Qaeda's ability to plan, train for and execute large scale operations such as 9/11, al Qaeda has increasingly turned to franchise operations, leveraging the individual jihad and encouraging HVEs.[199] As the core leadership of al Qaeda is degraded, the organization and its increasingly diffuse and capable affiliates will still seek to carry out attacks inside the United States and across Western interests. [200] The broader al-Qaeda movement is highly adaptive, and is placing "greater emphasis on smaller, simpler plots that are easy to carry out."[201]

Espionage

Overall, the loss of information poses an immense threat to United States national security. The FBI estimates each year foreign intelligence services and their collectors become more creative and sophisticated in their methods to steal innovative technology.[202] Traditional military espionage the likes of Robert Phillip Hanssen, a former FBI agent who provided highly classified national-security information to Russia and the former Soviet Union, is only one part of a coordinated espionage effort.[203] Like the Al Qaeda threat, espionage has also evolved with the times. Economic and industrial espionage is a growing threat. Last March, Director of the Federal Bureau of Investigation Robert Mueller III stated the FBI estimated that "pending economic espionage cases cost the American economy more than $13 billion. In the last four years, the number of arrests the FBI has made associated with economic espionage has doubled; indictments have increased five-fold; and convictions have risen eight-fold."[204] Counterintelligence must remain a core focus of DoD personnel and installation security, and will continue to require specialized policies and programs.

The Malicious Cyber Insider Threat

The evolution of the insider must also consider the access now available to any user of DoD information systems, whether an ordinary user with basic permissions, or a privileged user with additional accesses and permissions that permit more powerful manipulations of the system up to "unrestricted access to the entire system."[205] Malicious insiders may exceed or misuse their access to take information, or compromise the function or integrity of systems. Independent of their motivations, insider threats can take advantage technology and access to information systems to cause tremendous harm to national security. Edward Snowden is a fugitive American computer specialist who disclosed stolen Top Secret information on United States and British mass-surveillance programs while employed to support government information systems.[206] Chelsea Manning – formerly U.S Army Specialist Bradley Manning – also used access to classified systems to download and later disclose sensitive information. The unintended consequences of post 9/11 connectivity and the increased reliance on technology access have left the United States vulnerable to the damage that a Snowden or Manning can inflict.

This presents a paradox: While our national security depends on access to large amounts of information to "connect the dots," perform involved analyses, or manage complex activities, these same information systems pose a vulnerability. In the absence of robust cyber security, a single insider could steal more information in a day electronically than could have been physically smuggled out of a facility in a year, or could crash a system relied upon by thousands.

Information assurance and cyber security policies and practices must stay abreast of changing risks.

While exhaustive cyber specific recommendations lie beyond the scope of this report, we have framed our recommendations to be broad and useful against the broader definition of the evolving insider threat.

GLOSSARY

Access: The ability and opportunity to obtain knowledge of classified information. Access presumes favorable adjudication eligibility.

Access Control: A procedure to identify and/or admit personnel with proper security clearance and required access approval(s) to information or facilities using physical, electronic, and/or human controls.

Access Eligibility Determination: A formal determination that a person meets the personnel security requirements for access to a specified type or types of classified information.

Adjudication: Evaluation of personnel security investigations and other relevant information to determine if it is clearly consistent with the interests of national security for persons to be granted or retain eligibility for access to classified information, and continue to hold positions requiring a trustworthiness decision.

Adverse Information: Any information that adversely reflects on the integrity or character of a cleared employee that suggests his or her ability to safeguard classified information may be impaired, or that his or her access to classified information may not clearly be in the interest of national security. See also *derogatory information*.

Clearance: An administrative authorization for access to National Security Information (NSI) up to a stated classification level (e.g., TOP SECRET, SECRET, CONFIDENTIAL).

Continuous Evaluation (CE): Pursuant to Executive Order 13467, CE is defined as "reviewing the background of an individual who has been determined to be eligible for access to classified information or eligible to hold a sensitive position (including additional or new checks of commercial databases, government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements of eligibility."

Derogatory Information: Information that could adversely reflect on a person's character, trustworthiness, loyalty, or reliability (e.g., a history of drug abuse or criminal activity). Information that is unrelated to character may be of adjudicative significance, but not derogatory information (e.g., foreign connections).

Eligibility: A determination that a person meets personnel security standards for access to program material. See also *adjudication*.

Financial Disclosure: A personnel security requirement for clearance processing that requires subjects to provide information regarding their total financial situation (e.g., assets, liabilities, and indebtedness).

Interim Security Clearance: A security clearance based on the completion of minimum investigative requirements granted on a temporary basis, pending the completion of the full investigative requirements.

Joint Personnel Adjudication System (JPAS): The centralized DoD database of standardized personnel security processes that virtually consolidates the DoD Central Adjudication facilities (CAFs) by offering real time information concerning clearances, access, and investigative statuses to authorized DoD security

personnel and other interfacing organizations (such as DSS, DMDC, Defense Civilian Personnel Management (DCPM), and the Air Force Personnel Center (AFPC)).

National Agency Check (NAC): A Personnel Security Investigation (PSI) consisting of a records review of certain national agencies, including a technical fingerprint search of the files of the Federal Bureau of Investigation.

National Agency Check with Local Agency Checks and Credit Check (NAC-LC): A Personnel Security Investigation (PSI) covering the past 5-7 years and consisting of a National Agency Check (NAC), financial review, verification of date and place of birth, and Local Agency Checks (LACs).

National Security Position: 5 CFR 732.102 defines such positions as those involving activities of the Government concerned with the protection of the Nation from foreign aggression or espionage, including development of defense plans or policies, intelligence or counterintelligence activities, and related activities concerned with the preservation of the military strength of the United States, including regular use of, or access to, classified information.

Need for Access: A determination that an employee requires access to a particular level of classified information in order to perform or assist in a lawful and authorized Governmental function.

Need-to-Know: A determination which is made by an authorized holder of classified or proprietary information as to whether or not a prospective recipient requires access to the specific information in order to perform or assist in a lawful and authorized Governmental function.

Need-to-Know Determination: According to DoD Directive 8500.1, a decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties.

Periodic Reinvestigation (PR): An investigation conducted every 5 years for the purpose of updating a previously completed background or special background investigation. The scope consists of a personal interview, NAC-LC, credit bureau checks, employment records, employment references, and developed character references, over the relevant period of inquiry (e.g., 5 or 7 years).

Personnel Security Determination: A discretionary security decision by appropriately trained adjudicative personnel of all available personal and professional information that bears on the individual's loyalty to the United States (U.S.), strength of character, trustworthiness, honesty, reliability, discretion and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and the willingness and ability to abide by regulations governing the use, handling, and protection of classified information and/or the execution of responsibilities of a sensitive position.

ACRONYMS

ACES	**Automated Continuous Evaluation System**
AIM	**Assessment for Individual Motivation**
ARC	**Automated Records Check**
CAPE	**Cost Analysis and Program Evaluation**
CE	**Continuous Evaluation**
CECD	**Continuous Evaluation Concept Demonstration**
DNI	**Director of National Intelligence**
DoD	**Department of Defense**
DoD CAF	**Department of Defense Central Adjudication Facility**
DONCAF	**Department of the Navy Central Adjudication Facility**
DSS	**Defense Security Service**
EO	**Executive Order**
eQIP	**Electronic Questionnaires for Investigations Processing**
FBI	**Federal Bureau of Investigation**
FIPPs	**Fair Information Practice Principles**
FIS	**Federal Investigation Service**
FIS	**Federal Investigative Standards**
FSO	**Facility Security Officer**
G-2	**Department of the Army Intelligence**
GAO	**Government Accountability Office**
HIPAA	**Health Insurance Portability and Accountability Act**
IG	**Inspector General**
IMESA	**Identity Management Enterprise Services Architecture**
IRTPA	**Intelligence Reform and Terrorism Prevention Act**
JPAS	**Joint Personnel Adjudication System**
JTMU	**Joint Threat Management Unit**
MHS	**Military Health System**
MOS	**Military Occupational Specialties**
MOU	**Memorandum of Understanding**
NCIS	**Naval Criminal Investigative Service**
NDAA	**National Defense Authorization Act**
NAC	**National Agency Check**
NAC-LC	**National Agency Check with Local Agency Check and Credit Check**
NISPOM	**National Industrial Security Program Manual**
NJP	**Non-judicial punishment**
ODCMO	**Office of the Deputy Chief Management Officer**
ODNI	**Office of the Director of National Intelligence**
OMB	**Office of Management and Budget**

OPM	**Office of Personnel Management**
PAC	**Performance Accountability Council**
PII	**Personally identifiable information**
PRP	**Personnel Reliability Program**
SecEA	**Security Executive Agent**
TAPAS	**Tailored Adaptive Personality Assessment System**
TEI	**The Experts, Inc.**
TMU	**Threat Management Unit**
USC	**United States Code**
USD(AT&L)	**Under Secretary of Defense for Acquisition, Technology, and Logistics**
USD(I)	**Under Secretary of Defense for Intelligence**
USD(P&R)	**Under Secretary of Defense for Personnel and Readiness**
USD(P)	**Under Secretary of Defense for Policy**
USIS	**US Investigations Services**
VA	**Department of Veterans Affairs**

ENDNOTES

[1] "[P]rior to September 11, 2001, we reported that DOD processed about 200,000 security clearances annually. For fiscal year 2008, we reported that DOD approved personnel security clearances for approximately 630,000 military, civilian, and industrial personnel." GAO-11-185T. DoD Personnel Clearances. Preliminary Observations on DOD's Progress on Addressing Timeliness and Quality Issues. Testimony before the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate. Statement of Brenda S. Farrell, Director Defense Capabilities and Management. 11 Nov 2010, p. 1.

[2] Reported from DoD/CAF, 31 October 2013. This information based on the JPAS data prepared for the 2013 Intelligence Authorization Act (IAA) Report on 7 October 2013.

[3] GAO-12-800, p.17-18 and GAO-14-157T, p. 6.

[4] DoD 5200.2-R, p.10 (1987)

[5] "In February 2008 and in subsequent reports examining personnel security clearance processes, GAO has highlighted the importance of a strong requirements-determination process in managing the workload and costs associated with the security clearance process. GAO noted that, while having a large number of cleared personnel can give the military services, agencies, and industry a great deal of flexibility when assigning personnel, having unnecessary requirements for security clearances increases the investigative and adjudicative workloads that are required to provide the clearances and flexibility. (GAO IG Report: Security Clearances: Actions Needed to Strengthen Controls Over Top Secret Security Clearance Requirements, U.S. Government Accountability Office, Office of Inspector General, Report No. OIG-13-3, September 2013, p. 5)

[6] "DoD makes an 'eligibility' determination prior to granting 'access' to improve support to the warfighter and the mobility of personnel requiring access. These individuals may not have been briefed yet, but may be briefed at any time without any additional investigative or adjudicative actions if required by their duties." (Report on Security Clearance Determinations, January 2013, ODNI, p. 4).

[7] DoD Defense Security Service. Personnel Security Management Office for Industry. "Periodic Reinvestigations." Accessed on 8 Nov 2013 via http://www.dss.mil/psmo-i/index.html.

[8] Interview with DSS officials on 6 November 2013.

[9] DSS reports that its oversight process focuses on whether the contractor's process for determining the number of cleared personnel is reasonable given the nature of the contract and the requirements for personnel. Coordination with the acquisition system is minimal once the contract is executed.

[10] DoDI 1400.25, Vol. 731, p. 7.

[11] GAO-13-728T, p.5. "In the absence of guidance to determine if a position requires a security clearance, agencies are using a tool that OPM designed to determine the sensitivity and risk levels of civilian positions which, in turn, inform the type of investigation needed. OPM audits, however, found inconsistency in these position designations, and some agencies described problems in implementing OPM's tool. In an April 2012 audit, OPM reviewed the sensitivity levels of 39 positions in an agency within DOD and reached different conclusions than the agency for 26 of them. Problems exist, in part, because OPM and the Office of the Director of National Intelligence did not collaborate on the development of the position designation tool, and because their roles for suitability-consideration of character and conduct for federal employment-and security clearance reform are still evolving."

[12] DODI 5145.03, p.1.

[13] Executive Order 13467 (2008). Section 2.3, C, iii. "The Director of National Intelligence shall serve as the Security Executive Agent. The Security Executive Agent [...] may issue guidelines and instructions to the heads of agencies to ensure appropriate uniformity, centralization, efficiency, effectiveness, and timeliness in processes relating to determinations by agencies of eligibility for access to classified information or eligibility to hold a sensitive position."

[14] OPM and ODNI proposed language to this effect in 78 FR 102 on May 28, 2013. The language is currently under review.

[15] Executive Order 12968 (1995). Section 1.2, B.

[16] According to DoDIG, "We also concluded that some policies, procedures, rules, regulations or management practices may be contributing to persistent misclassification of material….However, we did find several instances where the inaccurate use of dissemination control and handling markings could unnecessarily restrict information sharing….The most common discrepancy was incorrect marking of documents." (DoDIG-2013-142, DoD Evaluation of Over-Classification of National Security Information, p. iii.)

[17] For further discussion on public trust positions and national security positions, please see 5 CFR 731.106 - Designation of public trust positions and investigative requirements, 5 CFR 732.102, 5 CFR 732.201, and DoD 5200.2-R (C3.4.3) for Access to Classified Information by Non-U.S. Citizens.
[18] DoD 5200.2-R (1987, reissued 1996), Section C.
[19] DoD 5200.2-R, Section D.
[20] Executive Order 12968 (1995).
[21] Letter from Office of the Inspector General, Office of Personnel Management to members of the Senate Committee on Homeland Security and Government Affairs. November 5, 2013.
[22] "Investigative Standards for Background Investigations for Access to Classified Information," 1997, http://www.dhra.mil/perserec/adr/invstandards/invstandframeset.htm.
[23] GAO-08-352T, p. 10.
[24] 31 October 2013 Memorandum from the Department of Defense, Human Resources Activity, Defense Manpower Data Center
[25] Office of the Director of National Intelligence, Researching the Use of Social Media for Continuous Evaluation, presentation, September 19, 2013 cited "34% of individuals"
31 October 2013 Memorandum from the Department of Defense, Human Resources Activity, Defense Manpower Data Center cited "20% of individuals.
[26] Office of the Director of National Intelligence, Researching the Use of Social Media for Continuous Evaluation, presentation, September 19, 2013.
[27] "Approach to Reform." Office of the National Counterintelligence Executive. http://www.ncix.gov/SEA/reform/approach.php. Accessed 8 November 2013.
[28] OPM Inspector General Patrick McFarland to The Honorable Claire McCaskill, et al, letter, November 5, 2013.
[29] "The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudicative process is the careful weighing of a number of variables known as the whole person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination," 32 CFR 154, Appendix H to Part 154.
[30] GAO-09-400, p. 6.
[31] GAO-13-728T, p. 7.
[32] Security Clearances: Additional Mechanisms May Aid Federal Tax-Debt Detection. GAO-13-733. Washington D.C.: September 2013.
[33] Senate Bill, "Enhanced Security Clearance Act of 2013,"
[34] Adjudicative Guidelines for Determining Eligiblity for Access to Classified Information, December 29, 2005. 2.(b).
[35] DoD 5200.2-R, "Personnel Security Program," January 1987, Administrative Reissuance Incorporating Through Change 3, February 23, 1996, 142.
[36] Exec. Order 12968, as amended. Sec. 1.2(b)
[37] EO 13467.
[38] SF-86 Authorization for Release of Information.
[39] EO 12968, as amended.
[40] FIS 1997, amended 2004; USD(I) to DoD Security Directors, memorandum, February 14, 2013, *Implementation of Revised Federal Investigative Standards*. (Approved but not yet released).
[41] October 31, 2013, Memorandum from the Department of Defense, Human Resources Activity, Defense Manpower Data Center
[42] Federal Bureau of Investigation (FBI) Washington Field Office Response to request for information on FBI's Rap Back Service.
[43] EO 12968, as amended. *Access to Classified Information.* SEC.1.2(d)
[44] Director of National Intelligence Memorandum (E/S 00672, *Periodic Reinvestigations*).
[45] EO 12968, as amended. *Access to Classified Information* SEC 1.2.(b)
[46] "Privacy Policy Guidance Memorandum: The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security," Memorandum Number: 2008-01, Hugo Teufel III, Chief Privacy Officer. December 29, 2008, http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.
[47] Defense Science Board. "Task Force Report: Predicting Violent Behavior." (Washington D.C.: Department of Defense, August 2012).

[48] In both the Independent Review of the Ft. Hood shooting as well as the subsequent DSB report "Predicting Violent Behavior," TMUs are discussed extensively as a "best practice" used by local government, schools, and corporations as an effective tool in helping prevent violence. The DSB report also cites the similarity between adult sexual assault and other workplace violence issues and the potential to leverage the personnel assigned to the multidisciplinary Case Management Group (CMG). Defense Science Board. "Task Force Report: Predicting Violent Behavior." (Washington D.C.: Department of Defense, August 2012).
[49] *Ibid*, p.23.
[50] *Ibid*, p.23.
[51] The mission of the NCIS TMU is stated on their website: "The Threat Management Unit (TMU) was established to provide criminal and behavioral analysis and risk assessments for NCIS investigations in an attempt to review, and ultimately mitigate, the potential for violence. The TMU is a multidisciplinary support team made up of special agents, staff psychologists, analysts and others. Investigative analysis provided by the TMU includes violence risk assessments, interview and interrogation strategies, and management plans. The TMU helps to identify risk factors, patterns of escalation, and to construct an environment that inhibits or prevents violence. The services provided by the TMU cover a wide range of topics, including, but not limited to terrorism, school violence, sexual crimes, stalking, cyber-crimes (cyber stalking), domestic violence, arson, sabotage, communicated threats, insider threats and pre-attack behavior." http://www.ncis.navy.mil/CoreMissions/FI/Pages/ThreatManagementUnit.aspx (Accessed November 12, 2013).
[52] NGA began implementation of a threat management program mandated by the Secretary of Defense in a 26 March 2013 memorandum. The unit is a component of the NGA Police Force and is intended to comply with the recommendations of the DSB Task Force on predicting violent behavior. It responds to referrals of concern for, or displays of, aggressive behavior, and conducts investigations to confirm or formally rule out any actual threat.
[53] Veterans Health Administration Directive 2012-026. "Sexual Assaults and Other Defined Public Safety Incidents in Veterans Health Administration (VHA) Facilities." Issued 27 September 2012.
[54] Interagency Security Committee. "Violence in the Federal Workplace: A Guide for Prevention and Response." 1st Edition, April 2013.
[55] USD(P&R) is issuing an update to policies and procedures to address preventing violence in the workplace, integrating existing programs such as suicide, sexual assault, and family violence with information on violence and self-radicalization to provide more comprehensive program. The expected completion date is December 2013.
[56] Harrell, Erika. "Workplace Violence Against Government Employees, 1994-2011." (2013).
[57] The case of Dr. Bruce Ivins, a United States Army Medical Research Institute of Infectious Diseases (USAMRIID) microbiologist is illustrative. In September and October of 2001, five people in the United States died from anthrax, 22 were infected, after letters containing anthrax were discovered. The letters were attributed to Ivins. Ivins' history provides indicators of psychopathology and of multiple behaviors associated with an elevated risk of violence. He had a "significant and lengthy history of psychological disturbance and diagnosable mental illness. He committed numerous aggressive, antisocial and criminal acts include burglary, breaking and entry, theft, and vandalism. He abused prescription medications and alcohol. Ivins never truthfully, accurately reported this during the three decades he worked for USAMRIID, held a clearance, and was required to self-report. " (Report of the Expert Behavioral Analysis Panel: Amerithrax Report, 15).
[58] The Personnel Reliability Program (PRP), a system of for evaluating personnel in such sensitive military operations as nuclear-weapons command and control relies on peers and supervisors to report problematic behavior. PRP certification emphasizes the role of the unit commander, and the importance of both clear lines of accountability and a high degree of awareness of the life circumstances of subordinates. Furthermore, this model relies upon ensuring that unit members feel empowered – indeed, obligated – to report developments that may indicate that another team member is in trouble. PRP makes allowances for short-term, non-punitive removals of clearance – such as when a service member is under the effect of a prescription medication that temporarily diminishes mental acuity or physical strength. (Department of Defense Instruction, "Nuclear Weapons Personnel Reliability Program," July 16, 2012, 1) Similarly AR50-1 establishes a Biological Personnel Reliability Program to ensure that persons with access to biological select agents and toxins meet high standards of reliability, and are subject to continuing evaluation. (Army Regulation 50-1 Biological Surety, July 28, 2008).
[59] Virginia Code §.23-9.2:10 "Violence Prevention Committee; Threat Assessment Team."
[60] USD(P&R) is issuing an update to policies and procedures to address preventing violence in the workplace, integrating existing programs such as suicide, sexual assault, and family violence with information on violence and self-radicalization to provide more comprehensive program. The expected completion date is December 2013. This

update addresses Recommendation 2.6, "Protecting the Force: Lessons from Fort Hood," Report of the DoD Independent Review.

[61] Defense Science Board. "Task Force Report on Predicting Violent Behavior" included this recommendation in its executive summary. It is also Recommendation 2.10, "Protecting the Force: Lessons from Fort Hood," Report of the DoD Independent Review.

[62] A review of Tricare insurance records, PDTS prescription records, VBA and VHA records, training records, and quality assurance records was completed pursuant to a medical review by subject matter experts. Section 1102 of Title 10, US Code, prohibits the disclosure of information stemming from this review. Any statements that make informed speculations regarding the perpetrator's mental state stem from descriptions of his behavior in publically releasable investigative reports or publically available accounts.

[63] Aaron Alexis appeared, in retrospect, to have been psychotic in Newport, Rhode Island, shortly before he began contracting duties in the National Capital Region. Psychosis is the *sine qua non* of Schizophrenia and Schizoaffective disorder, but it is also seen in mood disorders such as depression and bipolar disorder, and it can stem from medical illnesses and withdrawal from or use of intoxicants. Alexis is dead, and any diagnosis is speculative. It is important to note, however, that one study of homicide during untreated first episode psychosis showed it occurred at a rate of 1 in 629 presentations. The rate of homicide after treatment of psychosis was 1 in 9090, which suggests that earlier treatment of first-episode psychosis might prevent some homicides (O. Nielssen and M. Large, Rates of Homicide During First Episode of Psychosis and After Treatment, A Systematic Review and Meta-analysis, Schizophrenia Bulletin 36 (2010):702-712.

[64] Violence prediction, owing to its prospective nature and the dynamic nature of risks over time, is fraught with difficulty. Base rates for serious violence are low. In the Clinical Antipsychotic Trials of Intervention Effectiveness (CATIE) study, the 6-month prevalence of causing serious injury or assault with a weapon was 3.6% (J Swanson et al, A National Study of Violent Behavior in Persons with Schizophrenia, Archives of General Psychiatry; 63 (2006):490-499). Suggestions that better accuracy is imminent in short-term predictions of violence have yet to be tested and confirmed. Clinical usefulness of actuarial scales is not yet established and, in any case, actuarial scales have inherent limitations. The number of people needed to detain (NND) is a term most widely used in risk management. It is the inverse of the positive predictive value of any predictive algorithm used at any given base rate for violence. Using a well-regarded scale, the Violence Risk Assessment Guide (VRAG) which has a sensitivity of 0.73 and a specificity of 0.63, at the base rate of violence described above, the number of individuals that need to be detained to prevent one violent act is 15, (A Buchanan, *Risk of Violence by Psychiatric Patients: Beyond the "Actuarial Versus Clinical" Assessment Debate*, *Psychiatric Services*; 59 (2008):184-190) a relatively high number which would naturally herald concerns for individual civil liberties and the social utility of current science.

[65] Mental illness includes many conditions that have a negative or no correlation to an increased propensity for violence in comparison to unaffected cohorts, such as the subtype of schizophrenia with "negative" symptoms (J Swanson J et al). Moreover, schizophrenia is at least an order of magnitude less common than anxiety disorder diagnoses.

[66] Aaron Alexis likely had the following risk factors for violence: a past history of violence, prior arrests, alcohol abuse, risk taking behavior suggesting loss of control or impulsivity, access to weapons, intention to harm, and lack of concern over the consequences of violent acts. Other risk factors for violence, often seen in psychiatric settings, which are less substantiated or unsubstantiated in this case are: the totality of his circumstances and mental state, young age at first arrest, cruelty to animals or people, fire setting, treatment non-compliance, provocative or non-protective behavior by a significant other or caretaker, seeing oneself as a victim, and a lack of empathy or compassion. A. Buchanan et al, Resource Document on Psychiatric Violence Risk , *Am J Psychiatry, 169* (2012): data supplement, p. 1-9.

[67] Many factors associated with violence that can be seen in the absence of severe mental illness. Some of these factors overlap with risk factors seen in mentally ill persons. These include experience of physical or sexual abuse during childhood, parental history of criminal involvement, criminal history, a history of violent behavior (homicide, stalking, and assault), aggression and hostility, and poor impulse control. K. Witt, R. van Dorn, S. Fazel, *Risk factors for Violence in Psychosis: Systematic Review and meta-Regression Analysis of 110 Studies*, PLOS ONE 8:2(2013). Situational risk factors of violence include financial stressors, narcissistic injury, loss or setback at work, a lack of social support, and loss of relationships. Randy Borum, Robert Fein, et al., *Threat Assessment: Defining an Approach for Evaluating Risk of targeted Violence*, Behavioral Sciences and the Law 17: 3 (1999); Gregory Saathoff, Gerald DeFrancisco, et al., Amerithrax Case: Report of the Expert Behavioral Analysis Panel (Vienna, VA, 2010).

[68] While precise data are not available, it has been estimated that 1 in 10,000 persons with schizophrenia will commit homicide annually in the United States. P. Mullen, *Schizophrenia and violence: from correlations to preventive strategies*, Advances in Psychiatric Treatment 12 (2006): 239-48. Based on crime data from the Federal Bureau of Investigation for 2010, males 18-24 committed murder at more than double that rate, approximately 2.5 per 10,000. C. Puzzanchera, G. Chamberlin, and W. Kang, Easy Access to the FBI's Supplementary Homicide Reports: 1980-2011, available at www.ojjdp.gov/ojstatbb/ezashr/. Research from several European countries reports much lower homicide rates among persons with schizophrenia, approximately 1 per 35,000. O. Nielssen et al., *Homicide of strangers by people with a psychotic illness*, Schizophrenia Bulletin 37 (2011): 572-79. However differences in access to mental health treatment, in baseline murder rates, and in access to firearms mean these numbers are not directly comparable.

[69] The cost of mental health care, in Defense Health Programs only, was $2.4 billion in FY12. This does not include line funding to support mental health programs. DoD's Psychological Health and TBI program is defined by six strategic initiatives: Access to Care, Leadership and Advocacy, Quality of Care, Resilience, Surveillance, and Transition. Psychological Health accounts for most outlays, and Access to Care, which is the initiative used to obtain clinical and support care for patients, is by far the largest of the initiatives. DoD briefing to Office of Management and Budget, *Mental Health Resourcing FY 2010 to FY 2014*, (30 July 2013).

[70] Defense Manpower Data Center (DMDC), *APF Civilian Counts by Prior Military Service Status* (30 September 2013). Comparable data on the contractor workforce does not exist. DoD needs to develop a means to better track data such as these for the DoD contractor workforce.

[71] The current exclusions, aside from treatment associated with sexual assault, for counseling stemming from family, marital, grief, or combat-related problems could be viewed as arbitrary. Adjustment problems related to service in a military combat environment, including PTSD, family and marital problems, and grief can vary widely in degree of functional limitation. Furthermore, PTSD rarely exists in isolation. It is often complicated by depression, other anxiety disorders, or substance abuse. Nearly all mental illness is amenable to treatment, and any effort to except these illnesses risks stigmatizing the care for other mental illnesses.

[72] By many measures, the burden of mental illness has increased in the active duty force. From 2000-2011, nearly one million active duty service members were diagnosed with at least one mental disorder. Incidence of mental health diagnoses rose nearly two thirds over the period, and the increase was largely attributable to anxiety, depression, PTSD, and adjustment disorders. Armed Forces Health Surveillance Center, *Mental Disorders and Mental Health Problems, Active Component, US Armed Forces 2000-2011*, Medical Surveillance Monthly Report, 19 (June 2012): 11-16. Use of medications, especially antipsychotic drugs, also rose precipitously over the period and strong policy responses were formulated to decrease medication use and foster the use of psychotherapy. Assistant Secretary of Health Affairs, *Guidance for Mental Health Provider Training for the Treatment of Post-Traumatic Stress Disorder and Acute Stress Disorder*, December 13, 2010; *Guidance for Providers Prescribing Atypical Antipsychotic Medication* (22 February 2012); Assistant Secretary of Health Affairs, *Clinical Policy Guidance for Assessment and Treatment of Post-Traumatic Stress Disorder* (24 August, 2012); and Center for Healthcare Management Studies, Health Program Analysis and Evaluation, Prescription Drug Use Study: Year 1 Findings to Date (18 July 2011).

[73] R. Ireland, A. Kress and L. Frost, *Association Between Mental Health Conditions Diagnosed During Initial Eligibility for Military Health Care Benefits and Subsequent Deployment, Attrition, and Death by Suicide Among Active Duty Service Members*, Military Medicine, 177 (2012): 1149-1156.

[74] DoD Instruction (DoDI) 6130.03, *Medical Standards for Appointment, Enlistment, or Induction into the Military Services*, has relatively restrictive criteria for psychological *diagnoses*, including now common diagnoses in children and adolescents (such as ADHD) that may not confer functional limitations in adulthood, but speaks less to non-cognitive traits, which might be better predictors for mental illness or attrition in uniform. Much effort in the past two years to change accession medical standards in the psychological realm has been focused on the issue of possibly inducting transgendered individuals. An Accessions Medical Standards Working Group is working to revise the list of disqualifying (or waiver-requiring) mental health conditions in DoDI 6130.03 as the list is outdated and in some cases does not comport with current nosology or phenomenology of mental diseases. Nascent effort has been directed toward addressing the functional limitations associated with deficits in non-cognitive or adaptive personality traits.

[75] The current procedure for referring a potential recruit for a clinical psychological interview at a Military Entry Processing Station is to use the Omaha-5 questionnaire as a nidus for discussion. MPP, OUSD-Personnel and Readiness. Its questions relate to law enforcement encounters (including juvenile or dropped encounters), school

authority encounters (suspension or expulsion), behavioral health encounters (with providers or through the use of use of psychoactive medication), self-mutilation, and living out of the home before age 18.

[76] The QUIC-R Database shows that in FY2007 , the year of Alexis' accession, 530,000 recruits took enlistment tests, 342,000 proceeded to medical exams, 327,000 were found to be qualified by USMEPCOM or had Service waivers, 278,000 proceeded to the initial oath and behavior assessment, 244,000 enlisted and shipped to recruit training, and 217,000 completed recruit training. Accessions with waivers were at 9.7% in FY2012, but 25.2% in 2007. MPP, OUSD-Personnel and Readiness.

[77] Longitudinal changes in the prevalence of psychiatric disorders can be associated with an actual change in prevalence, changes in case definitions (which are manifest given changes in the Diagnostic and Statistical Manual (DSM), including changes in the required number of symptoms, age of onset, or duration of symptoms, which represents a change in the diagnostic threshold), changes in the public sentiment on mental disorders, or diagnostic advances, which might owe to changes in access to health care. Policy changes also might affect rates, including the implementation of the Mental Health Parity and Addiction Equity Act, Public Law No. 110–343, and the Patient Protection and Affordable Care Act, Public Law No. 111–148. These policies promote provision of mental health services in primary care settings and include provisions that guarantee care for children with preexisting conditions. Ruth Perou et al., *Mental Health Surveillance Among Children- United States, 2005–2011*, Morbidity and Mortality Weekly Report 62 (17 May 2013): 1- 35.

[78]M. Gubata et al., *A Noncognitive Temperament Test to Predict Risk of Mental Disorders and Attrition in US Army Recruit*, Military Medicine 177 (2012): 374-379.

[79] Accession Medical Standards Analysis and Research Activity (AMSARA), Retrospective Analysis of Non-Cognitive Personality Scales: Assessment of Individual Motivation and Tailored Adaptive Personality Assessment System, AMSARA Annual Report (2012): 19-21, available at www.amsara.amedd.army.mil/AMSARAAR.aspx.

[80] The six months after entry into recruit training coincides with the period of eligibility for commanders to process "entry level separations."

[81] DoD Active Duty Separations, Service by Separation by ISC, FY2000 and FY 2007-FY2012 (MPP, OUSD-Personnel and Readiness).

[82] Ruth Perou et al.

[83] Patrick Monahan, Zheng Hu, Patricia Rohrbeck, *Mental Disorders and Mental Health Problems among Recruit Trainees, US Armed Forces, 2000-2012*, Medical Surveillance Monthly Report 20 (July 2013), 13-18.

[84] Hospitalizations are up sharply, especially for PTSD, depression, alcohol abuse and dependence, and adjustment disorders. In regard to the latter finding, 8 of 10 service members hospitalized for adjustment disorder never deployed. Hospitalizations for this condition are highest in young, inexperienced Service members. Armed Forces Health Surveillance Center, *Summary of mental disorder hospitalizations, active and reserve components, U.S. Armed Forces, 2000-2012*, Medical Surveillance Monthly Report 20 (July 2013), 4-11.

[85] The review team also explored the use of psychological testing in each of the Services at career points other than recruit training. We cannot say that increasing their use would offer any benefit beyond the known benefits that accrues from use of trained military providers to inform command decisions about the disposition of mental health patients. No changes are recommended.

[86] Personality disorder separations in FY00 were 4217, in FY07 were 4127, and in FY12 were 300. Adjustment disorder separations were 0 in FY00, 102 in FY07, and 1022 in FY12. Robust policy changes to limit personality disorder discharges started in FY07. These changes may have not only affect discharges, they may have affected diagnoses. In 2003, the incidence of personality disorder (PD) diagnoses per 100,000 person years was 505. It was 514 in 2005 and 513 in 2007. After the policy change, diagnoses dropped precipitously—to 344 in 2009 and 284 in 2011. In FY12, ASD-Health Affairs introduced clinical guidance regarding adjustment disorders (AD) that acknowledged that VA Schedule of ratings for Disabilities (VASRD) characterizes some adjustment pathology as "chronic," thus meriting disability compensation as opposed to administrative separation in cases where suitability for military service was affected. In FY13, the DoD Instruction regarding Physical Disability Evaluation was changed to reflect this standard. Undersecretary of Defense for Personnel and Readiness, *Physical Disability Evaluation*, DoD Instruction 1332.38 (10 April 2013). Trends in PD and AD diagnoses are being followed closely.

[87] Entry-level performance and conduct discharges for FY00 were 6344, for FY07 were 2,421, and for FY12 were 4190. Alcohol-related discharges were relatively steady at 787 in FY00, 899 in FY07, and 968 in FY12. FY07 represented a period of large contingency operations and relatively robust opportunities in the civilian economy for individuals in the typical recruit's age cohort. The denominators were relatively constant over the period: The AD force was 1.402M +/- 0.024M and the amount of service members who enlisted and shipped to recruit training was

231K+/- 23K. Undersecretary of Defense for Personnel and Readiness, DoD Active Duty Separations: Service by Separation by ISC.

[88] Less than half of Service members who screened positive for a mental health problem sought help from a behavioral health provider, primary care provider or chaplain. C.W. Hoge, C. Castro, et al., *Combat Duty in Iraq and Afghanistan, Mental Health Problems, and Barriers to Care*, New England Journal of Medicine 351 (1 July 2004): 13-22 and Office of the Surgeon, MNF-I and Office of the Surgeon General, USAMC, Mental Health Advisory Team (MHAT)-IV Final Report (17 November 2006), available at www.combatreform.org/MHAT_IV_Report_17NOV06.pdf.

[89] Defense Centers of Excellence for Psychological Health and Traumatic Brain Injury (DCoE), Program Evaluation and Efficacy Support Services, PH Effectiveness Initiative: Information Collection and Assessment Report of Findings (14 June 2013), on file with Assistant Secretary of Defense for Health Affairs.

[90] Executive Order 13625, *Improving Access to Mental Health Services for Veterans, Service Members, and Military Families* (31 August 2012).

[91] DoD presentation to Office of Management and Budget, *Mental Health Resourcing FY 2010 to FY 2014* (30 July 2014).

[92] These efforts, discussed above are underway and mandated on several fronts: law in NDAA 2013 Section 739, in Executive Order 13625, and in the DoD-VA Integrated Mental Health Strategy (Strategic Actions #10 and #12).

[93] Process measures for programs include access to care, timeliness, and type of care rendered. Outcome measures, recently codified in an ASD-Health Affairs Memorandum, include actual measurements of patient response to treatment. Assistant Secretary of Defense for Health Affairs, *Military Treatment Facility Mental Health Clinical Outcomes Guidance* (9 September 2013). The Services are collaborating on a data portal to collect outcome data.

[94] Not all efforts at treatment outside of the MHS present this concern, and safeguards can be placed that both reduce stigma associated with obtaining care while protecting the commander's interests and accountability to all Service members under his command and the interests of local and national security. For instance, the Army's Confidential Alcohol Treatment Program (CATEP) has strict provisions for a Commander to be notified if a soldier: is at risk of harming himself or someone else is involved in: a criminal investigation, legal actions or legal proceedings; official duties that are part of the nuclear, biological or chemical surety program; using illegal substances, alcohol related incident, abusing prescription medication; or does not adhere to the treatment plan (U.S. Army briefing to the DoD Addictive Substances Misuse Advisory Committee, 17 July 2013).

[95] Hunt, S and Grieg, T, Information Paper from Joint VA-DoD HEC Health Information Sharing Task Force, February 15, 2012.

[96] The Joint VA-DoD Health Executive Council (HEC) Information Sharing Task Force (Information Paper briefed to the HEC February 15, 2012) and Strategic Action #14 of the DoD/VA Integrated Mental Health Strategy (IMHS) reviewed DoD and VA policies related to sharing of health and mental health information. The conclusion of both efforts was that DoD and VA are allowed to share health information, including mental health information, without patient authorization (i.e. bi-directional health information sharing). Practice in some cases is inhibited by poor interoperability of DoD's and VA's electronic medical records. Innovations such as the Bidirectional Health Information Exchange, JANUS, and HAIMs have the potential to help close the gap on information sharing, but there have been setbacks in execution. Integrated Mental Health Strategic Action #14, "Policies Regarding Mental Health Clinical Information Sharing," is complete, and the agencies have agreed on plans to foster information sharing regarding mental health between the systems. VA providers are under no legal obligation to report on a Service member's behavior to his commander.

[97] *Military Culture: Core Competencies for Health Care Professionals* is available to DoD, VA and community health care providers http://www.health.mil/courses.aspx (select drop-down box for "Military Culture Training for Health Care Professionals"). The first module, entitled Self-Assessment and Introduction to Military Ethos is currently available and offers 2 hours of continuing education credit at no cost to health care professionals. Modules 2 through 4 will be available later in Fiscal Year 2014. The Center for Deployment Psychology has developed a companion website for the course at: www.deploymentpsych.org/military-culture.

[98] Undersecretary of Defense for Personnel and Readiness, *Mental Health Evaluations of Members of the Military Services*, DoD Instruction 6490.04(4 March 2013).

[99] For several years prior to 2012, it was at times difficult to start the process of compelling a service member to obtain a mental health evaluation if the Service member was acting aberrantly. Procedural barriers, which stemmed from law and subjected many commanders to investigations after mental health referrals, made it difficult at times to pursue command-directed mental health evaluations. Lengthy protocols for command-directed mental health evaluations led many commanders to face investigation for simply acting in the unit's best interests. Investigations

of small procedural irregularities formed a large portion of the DoD IG investigations over the period. Many complaints were substantiated. Moreover, there was a long period where providers struggled with involuntary admission of patients that stemmed from protections in law against misdiagnosis. The tenor of these protections could favor, in some cases where diagnostic clarification was necessary, patient autonomy over the military mission. This situation was analogous in many ways to state laws for involuntary commitment, which are also evolving. The sequelae of this situation may lead to continued reticence to refer Service members for behavioral health care that may result in admission or adverse action, despite changed language in DoDI regarding mental health evaluations. Undersecretary of Defense for Personnel and Readiness, *Mental Health Evaluations of Members of the Military Services*, DoD Instruction 6490.04(4 March 2013). Training, mandated in the instruction, will be essential to striking a balance between patient's rights and the needs of the military mission.

[100] National Defense Authorization Act for Fiscal Year 2012, Public Law 112-81, § 711b amended 10 U.S.C. Section 1090a.

[101] The first research program is " Behavioral-Based Predictors of Workplace Violence in the Army STARRS" "Abstract: The objective is to develop practical behavioral-based risk prediction indices for workplace violence perpetration and victimization in the Army based on analyses of the Army Study to Assess Risk and Resilience in Servicemembers (A-STARRS). The proposed research has 13 specific aims that involve analyzing: (i) the A-STARRS integrated administrative data file (IADF) for all Soldiers on active duty 1/1/04-12/31/09 (approximately 1.6M Soldiers and 75.5 million person-months); (ii) self-report data collected in a series of A-STARRS surveys; (iii) genetic data collected from A-STARRS survey respondents in two surveys; (iv) neurocognitive data collected from A-STARRS respondents in one survey; and (v) retrospective and prospective IADF data merged with the survey sample data. Analyses of these complex databases will be of two broad types. First, data mining will be used to generate optimal prediction equations for workplace violence perpetration-victimization in each sample first based exclusively on IADF data and then adding in survey, genetic, and neurocognitive data available for the sample. These analyses will be used to produce computer programs Army leadership can use to predict risk of future workplace violence for each Soldier in the Army for whom the relevant predictor data are available. If the survey predictors improve on models that use only IADF predictors, we will also develop suggested short surveys containing the items found to be most predictive of workplace violence. Second, theoretically-guided analyses will be carried out to examine potentially important modifiable risk-protective factors that can help inform intervention design efforts after high-risk Soldiers are targeted using the prediction equations developed in the data mining phase of the research." The second program is the "Multimodal Retrospective and Prospective Unit-Level Analysis of Military Workplace Violence." "Abstract: Hypotheses are (1) deployment characteristics, including number of deployments and combat intensity, will increase MWV; (2) disciplinary infractions, minor crimes, PTSD and other mental problems, and substance abuse will increase MWV; (3) treatment and social support will mediate the relationships among deployment characteristics, intervening outcomes, and MWV; and (4) individual and family/peer risk and protective factors and training will moderate the relationships between deployment, intervening outcomes, and MWV. The project has three aims: (1) identify and test predictors of targeted MWV (e.g., threats, aggravated assault, homicide) at multiple ecological levels (individual, unit, installation) and multiple time points relative to military service and deployment; (2) identify and test mediating and moderating factors for targeted violence; (3) develop recommendations for individual-, unit-, and installation-level procedures and tools to prevent or leverage dynamic and protective factors to reduce targeted violence." The Defense Center of Excellence for Psychological Health and Traumatic Brain Injury is also conducting a literature review of violence screening programs and practices (e.g., workplace violence, domestic violence, and sexual violence) within the Services, Postal Service, private industry and academia with regard to best practices.

[102] VA/DoD Clinical Practice Guideline For Assessment And Management Of Patients At Risk For Suicide. Department of Veterans Affairs and Department of Defense. The Assessment and Management of Risk for Suicide Working Group. Version 1.0 – June 2013.

[103] DoD/VA Integrated Mental Health Strategy (IMHS) Strategic Action #26: Translation of Mental Health Research into Innovative Programs, focuses on promoting the translation of mental-health related research into innovative actions, programs, and policies for returning Service members, Veterans, and families.

[104] A DoD/VA Joint Incentive Fund project began in Fiscal Year 2013 to pilot test the use of a Practice-Based Implementation Network for PTSD interventions throughout DoD and VA.

[105] Deputy Inspector General for Intelligence, Department of Defense, Assessment of Security Within the Department of Defense – Tracking and Measuring Security Costs, Report No. 10 INTEL-09 (Washington, D.C., 6 August 2010), p. 3.

[106] Deputy Inspector General for Intelligence and Special Program Assessments, Department of Defense, Assessment of Security Within the Department of Defense –Security Policy, Report No. DoDIG-2012-114 (Washington, D.C., 27 July 2012), p. 3-4.

[107] Under Secretary of Defense, Intelligence, Defense Security Enterprise Strategic Plan (Washington, D.C., 2013), 4.

[108] Under 2002 Unified Command Plan, CDR USNORTHCOM was assigned the lead for DoD's overall antiterrorism program as well as the responsibility for tactical control for force protection within the Continental United States. President of the United States, Unified Command Plan, (Washington, D.C., 24 Oct 2002).

[109] NOTE: The governing manual for DSS evaluations is the National Industrial Security Program Operating Manual (NISPOM). The NISPOM "prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information" for the purposes of controlling the disclosure of classified information. (DoD 5220.22-M (NISPOM), Section 1-100, February 28, 2006, p. 1-1-1)

In order to enforce NISPOM requirements, DSS evaluates contractor facilities; authenticates the security clearances of contracting personnel; assesses the suitability of foreign ownership in covered industries; tracks suspicious activity reports that may lead to counterintelligence investigations by law enforcement; and provides security training to DoD and contracting personnel.

DSS oversight specifically involves "educating personnel on security requirements, accrediting information systems that process classified information, approving classified storage containers, … assisting contractors with security violation investigations, … and conduct[ing] periodic security reviews to assess whether contractors facilities are adhering to NISPOM requirements and to identify actual and potential security vulnerabilities." (GAO-08-695T, April 15, 2008. p. 4)

Contracting organizations must report adverse information concerning any of their cleared employees, suspicious contacts, and any security violations. In fiscal year 2011, DSS conducted 10,375 security reviews on 13,352 corporate offices. DSS cleared 950,000 contracting personnel security clearances and adjudicated an additional 194,397.

[110] A significant part of DSS's review process is interviewing site employees as part of the normal cycle of recurring visits. In these interviews, DSS is looking for signs of adequate training and awareness programs regarding the protection of classified material and the assessment of personnel – for example, whether a site has adequate standards for detecting and responding to suspicious contacts. DSS seeks to interview enough employees at a given site to get a good sense of how well trained the workforce is in overall security systems, and in classified-storage protocols. The desired proportion of employees DSS tries to interview is typically 5-10 percent of the site workforce, though this percentage may be higher at a smaller firm. It is often difficult to interview enough employees at a contractor like The Experts Inc., where the cleared workforce is widely dispersed.

[111] Defense Security Service, Briefing to review teams, 1 October 2013.

[112] Defense Security Service, Briefing to review teams, 22 October 2013.

[113] DSS should be given the authority and manpower to better address the risks associated with a contracting organization's ability to implement necessary security requirements. One specific problem that should be addressed in the near term is the infrequency of DSS site visits. These visits are valuable not only for "deterrent" value, but also as an opportunity to educate contractors on sound security practices.

Ideally, DSS would visit all sites 3-5 times each year. For fiscal reasons, that's not possible now. DSS can do "no-notice assessments," showing up with no warning. This seldom occurs, since DSS is leery of seeming like an adversary of the contractors.

[114] A significant part of DSS's review process is interviewing site employees as part of the normal cycle of recurring visits. In these visits, DSS is looking for signs of adequate training and awareness programs regarding the protection of classified material and the assessment of personnel – for example, whether a site has adequate standards for detecting and responding to suspicious contacts.

DSS seeks to interview enough employees at a given site to get a good sense of how well trained the workforce is in overall security systems, and in classified-storage protocols. The desired proportion of employees DSS tries to interview is typically 5-10 percent of the site workforce; this percentage may be higher at a smaller firm. It is often difficult to interview enough employees at a contractor like The Experts Inc., where the cleared workforce is widely dispersed.

DSS had rated the Experts, Inc. facility at the lowest tier of risk because the sensitive information it supervised was physically located at other sites. In its site visit, DSS rated the site's compliance as "satisfactory," the most common DSS rating by far. Had DSS found security flaws, it would have identified them in an effort to the company to

improve its procedures. Had DSS found grave weaknesses, it could have notified the government customer – in this case, the Navy – and then invalidated the contractor's ability to bid on additional government work.
However, only the Navy could have halted the firm's contract performance – and, in practice, this rarely happens. Even if a very serious deficiency had been documented, DSS could not have revoked The Experts, Inc.'s facility clearance without agreement from the Navy. Most importantly, the DSS assessment of TEI did not include an analysis of the unique risks associated with The Experts, Inc.'s highly distributed workforce, in which personnel had scant contact with supervisors – and, therefore, lacked clear lines of accountability.

[115] FSO reporting requirements under NISPOM are generally triggered only as issues and incidents arise – not as a running (say, monthly or quarterly) requirement. This passive approach to information gathering is reflected in the numbers: DSS is responsible for overseeing about 13,500 facilities. It has received adverse information from only about 10 percent of them. The Experts, Inc.'s FSO wasn't even physically present at the site – he was on convalescent leave in North Carolina.
An FSO may never visit the workplace, and may not even be acquainted with the government's facility security manager or contracting official. In such cases, unclear chains of command over contract employees undermine security.
DSS's current incident-reporting system is reliant on company self-reporting, which in turn generally relies upon employees reporting to FSO's about colleagues' behavior.
[116] Intelligence Reform and Terrorism Prevention Act (IRTPA), Sec. 3001 (PL 108-458, December 17, 2004)
[117] GAO-04-344, p. 4.
[118] A 2013 GAO report noted: "Executive branch agency efforts to improve the personnel security process have emphasized timeliness but not quality. In May 2009, GAO reported that with respect to initial top secret clearances adjudicated in July 2008, documentation was incomplete for most of OPM investigative reports. GAO independently estimated that 87 percent of about 3,500 investigative reports that DOD adjudicators used to make clearance decisions were missing required documentation. In May 2009, GAO recommended that [OPM] direct the Associate Director of OPM's Federal Investigative Services to measure the frequency with which its investigative reports met federal investigative standards in order to improve the completeness – that is, quality – of future investigation documentation. As of March 2013, however, OPM had not implemented this recommendation…. OPM continues to assess the quality of investigations based on voluntary reporting from customer agencies, the number of investigations returned for rework is not by itself a valid indicator of the quality of investigative work..."
Government Accountability Office, Further Actions Needed to Improve the Process and Realize Efficiencies, testimony before the U.S. Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on the Efficiency and effectiveness of Federal programs and the federal Workforce, and on Financial and Contracting Oversight, by Brenda S. Farrell, GAO-13-728T (Washington, D.C., 20 June 2013), p. 6-7.
[119] Farrell testimony, GAO-04-344, p. 7-9.
[120] Testimony of OPM Inspector General Patrick McFarland, June 20, 2013.
[121] A cost comparison between the State Department and DoD for clearances: OPM charges DoD a minimum of $752-$809 for each Secret-clearance investigation, and $4,005-$4,399 for each Top Secret investigation. OPM Notice 12-07, September 2012, http://www.opm.gov/investigations/background-investigations/federal-investigations-notices/2012/fin12-07.pdf. This does not include adjudication (the part of the process following investigation, in which an applicant's record is evaluated), which is handled by DoD. For its part, the State Department spends approximately $1,200 combined for its own investigation *and* adjudication of each Secret-level clearance, both of which are managed in-house – and only $3,500 for a Top Secret clearance. This does not include overhead costs for full-time staff and facilities, but it does include the cost for State's part-time contractors to conduct investigative leads worldwide. Interviews with Department of State officials. While it is difficult to directly compare the costs it appears OPM's costs for processing Secret clearances are at best about equivalent to those for the State Department (when factoring in the added expense of adjudication), while the expense for OPM's investigation of Top Secret clearances is higher than what State pays for investigation and adjudication combined.
[122] Senate Report 113-44 on the Senate's version of the National Defense Authorization Bill for Fiscal Year 2004 requires a joint report between DoD and ODNI, finding that "…DoD and DNI have been eager to modernize the security investigation process, believing that doing so would actually improve security, reduce the time needed for investigations, and reduce costs. OPM has been slow to address these cost and reform measures." U.S. Senate Committee on Armed Services, National Defense Authorization Act for Fiscal Year 2014 Report to Accompany S. 1997 (Washington, D.C., 20 June 2013), p. 151.
[123] The State Department is a model for successful in-house operation of consolidated investigations and adjudications, relying on well-trained and experienced case managers who ensure that a sufficiently thorough

investigative report is provided to adjudicators. State Department case managers then farm out leads as required to a cadre of contractor field investigators who carry out individual records checks and interviews, but do not manage the investigation. These personnel are paid for each lead they pursue, and are not full-time employees. DoD should draw upon the State Department mode and integrate with OPM to approximate the benefits from completing both the background investigation and adjudication in-house. Case managers are critical to State Department's success. A cadre of experienced DoD case managers sitting within OPM spaces could help integrate the background investigations with adjudications. Also, a DoD case manager should drive an increase in quality by insuring meeting the minimum federal investigative standards, but with the latitude to follow up on leads developed in the investigation. Telephone interviews with Bureau of Diplomatic Security personnel, Department of State, 16 October 2013.

[124] At an October 31, 2013 Senate hearing, Senator Thomas Carper noted, "the Department of Justice has joined a lawsuit against...US Investigations Service (USIS)...[which] performs about 45 percent of the background investigations that are contracted out by the Office of Personnel Management. According to this law suit, USIS engaged in a practice that company insiders referred to as 'dumping.' Under this alleged scam, USIS would send investigations back to the Office of Personnel Management even though they had not gone through the full review process. Through this 'dumping,' USIS maximized its profits." ("Opening Statement of Chairman Thomas. R. Carper: 'The Navy Yard Tragedy: Examining Government Clearances and Background Checks,'" Senate Homeland Security and Government Affairs Committee, October 31, 2013.

[125] "Electronic Questionnaires for Investigations Processing (e-QIP).... [A] web-based automated system that was designed to facilitate the processing of standard investigative forms used when conducting background investigations for Federal security, suitability, fitness and credentialing purposes." (opm.gov, accessed 4 Nov 2013, http://www.opm.gov/investigations/e-qip-application/)

[126] According to the Current Investigative Standards for Background Investigation for Access to Classified Information, the investigation for a Secret clearance includes:
Completion of SF-86
National Agency Check
Financial Review
Date and Place of Birth
Local Agency Checks
Expanding for Issues

The table below highlights the various tenets of a security clearance both for Secret and Top Secret background investigations. The general process for both clearances is similar although the level of detail and information gathered for a Top Secret clearance is more substantial. (Source: U.S. Government Accountability Office, Background Investigations: Office of Personnel Management Needs to Improve Transparency of Its Pricing and Seek Cost Savings, 9. GAO-12-197. Washington, D.C.: February 28, 2012.)

Table 1: Information Gathered in Conducting a Typical Investigation to Determine Suitability and Eligibility for a Security Clearance

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

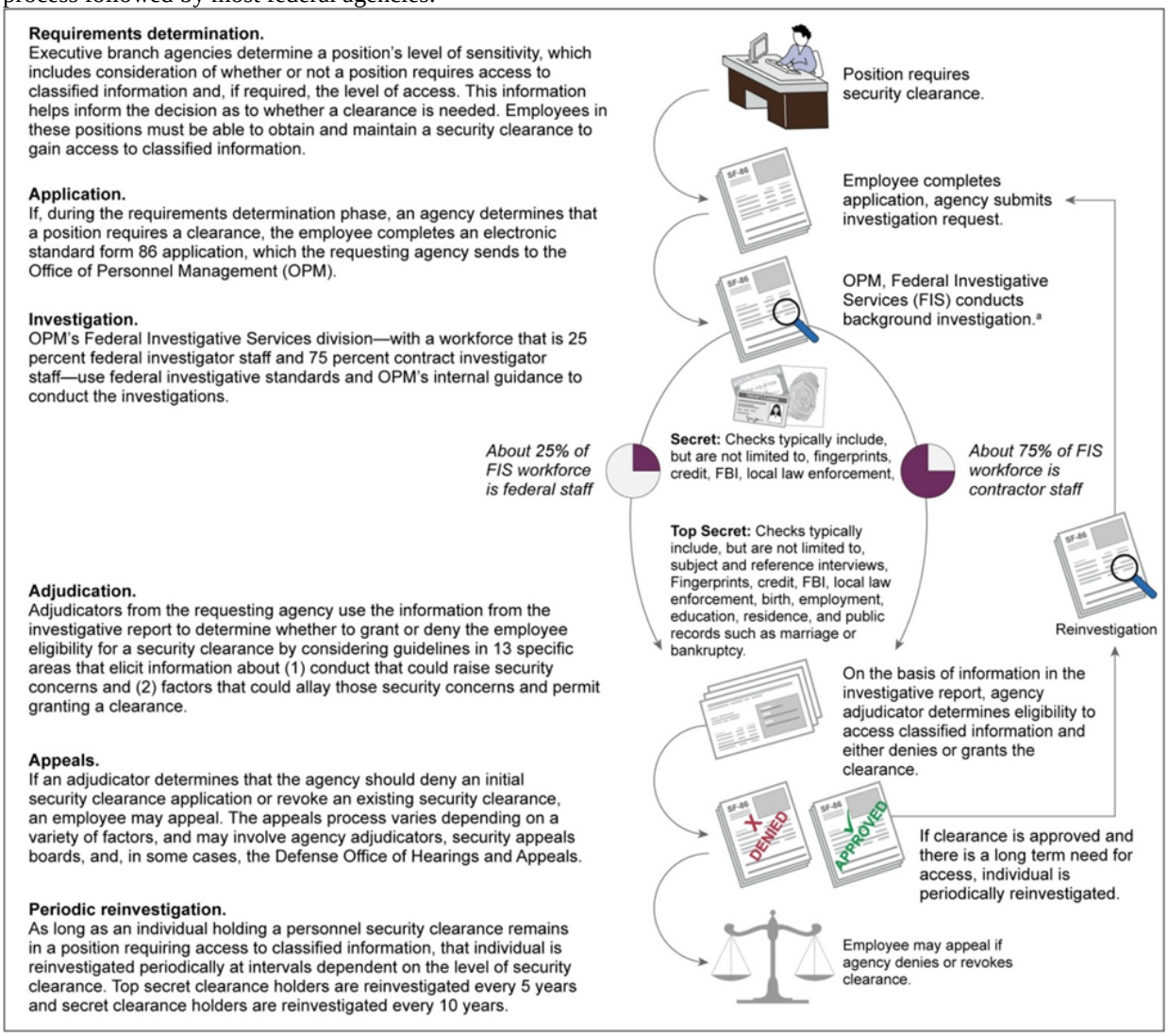
Source: DOD and OPM.

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

V = Components with this notation are checked through a mail voucher sent by OPM's Federal Investigative Services.

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

[127] The table below illustrates the current steps used to grant a security clearance which is representative of the process followed by most federal agencies:



(*Personnel Security Clearances: Full Development and Implementation of Metrics Needed to Measure Quality of Process*. GAO-14-157T. Washington D.C.: October 2013.).

[128] NISPOM, 2-200, p. e.

[129] GAO-12-800, p. 19.

[130] A cost comparison between the State Department and DoD for clearances:

OPM charges DoD a minimum of $752-$809 for each Secret-clearance investigation, and $4,005-$4,399 for each Top Secret investigation. (OPM Notice 12-07, September 2012, http://www.opm.gov/investigations/background-investigations/federal-investigations-notices/2012/fin12-07.pdf). This does not include adjudication (the part of the process following investigation, in which an applicant's record is evaluated), which is handled by DoD.

For its part, the State Department spends approximately $1,200 combined for its own investigation and adjudication of each Secret-level clearance, both of which are managed in-house - and only $3,500 for a Top Secret clearance. This does not include overhead costs for full-time staff and facilities, but it does include the cost for State's part-time contractors to conduct investigative leads worldwide. (Interviews with Department of State DSS officials).

While it is difficult to directly compare the costs, it appears OPM's costs for processing Secret clearances are at best about equivalent to those for the State Department (when factoring in the added expense of adjudication), while the expense for OPM's investigation of Top Secret clearances is higher than what the State Department pays for investigation and adjudication combined.

[131] *Ibid*.
[132] Letter from OPM Inspector General to Chairs and Ranking Members of Homeland Security and Governmental Affairs subcommittees, November 5, 2013.
[133] Seattle Police Department Incident Report 04-181918.
[134] "Adjudicating Incomplete Personnel Security Investigations," USD(I) Memorandum, March 10, 2010.
[135] GAO-13-728T.
[136] "Strategic Goals". Office of the National Counterintelligence Executive http://www.ncix.gov/SEA/reform/goals.php.
[137] Executive Order 13467 "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees , and Eligibility for Access to Classified National Security Information" http://www.ncix.gov/SEA/reform.php.
[138] "Approach to Reform". Office of the National Counterintelligence Executive http://www.ncix.gov/SEA/reform/approach.php.
[139] *Ibid.*
[140] Resource Center: Specially Designated Nationals List. United States Department of Treasury http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx.
[141] Security Clearances: Additional Mechanisms May Aid Federal Tax-Debt Detection. GAO-13-733. Washington D.C.: September 2013.
[142] *Ibid.*, p. *13-14*.
[143] *Ibid.*, p. *15-16*.
[144] Prioletti, Brian. Statement for the Record, Open Hearing on Security Clearance Reform, Senate Committee on Homeland Security and Governmental Affairs. October 31, 2013.
[145] Army Continuous Evaluation Concept Demonstration (CEDC) briefing for the Washington Navy Yard Independent Review Team, October 3, 2013.
[146] The Naval Criminal Investigative Service (NCIS) TMU consists of a small group of full-time NCIS agents, part-time analysts, and a staff psychologist, as well as a larger group of agents and investigators who handle TMU-related matters in the field. http://www.ncis.navy.mil/CoreMissions/FI/Pages/ThreatManagementUnit.aspx (Accessed 12 November 2013).
[147] Threat management teams may include representatives of security, legal, personnel/human resource departments, health care providers, as well as psychologists, psychiatrists, attorneys, analysts, and investigators. They may reach out to network of part-time advisory personnel including physicians, clergy, behavioral experts, and others.
[148] CMG is "A multi-disciplinary group that meets monthly to review individual cases of Unrestricted Reports of sexual assault. The group facilitates monthly victim updates and directs system coordination, accountability, and victim access to quality services." Department of Defense Instruction 6495.02, *Sexual Assault Prevention and Response (SAPR) Program*, March 28, 2013. http://www.dtic.mil/whs/directives/corres/pdf/649502p.pdf (Accessed 12 November 2013).
[149] Secretary of Defense, Final Recommendations of the Defense Science Board Report on Predicting Violent Behavior (26 March 2013), p. 1.
[150] *Ibid.*
[151] *Ibid.*
[153] De Choudhury, Munmun. "Role of social media in tackling challenges in mental health." *Proceedings of the 2nd International Workshop on Socially-Aware Multimedia*, pp. 49-52. ACM, 2013.
[154] Meloy, J. Reid, and Mary Ellen O'toole. "The concept of leakage in threat assessment." *Behavioral sciences & the law* 29, no. 4 (2011): p. 513-527.
[155] 28 U.S.C. § 534(a) and (c).
[156] DoD Directive 7730.47 (dated October 15, 1996) implements 28 U.S.C. § 534(a) and (c) and states that DoD shall "ensure that the Defense Manpower Data Center (DMDC) formulates a data collection mechanism to track and report …information from initial contact through investigation, prosecution, confinement, and release, and to report National Incident-Based Reporting System data to the Federal Bureau of Investigation."
[157] Federal Bureau of Investigation, Pre-Attack Behavioral Indicators of Violent Intent Briefing, October 18, 2013.
[158] Navy policy, OPNAVINST 5350.4 mandates that all confirmed drug and alcohol abuse incidents be referred and assessed by a Medical Officer (MO), Licensed Independent Practitioner (LIP) or Substance Abuse Rehabilitation Program (SARP) counselor. A screening and recommendation from a MO or LIP must be obtained prior to transferring a member to a SARP facility for treatment. In Alexis' case, it appears that his CO did not consider any

incident involving Alexis an "alcohol-related incident," so no referral was generated. A review of the Navy's Alcohol and Drug Management Information Tracking System (ADMITS) showed that Alexis had only educational training, AWARE once at recruit training and at his operational command, and no treatment referrals.

[159] Review of his presentation at the Navy Gateway in Newport, RI shows evidence that Alexis had paranoid delusions and, in all likelihood, auditory hallucinations. These "positive" psychotic symptoms increase the risk of both minor and serious violence in schizophrenia (in the absence of a clinical intervention, no diagnosis of Alexis can be proffered). Violence is uncommon yet problematic among schizophrenia patients (Swanson J et al, A National Study of Violent Behavior in Patients with Schizophrenia, Arch Gen Psychiatry 2006;63:490-99).

[160] DoDI 6490.4- *Mental Health Evaluations of Members of the Military Services*, March 4, 2013.

[161] Previous aggressive behavior is a predictive factor for homicide, suicide, sexual violence, and even, apropos this case, violence after a psychotic break (Witt K, van Dorn R, Fazel S (2013) Risk factors for violence in Psychosis: Systematic review and Meta-regression Analysis of 110 Studies. PLoS ONE 8(2): e55942).
Alexis had a history of reckless and violent behavior before accession, during service, and in civilian life prior Navy Yard incident. The vast majority of candidates for accession into the military are between 18 and 30 years old, which is roughly consistent with the period of initial mood episodes, including mania, and psychotic breaks (females trend later; males earlier).

[162] Examples of these efforts include: DoDI 6490.08 Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Service Members, 17 August 2011; DoDI 6490.10 Continuity of Behavioral Health Care for Transferring and Transitioning Service Members, 26 March 2012.

[163] D. Fikretoglu et al., *Twelve Month Use of Mental Health Services in a Nationally Representative, Active Military Sample*, Med Care 46 (February 2008): p. 217-23.

[164] Executive Order 13625, "Improving Access to Mental Health Services for Veterans, Service Members, and Military Families," August 31, 2012.

[165] The issue of diagnostic clarification and ethical disposition of patients has merited increased scrutiny in past years. A Service Chief and another physician at a forensic psychiatry service at Madigan Army Medical center, had privileges suspended after the service implemented a "best practice" to lend more validity to conferred diagnoses in medical boards. Accusations included a report that the team acted in the interest of saving the government money in subsequent disability payments. A subsequent investigation, which was publically released, found the accusations to be unsubstantiated. The Service Chief had his privileges restored. His commander, who was suspended during the investigation, was reinstated to command. While the investigative process was underway, US Army Medical Command promulgated a policy guidance memorandum that directed clinicians to exercise caution in conferring diagnoses of malingering, personality disorders, and adjustment disorders in mental health patients. This directive was superseded by policy guidance from the Office of The Assistant Secretary of Defense- Health Affairs (*Clinical Policy Guidance for Assessment and Treatment of Post-Traumatic Stress Disorder*, August 24, 2012).. The MEDCOM policy is to be rewritten with the roll-out of DSM-V.

[166] Ritchie, EC *Military Forensic Mental Health* in Ritchie, EC ed. Combat and Operational Behavioral Health, Borden Institute, Fort Dietrich, MD.

[167] Dual responsibilities are not anathema to the provision of health care in civilian settings. In cases when an individual presents a risk of self-harm or menace to the well-being of others, therapeutic practice clearly mandates a balance between an individual's confidentiality rights within a mental health care setting with broader social obligations. One example of this is the Tarasoff protocol, which sets a duty for all healthcare providers to warn and protect potential targets of potentially violent offenders. (*Tarasoff v. The Regents of the University of California*. Supreme Court of California, 1976.)

[168] DoD Directive 5200.43 defines the Defense Security Enterprise (DSE) as, "the organizations, infrastructure, and measures (to include policies, processes, procedures, and products) in place to safeguard DoD personnel, information, operations, resources, technologies, and facilities against harm, loss, or hostile acts and influences." Deputy Secretary of Defense, Management of the Defense Security Enterprise, DoD Directive 5200.43 (Washington, D.C., 24 April 2013), 16. The DSE is managed by the DSE Executive Committee (DSE ExCom) which consists of representatives from each of the USD offices, the DoD CIO, and the DA&M; security program executives designated by the Service Secretaries and the Chairman of the JCS; and the Directors of the DoD SAPCO, the Security Directorate of the DUSD(I&S), and the Counterintelligence Directorate of the ODUSD(I&S). While this multi-stakeholder structure may be an effective means for gathering input and building consensus, leadership is not centralized and is delegated to individuals who do not have the stature and authority needed to ensure accountability and advocate for needed resources.

[169] The draft DoD Directive on the DoD Insider Threat program is DoD Directive 5205.jj.

[170] Defense Security Service, Stakeholder Report 2012 (Washington, D.C., 2012), 34. In a typical security vulnerability assessment site visit, DSS conducts the following: briefing with senior management and the facility security officer; review of corrective actions from the previous vulnerability assessment (if any); review of business records to any corroborate reported information; interviews of personnel and visitors concerning the contractors security program; interviews with any foreign personnel regarding classified activity and access to export-controlled technology; an after-hours vulnerability assessment, for facilities with multiple shifts, advice and assistance in mitigating risks and identifying threats; and scoring/ rating of vulnerabilities (if any, including those corrected immediately during the assessment). Defense Security Service, 2013 DSS Vulnerability Assessment Rating Matriz: Vulnerabilities and NISP Enhancement Categories (Washington, D.C., September 2013), available at www.dss.mil/isp/fac_clear/security-rating-matrix.html.

[171] DSS had rated the Experts, Inc. facility at the lowest tier of risk because the sensitive information it supervised was physically located at other sites. In its December 2011 site visit, DSS rated the site's compliance as "satisfactory," the most common DSS rating by far. Defense Security Service, Briefings to review teams, 1 and 22 October 2013.

[172] Defense Security Service, Briefing to review teams, 22 October 2013.

[173] HP cancelled several of its subcontracts with TEI, resulting in a substantial loss of its workload.

[174] In 2010, DoD maintained approximately 3.9 million clearances for civilian and military personnel, and contractors. Government Accountability Office, Testimony Before the U.S. Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, GAO-12-815T (Washington, D.C., 21 June 2013), 1-2. Maintaining and granting this many clearances is an enormously challenging process.

[175] "DOD met the 60 day IRTPA timeliness objective for initial personnel security clearances, as well as the 20 day objective for the timeliness of adjudications, for each of the first, second, and third quarters of fiscal year 2010, according to data provided by the Performance Accountability Council." GAO-11-185T, Highlights page.

[176] A 2013 GAO report noted: "Executive branch agency efforts to improve the personnel security process have emphasized timeliness but not quality. In May 2009, GAO reported that with respect to initial top secret clearances adjudicated in July 2008, documentation was incomplete for most of OPM investigative reports. GAO independently estimated that 87 percent of about 3,500 investigative reports that DOD adjudicators used to make clearance decisions were missing required documentation. In May 2009, GAO recommended that [OPM] direct the Associate Director of OPM's Federal Investigative Services to measure the frequency with which its investigative reports met federal investigative standards in order to improve the completeness – that is, quality – of future investigation documentation. As of March 2013, however, OPM had not implemented this recommendation…. OPM continues to assess the quality of investigations based on voluntary reporting from customer agencies, the number of investigations returned for rework is not by itself a valid indicator of the quality of investigative work..." GAO-13-728T, p. 6-7.

[177] At an October 31, 2013 Senate hearing, Senator Tom Carper noted, " the Department of Justice has joined a lawsuit against...USIS...[which] performs about 45 percent of the background investigations that are contracted out by the Office of Personnel Management. According to this law suit, USIS engaged in a practice that company insiders referred to as 'dumping.' Under this alleged scam, USIS would send investigations back to the Office of Personnel Management even though they had not gone through the full review process. Through this 'dumping,' USIS maximized its profits." ("Opening Statement of Chairman Thomas. R. Carper: 'The Navy Yard Tragedy: Examining Government Clearances and Background Checks,'" Senate Homeland Security and Government Affairs Committee, October 31, 2013.

[178] GAO -08-352T, p. 9.

[179] S. 1197, Sec. 931.

[180] Senate Bill: S 1197 PCS.

[181] "In 2005, the Office of Management and Budget designated OPM as the agency responsible for, among other things, the day-to-day supervision and monitoring of security clearance investigations, and for tracking the results of individual agency-performed adjudications, subject to certain exceptions. However, the Office of the Director for National Intelligence can designate other agencies as "authorized investigative agenc[ies]" pursuant to 50 U.S.C. 435b(b)(3), as implemented through Executive Order 13467." GAO-12-197, 7 footnote 14.

[182] GAO-12-197, p. 7, Footnote 14.

[183] The DoD Independent Review Related to Fort Hood recommendation 2.6a is "revise current policies and procedures to address preventing violence toward others in the workplace" (p. 16).

[184] This DoD effort focuses on connecting DoD component law enforcement elements in specific regions of high-DoD interest to share data with local law enforcement including arrests, bookings, incident narratives, citations, and local warrant information that allows users to connect the dots during investigations. There are ten regions: Northwest, Southern California, Hawaii, Rio Grande (New Mexico), Gulf Coast (Texas), Southeast (Florida and Georgia), Virginia, NCR, and Northeast (Connecticut). The regional effort is known as the Law Enforcement Information Exchange (LInX). D-DEx is, in many ways, the eleventh region of LInX. NCIS is currently the lead agency for both LInX and D-DEx.

[185] The original DoD Independent Review Related to Fort Hood recommendation 2.10 is "Establish a consolidated criminal investigation and law enforcement database such as the Defense Law Enforcement Exchange" (page 19). D-DEx is an investigative tool that allows the sharing of criminal data/information between law enforcement agencies.

[186] NCIS is partnering with the FBI on a similar national-level effort to ensure information sharing between the DoD data exchange and the FBI's National Data Exchange (N-DEx). The greater the connectivity and the more records available to an investigator, the more likelihood that a DoD law enforcement official will be able to connect the dots and give context to the dots during targeted investigations. Additional funding could also address the ingestion of local agency data where there is no current participation in the existing systems.

[187] The DoD Independent Review Related to Fort Hood Recommendation 3.7 is "Review best practices, including programs outside the U.S. Government, to determine whether elements of those programs could be adopted to augment access control protocols to detect persons who pose a threat" (page 32). The Independent Review's recommendation 3.9 is "Develop timely information sharing capabilities among components including vehicle registration, installation debarment lists, and other access control information; accelerate efforts to automate access control that will authenticate various identification media… against authoritative databases; [and] … disseminate information to local commanders to enable screening at … installation access control points" (page 33).

[188] National Defense Authorization Act for Fiscal Year 2008, P. L. 110-181, Section 1069 required the Secretary to develop minimum access control standards no later than January 1, 2009.

[189] Directive-Type Memorandum (DTM) 09-012, "Interim Policy Guidance for DoD Physical Access Control" (Incorporating Change 3. March 19, 2013), Attachment 3, Physical Security Access Control Standards, ¶ 3a(2), p. 12.

[190] The DoD Inspector General issued its report "Navy Commercial Access Control System Did Not Effectively Mitigate Access Control Risks" on September 16, 2013, the day of Aaron Alexis' attack at the Washington Navy Yard. The Commander, Navy Installation Command disputes the findings and specific recommendations regarding a specific Navy program that manages the vetting of commercial vendors, contractors, and suppliers requiring routine access to Navy installations known as "RAPIDgate," but the DoD IG recommended that the Navy Commercial Access Control System be replaced such that access control would at least include vetting through the National Crime Information Center (NCIC).

[191] "Our Mission," National Insider Threat Task Force. http://www.ncix.gov/nittf/index.php.

[192] Erika Harrell, "Workplace Violence Against Government Employees, 1994-2011. Bureau of Justice Statistics April 11, 2013. http://www.bjs.gov/index.cfm?ty=pbdetail&iid=4615.

[193] Mark F. Giuliano Speech at the Washington Institute for Near East Policy Stein Program on counterterrorism and Intelligence. April 14. 2011. Federal Bureau of Investigation Website http://www.fbi.gov/news/speeches/the-post-9-11-fbi-the-bureaus-response-to-evolving-threats.

[194] Remarks of John O. Brennan, Assistant to the President for Homeland Security and Counterterrorism, on Ensuring al-Qa'ida's Demise -- As Prepared for Delivery. Paul H. Nitze School of Advanced International Studies, July 29, 2011. http://www.whitehouse.gov/the-press-office/2011/06/29/remarks-john-o-brennan-assistant-president-homeland-security-and-counter.

[195] Michael Daly, "NSA Surveillance Program Failed to Invade Tamerlan Tsarnaev's Privacy", The Daily Beast, June 12, 2013. http://www.thedailybeast.com/articles/2013/06/12/nsa-surveillance-program-failed-to-invade-tamerlan-tsarnaev-s-privacy.html.

[196] Alexandra Schuster, "Al Qaeda's Inspire Magazine Praises Boston Bombings, Takes credit for Inspiring Suspects", The Huffington Post, May 31, 2013. http://www.huffingtonpost.com/2013/05/31/al-qaeda-inspire-magazine-boston-bombings_n_3367314.html.

[197] Days before the attack al Qaeda leader Ayman Zawahiri issued a videotape calling for a 'lone wolf attack' inside the United States. Gordon Corera, "Al-Qaeda chief Zawahiri urges 'lone-wolf' attacks on US", BBC News, September 13, 2013. http://www.bbc.co.uk/news/world-middle-east-24083314.

[198] "Al-Qaida Leader Called for 'Lone Wolf' Atttack" WND, September 16, 2013. http://www.wnd.com/2013/09/al-qaida-leader-called-for-lone-wolf-attack/.
[199] *Hearing Before The Subcommittee On Counterterrorism And Intelligence Of The Committee On Homeland Security, House Of Representatives*. Jihadist Use Of Social Media—How To Prevent Terrorism And Preserve Innovation. December 6, 2011. http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg74647/pdf/CHRG-112hhrg74647.pdf.
[200] *The Future of Al-Qaeda. Results of A Foresight Project.* Canadian Security Intelligence Service. May 2013. Page 51. and *Is Al Qaeda's Internet Strategy Working?*. Brian Michael Jenkins. The Rand Corporation. December 2011. Testimony presented before the House Homeland Security Committee, Subcommittee on Counterterrorism and Intelligence on December 6, 2011.
[201] *Hearing Before the Senate Committee on Homeland Security and Government Affairs*
The Homeland Threat Landscape and U.S. Response, Director National Counterterrorism Center Matthew G. Olsen, September 19,2012. http://www.dni.gov/files/documents/Newsroom/Testimonies/Olsen%209-19%202012%20SFR.pdf.
[202] [202] *Statement of Robert S. Mueller, III Director of the Federal Bureau of Investigation Before the United States Senate Committee on Appropriations Subcommittee on Commerce, Justice, Science and Related Agencies,* 113th Congress (May 16, 2013).
[203] "Robert Phillip Hanssen Espionage Case" Press Release FBI National Press Office, February 20, 2001. http://www.fbi.gov/about-us/history/famous-cases/robert-hanssen.
[204] *Statement of Robert S. Mueller, III, Director of the Federal Bureau of Investigation Before the United States House of Representatives Committee on Appropriations Subcommitee on Commerce, Justice, Science and Related Agencies.* March 19, 2013. http://www.fbi.gov/news/testimony/protecting-the-nation-in-todays-complex-threat-environment.
[205] "The Super User: Organizations' Biggest Internal Threat". Bank Info Security. September 4, 2007. http://www.bankinfosecurity.com/super-user-organizations-biggest-internal-threat-podcast-transcript-a-556/op-.
[206] Chelsea J. Carter and Susanna Capelouto "Report: NSA, GCHQ among worst surveillance offenders, Snowden says" CNN http://www.cnn.com/2013/11/03/world/europe/edward-snowden-manifesto/.

Chief of Staff
Col Scott Hayford, USAF

Core Staff
Col Edward P. Pernotto, USAFR

Daniel P. Feehan, White House Fellow
MSgt Yolanda Hands, USAF
Erum Jilani, Defense Fellow
Clarissa Kornell, Defense Fellow
Mark Ribbing, OUSD (Policy)

Security Element
Amb Francis X. Taylor

SSA Michael T. Effley, FBI
Lance G. Hampton, PhD, OUSD (Policy)
Lt Col James S. Mehta, USAF

Human Factors Element
CAPT Mike Colston, MD, MC, USN

Wendy Tenhula, PhD

Independent Review of the Washington Navy Yard Shooting

NOVEMBER 2013