



July 2015

INSIDER THREATS

DOD Should Improve Information Sharing and Oversight to Protect U.S. Installations

Accessible Version

GAO Highlights

Highlights of [GAO-15-543](#), a report to the Committee on Armed Services, House of Representatives

Why GAO Did This Study

The attacks at Fort Hood, Texas, on November 5, 2009, and at the Washington Navy Yard, D.C., on September 16, 2013, drew nationwide attention to insider threats at DOD installations. DOD defines an insider threat as the threat that an insider will use her or his authorized access, wittingly or unwittingly, to do harm to the security of the United States.

House report 113-446 included a provision that GAO review DOD's antiterrorism and force protection efforts to address insider threats. This report evaluates the extent to which DOD has (1) reflected insider threat considerations in its force protection policies and other guidance, (2) shared actions that U.S. installations have taken to protect against insider threats, and (3) implemented recommendations from the official reviews of the 2009 Fort Hood and 2013 Washington Navy Yard shootings. GAO reviewed official reviews from the shootings, DOD force protection-related policies, interviewed agency officials, and visited eight nongeneralizable U.S. installations representing all four military services, a joint base, and different geographic locations.

What GAO Recommends

GAO recommends that DOD consistently use existing mechanisms to share information about actions taken to protect against threats, and take steps to improve the consistency of reporting and monitoring of the implementation of the recommendations from the 2009 Fort Hood review. DOD concurred with GAO's recommendations and cited related actions planned or under way.

View [GAO-15-543](#). For more information, contact Joseph W. Kirschbaum at 202-512-9971 or kirschbaumj@gao.gov.

July 2015

INSIDER THREATS

DOD Should Improve Information Sharing and Oversight to Protect U.S. Installations

What GAO Found

Since the 2009 Fort Hood shooting, the Department of Defense (DOD) has made efforts to update 7 of 10 key force protection-related policy and guidance documents and is taking steps to revise the remaining 3 to incorporate insider threat considerations. DOD's Fort Hood independent review recommended that the department develop policy and procedures to integrate disparate efforts to protect DOD resources and people against internal threats. GAO also found that DOD does not have a policy for when it would be appropriate for DOD military and contractor personnel to report to DOD base security officials when an individual is observed carrying a weapon on an installation, especially into a work environment. Senior DOD officials acknowledged this policy gap and agreed to take steps to address the issue.

Officials from the eight U.S. installations GAO visited identified actions taken to protect against insider threats. However, DOD has not consistently shared information across the department about the actions it has taken. DOD has issued guidance and recommendations addressing the 2009 Fort Hood shooting stating that DOD should identify and share leading practices to enhance the department's ability to protect the force. For example, installation officials have trained response personnel on active shooter training and piloted a workplace violence risk assessment program. However, DOD is not sharing all the information about such actions because DOD officials are not consistently using existing mechanisms to share information, such as lessons-learned information systems and antiterrorism web portals. Unless the military services consistently use existing mechanisms to share information on insider threats, U.S. installations may miss opportunities to enhance the department's ability to protect the force against such threats.

DOD has taken actions to implement the recommendations from the official reviews of the 2009 Fort Hood and 2013 Washington Navy Yard shootings. However, GAO was unable to identify the number of the 79 Fort Hood recommendations that were fully implemented because DOD has received inconsistent information from the military services and has conducted limited monitoring of recommendation implementation. For example, DOD and military service officials provided differing responses to a questionnaire on the implementation status of some Fort Hood recommendations. In addition, officials from three military services stated that they generally do not monitor the implementation of the recommendations from the Fort Hood independent review at the installation level. Until DOD and the military services improve the consistency of reporting and monitoring of the implementation of recommendations, DOD will be unable to know whether the deficiencies identified in the official review of the 2009 Fort Hood shooting have been addressed. With regard to the official reviews from the 2013 Washington Navy Yard shooting, DOD has taken initial actions towards implementing the four recommendations prioritized by the Secretary of Defense. For example, DOD issued an implementation plan that identifies milestones, timelines, and resource requirements needed to address the four recommendations.

Contents

Letter	1
Background	5
Majority of DOD’s Key Force Protection–Related Policy and Guidance Have Been Updated, but Some Guidance Do Not Yet Reflect Insider Threat Considerations	11
Selected Installations Have Taken Actions to Protect against Insider Threats, but DOD Has Not Consistently Shared This Information	16
DOD Is in the Process of Implementing Recommendations from the 2009 and 2013 Official Reviews, but Inconsistent Reporting and Limited Monitoring Prevent Status Assessment	21
Conclusions	30
Recommendations for Executive Action	31
Agency Comments and Our Evaluation	31
<hr/>	
Appendix I: Objectives, Scope, and Methodology	34
Appendix II: Department of Defense (DOD) and Service Reviews of the 2009 Fort Hood and 2013 Washington Navy Yard Shootings	40
Appendix III: Comments from the Department of Defense	45
Appendix IV: GAO Contact and Staff Acknowledgments	48
Appendix V: Accessible Data	49
Accessible Text	49
Agency Comments	51
<hr/>	
Related GAO Reports	54
<hr/>	
Tables	
Table 1: Examples of Past Incidents Involving DOD Insider Threats at U.S. Installations	5
Table 2: Examples of Actions Taken by Selected Installations GAO Visited to Protect against Insider Threats	16
<hr/>	
Figures	
Figure 1: Timeline of 2009 Fort Hood and 2013 Washington Navy Yard Shootings and Official Reviews and Related Tasking Memorandums	7

Figure 2: GAO's Framework of Key Elements to Incorporate at Each Phase of DOD's Insider-Threat Programs	10
Accessible Text for Figure 1: Timeline of 2009 Fort Hood and 2013 Washington Navy Yard Shootings and Official Reviews and Related Tasking Memorandums	49
Accessible Text for Figure 2: GAO's Framework of Key Elements to Incorporate at Each Phase of DOD's Insider-Threat Programs	49
Accessible Text for Appendix III: Comments from the Department of Defense	51

Abbreviations

ASD(HD&GS)	Assistant Secretary of Defense for Homeland Defense and Global Security
DOD	Department of Defense
OASD(HD&GS)	Office of the Assistant Secretary of Defense for Homeland Defense and Global Security

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



July 16, 2015

The Honorable Mac Thornberry
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

Violent attacks on U.S. installations have illustrated the danger posed to Department of Defense (DOD) facilities, resources, and personnel—including employees, contractors, dependents, and veterans—from insider threats. DOD defines an insider threat as the threat that an insider will use her or his authorized access, wittingly or unwittingly, to do harm to the security of the United States. Two incidents on U.S. installations drew nationwide attention about insider threats. On November 5, 2009, a lone Army officer shot and killed 13 people and wounded 32 others on-base at Fort Hood, Texas. Almost 4 years later, on September 16, 2013, a Navy contractor killed 12 civilian employees and contractors and wounded 4 others at the Washington Navy Yard, D.C. Insiders have significant advantages over others who intend to harm an organization because insiders may have an awareness of their organization’s vulnerabilities, such as loosely enforced policies and procedures, or exploitable security measures.

Over the years, we have completed a number of reviews related to insider threats. Our past work in 2012 and 2013 on insider threats in Afghanistan reported on the causes of, and safeguards against, insider attacks in Afghanistan and highlighted the need for improved sharing of biometric information and assessment of insider attacks.¹ More recently, we reported on DOD’s efforts to protect its classified information and systems from insider threats and recommended that the department identify an

¹GAO, *Afghanistan Security: New Steps Taken to Address Insider Attacks, but DOD Has Not Always Ensured That Personnel Are Prepared for Casualty Assessment Teams*, GAO-13-838SU (Washington, D.C.: Sept. 30, 2013); *Afghanistan: Key Oversight Issues*, [GAO-13-218SP](#) (Washington, D.C.: Feb. 11, 2013); and *Afghanistan Security: Renewed Sharing of Biometric Data Could Strengthen U.S. Efforts to Protect U.S. Personnel from Afghan Security Force Attacks*, GAO-12-471SU (Washington, D.C.: Apr. 20, 2012). Examples of biometric information include fingerprints, iris scans, and facial photographs.

insider threat program office and issue guidance that would assist DOD components in developing and strengthening insider threat programs.² DOD concurred or partially concurred with our recommendations, stating, among other things, that it will publish a detailed implementation plan in 2015 to assist components in implementing multiple actions required in all insider threat programs.

The House Armed Services Committee report accompanying a bill for the National Defense Authorization Act for Fiscal Year 2015 included a provision that we review DOD's antiterrorism and force protection efforts to address insider threats.³ This report evaluates the extent to which DOD has (1) reflected insider threat considerations in its force protection policies and other guidance, (2) shared actions that U.S. installations have taken to protect against insider threats, and (3) implemented recommendations from the official reviews of the 2009 Fort Hood and 2013 Washington Navy Yard shootings. As discussed with your staff, we focused our review on insider threats to force protection at U.S. installations and did not include DOD's overseas facilities.

To evaluate the extent to which DOD's force protection policies and other guidance reflect insider threat considerations, we obtained and reviewed 10 key DOD policies and other guidance related to force protection, covering a range of topics including counterintelligence, antiterrorism, and installation emergency management. We selected the 10 key policies and other guidance because they were referenced in DOD documents including the department's insider threat directive and the DOD independent and internal reviews of the 2009 Fort Hood and 2013 Washington Navy Yard shootings.⁴ We also verified that these 10 policies and other guidance are key to addressing force protection across the department with officials within the Office of the Assistant Secretary of

²GAO, *Insider Threats: DOD Should Strengthen Management and Guidance to Protect Classified Information and Systems*, [GAO-15-544](#) (Washington, D.C.: June 2, 2015).

³H.R. Rep. 113-446 at 201–202 (2014) accompanying H.R. 4435, a proposed bill for the National Defense Authorization Act for Fiscal Year 2015.

⁴DOD Directive 5205.16, *The DOD Insider Threat Program* (Sept. 30, 2014); Department of Defense, *Protecting the Force: Lessons from Fort Hood, Report of the DOD Independent Review* (January 2010); Department of Defense, *Security from Within: Independent Review of the Washington Navy Yard Shooting* (November 2013); and Department of Defense, *Internal Review of the Washington Navy Yard Shooting, A Report to the Secretary of Defense* (Nov. 20, 2013). See app. I for a list of all 10 key documents.

Defense for Homeland Defense and Global Security (OASD[HD&GS]) and the Office of the Under Secretary of Defense for Intelligence. We reviewed the key policies and other guidance to determine whether DOD had incorporated findings and recommendations from the 2009 Fort Hood independent review related to updating department guidance or incorporated training requirements identified in the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.⁵ We also reviewed DOD Instruction 5025.01, *DOD Issuances Program*, to determine DOD's policies for developing and updating its policies and guidance.⁶ We interviewed officials within the Office of the Secretary of Defense and the military services (the Army, Navy, Marine Corps, and Air Force) to obtain their perspectives on DOD force protection policy and its application to addressing insider threats.

To evaluate the extent to which DOD has shared actions that U.S. installations have taken to protect against insider threats, we selected and conducted site visits at eight nongeneralizable U.S. installations based on whether an installation had a known insider attack since 2009, proximity to other U.S. military installations where known insider attacks occurred, military service representation, joint basing, and geographic representation. Although findings from these eight installations are not generalizable to all installations, they provide context about the actions taken by these selected installations to protect against insider threats. The installations that we selected and visited are: Fort Hood, Texas; Rock Island Arsenal, Illinois; Washington Navy Yard, D.C.; Naval Submarine Base New London, Connecticut; Peterson Air Force Base, Colorado; Joint Base San Antonio, Texas; Marine Corps Base Quantico, Virginia; and the Pentagon, Virginia. From these site visits, we reviewed installation exercise information and after-action reports as well as DOD policies and guidance on antiterrorism, force protection, and lessons learned. We compared information gathered from installation officials on actions taken at their respective installations to DOD guidance containing recommendations for promoting information sharing on actions to protect against insider threats and to federal internal control standards for sharing information within an organization. We also interviewed officials at these

⁵White House, *Memorandum on the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* (Nov. 21, 2012).

⁶DOD Instruction 5025.01, *DOD Issuances Program* (June 6, 2014) (Incorporating change 1, effective Oct. 17, 2014).

installations to discuss efforts to address insider threats at their respective installations. In addition, we conducted interviews with officials from the Office of the Under Secretary of Defense for Intelligence, OASD(HD&GS), and each of the military services to identify actions that the department and military services had taken to address insider threats, such as identifying and sharing any actions to address insider threats.

To evaluate the extent to which DOD has implemented recommendations from the official reviews of the 2009 Fort Hood and 2013 Washington Navy Yard shootings, we evaluated the actions that DOD components had taken in response to reviews that either the Secretary of Defense or Secretary of Navy tasked appropriate DOD components to take as a result of these shootings. Specifically, for the 2009 Fort Hood shooting, we considered the DOD independent review commissioned by the Secretary of Defense and the service internal reviews. Similarly, we considered the DOD internal review and the independent review—both of which were directed by the Secretary of Defense as “official reviews” for the 2013 Washington Navy Yard shooting. We developed and administered questionnaires to the Office of the Under Secretary of Defense for Intelligence and OASD(HD&GS) to gather their responses on the status of implementation of the recommendations. For comparison purposes, we administered the same questionnaires to the military services on the implementation of the DOD independent and internal reviews and any internal reviews that the services may have conducted, and compared the results of these questionnaires to responses provided by OASD(HD&GS). During this comparison, we found some inconsistencies between questionnaire responses provided by OASD(HD&GS) and the questionnaire responses provided by the military services regarding the implementation of recommendations from the official review of the 2009 Fort Hood shooting. We also found limitations in the monitoring of recommendation implementation from that review and are making a recommendation to DOD to improve monitoring. In addition, we consulted with the DOD Office of Inspector General and the Army Audit Agency—both of which were conducting similar reviews during our engagement. We also interviewed DOD officials, DOD working groups, and service officials with knowledge of the recommendations and actions that have been identified or taken to address recommendations from the DOD independent and internal reviews of the 2009 Fort Hood and 2013 Washington Navy Yard shootings. Additional information about our scope and methodology can be found in appendix I.

We conducted this performance audit from June 2014 to July 2015 in accordance with generally accepted government auditing standards.

Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Examples of Insider Threats at U.S. Installations

Insiders have proven to be a threat to DOD facilities and personnel within the United States on multiple occasions. DOD acknowledged in its 2014 Quadrennial Defense Review that the United States is no longer a sanctuary for U.S. forces and the department must anticipate the increased likelihood of an attack on U.S. soil.⁷ Table 1 below provides examples of past incidents involving DOD insider threats at U.S. military installations.

Table 1: Examples of Past Incidents Involving DOD Insider Threats at U.S. Installations

Date	Event description
October 1995	An Army soldier shot at fellow soldiers of the 82nd Airborne Division conducting morning physical training, killing 1 officer and wounding 18 soldiers before being arrested at Fort Bragg, North Carolina.
November 2009	An Army soldier shot at fellow soldiers at a Soldier Readiness Processing Center, killing 13 soldiers and wounding 32 others before being arrested at Fort Hood, Texas.
May 2012	A Navy civilian worker set a fire aboard the USS Miami at Portsmouth Naval Shipyard, Maine, causing about \$700 million in damage, injuring several people, and contributing to the decommissioning of the ship.
March 2013	A Marine shot and killed 2 Marines and then killed himself in a residential barracks at Marine Corps Base Quantico, Virginia.
September 2013	A Navy contractor shot and killed 12 people and wounded 4 others at Washington Navy Yard, D.C. He was shot and killed by law enforcement officers on the scene.
April 2014 [Note A]	An Army soldier shot and killed 3 people and wounded 12 others and then killed himself at Fort Hood, Texas.

Source: GAO analysis of data from the U.S. Senate Committee on Homeland Security and Governmental Affairs, Department of Justice, Federal Bureau of Investigation, Department of Defense (DOD), and the military services. | GAO-15-543

Note A: DOD publically issued its report into the investigation of the April 2014 shooting at Fort Hood in January 2015. As a result, we did not include the April 2014 shooting in our evaluation.

⁷Department of Defense, *Quadrennial Defense Review* (Mar. 4, 2014).

Reviews of the 2009 Fort Hood and 2013 Washington Navy Yard Shootings

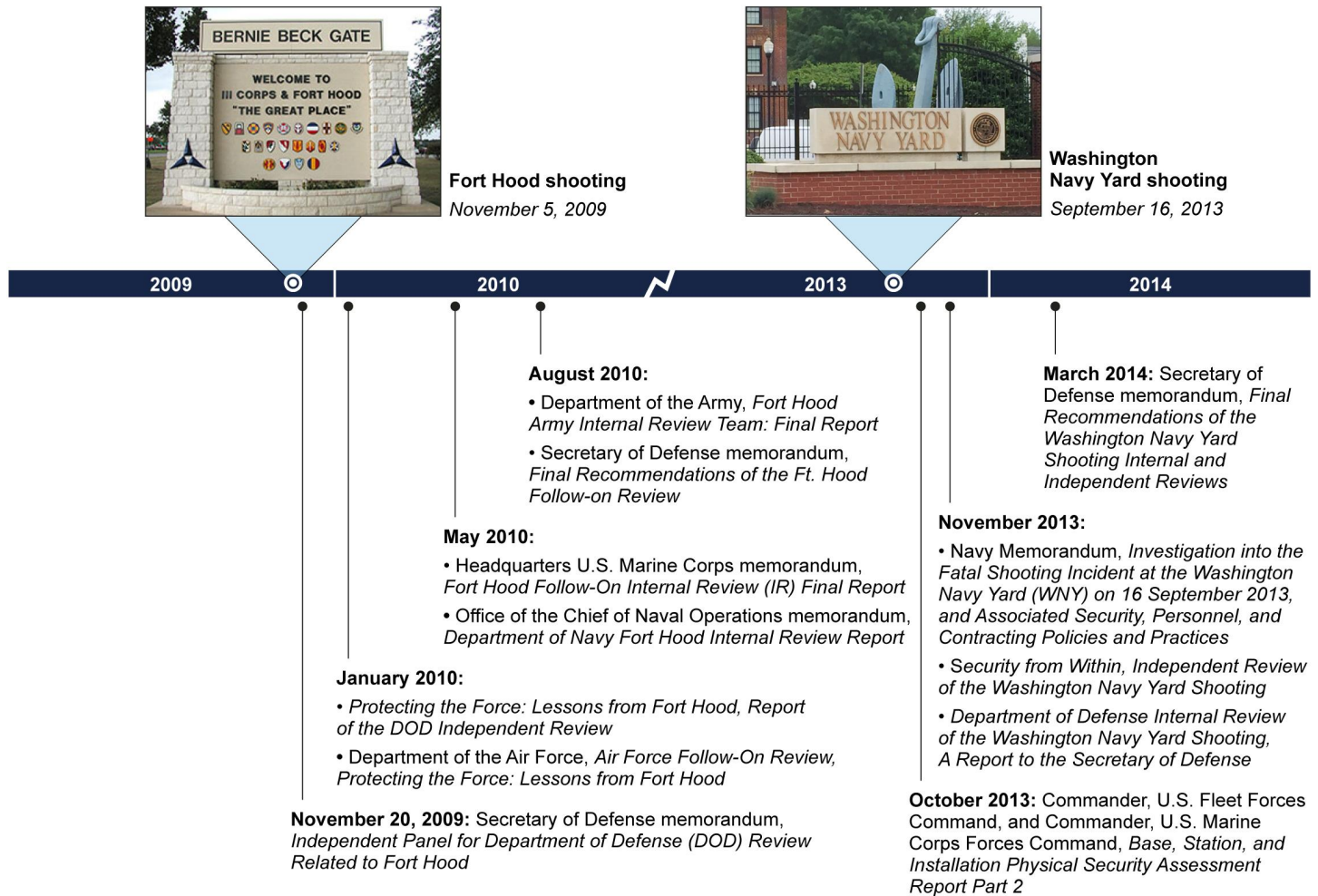
DOD and the military services completed a series of reviews after the 2009 Fort Hood shooting and the 2013 Washington Navy Yard shooting that led to the recommendations that the Secretary of Defense and Secretary of Navy tasked the department and Navy, respectively, to implement. Specifically, in response to the 2009 Fort Hood shooting, the Secretary of Defense directed the department to conduct an independent review of the incident. The results of this independent review, which were released in January 2010, identified 79 recommendations that the department could take to address findings associated with personnel policies, force protection, emergency and mass casualty response, and support to DOD healthcare providers.⁸ In response to the 2013 Washington Navy Yard shooting, the Secretary of Defense directed an independent review and an internal review of the incident to identify and recommend actions to address gaps or deficiencies in DOD programs, policies, or procedures regarding security at DOD installations and the granting and renewing of security clearances for DOD employees and contractor personnel.⁹ Both the Washington Navy Yard independent review and internal review were released in November 2013 and identified actions that were intended to improve DOD's force protection posture from insider threats.¹⁰ In March 2014, the Secretary of Defense directed DOD to implement four key recommendations that were a compilation of a number of recommendations from the Washington Navy Yard independent review and internal review. Similarly, the Department of the Navy conducted two internal service reviews in response to the Washington Navy Yard shootings. As a result, the Navy issued two reports with recommendations to the Navy and Marine Corps. Figure 1 shows a timeline of DOD's and the military services' reviews of the 2009 Fort Hood and 2013 Washington Navy Yard shootings. See appendix II for more information about these reviews.

⁸DOD, *Protecting the Force: Lessons from Fort Hood, Report of the DOD Independent Review*.

⁹Secretary of Defense Memorandum, *Department of Defense Independent Review of the Washington Navy Yard Shooting* (Sept. 30, 2013).

¹⁰DOD, *Security from Within: Independent Review of the Washington Navy Yard Shooting*; and DOD, *Internal Review of the Washington Navy Yard Shooting, A Report to the Secretary of Defense*. The independent review made 30 recommendations while the internal review made 73 recommendations.

Figure 1: Timeline of 2009 Fort Hood and 2013 Washington Navy Yard Shootings and Official Reviews and Related Tasking Memorandums



Source: GAO analysis of DOD information. | GAO-15-543

DOD Efforts to Establish an Insider Threat Program

In light of these insider attacks on U.S. installations and as part of its response to an executive order and national insider threat policy directing federal agencies to develop insider threat programs, DOD is developing

its own insider threat program.¹¹ Specifically, in September 2014, DOD issued a directive establishing a department-wide insider threat program that identifies policy and assigns responsibilities.¹² Among other things, the directive states that appropriate DOD policies shall be evaluated and modified to effectively address insider threats to DOD.

There are a number of DOD officials and organizations that have a role in protecting personnel, facilities, and resources on U.S. installations from insider threats. For example:

- The Under Secretary of Defense for Intelligence serves as the principal staff assistant to the Secretary of Defense with responsibility for personnel security and issuing department-wide guidance regarding insider threats. The Secretary of Defense also tasked the Under Secretary to oversee the implementation of the four recommendations and three studies that the Secretary of Defense directed DOD to undertake based on the independent review and internal review of the 2013 Washington Navy Yard shooting.
- The Assistant Secretary of Defense for Homeland Defense and Global Security (ASD [HD&GS]), within the Office of the Under Secretary of Defense for Policy, has responsibility for updating DOD antiterrorism policy.¹³ The Secretary of Defense also tasked the Assistant Secretary to oversee the implementation of the recommendations that were identified in the independent review of the 2009 Fort Hood shooting and the military service follow-on reviews.
- Military services are responsible for executing portions of the recommendations from the independent review of the 2009 Fort Hood shooting, funding certain programs that address insider threats, and executing DOD-wide policy and guidance.

¹¹Executive Order No. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, 76 Fed. Reg. 198 (Oct. 7, 2011); and White House memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* (Nov. 21, 2012).

¹²DOD Directive 5205.16, *The DOD Insider Threat Program*.

¹³In January 2015, the Office of the Under Secretary of Defense for Policy reorganized its missions and renamed the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs as the Assistant Secretary of Defense for Homeland Defense and Global Security. For the purpose of consistency, we will refer to the position in this report by its current title—the Assistant Secretary of Defense for Homeland Defense and Global Security.

-
- Geographic combatant commands have the primary responsibility for setting force protection postures and guidance in their areas of responsibility.

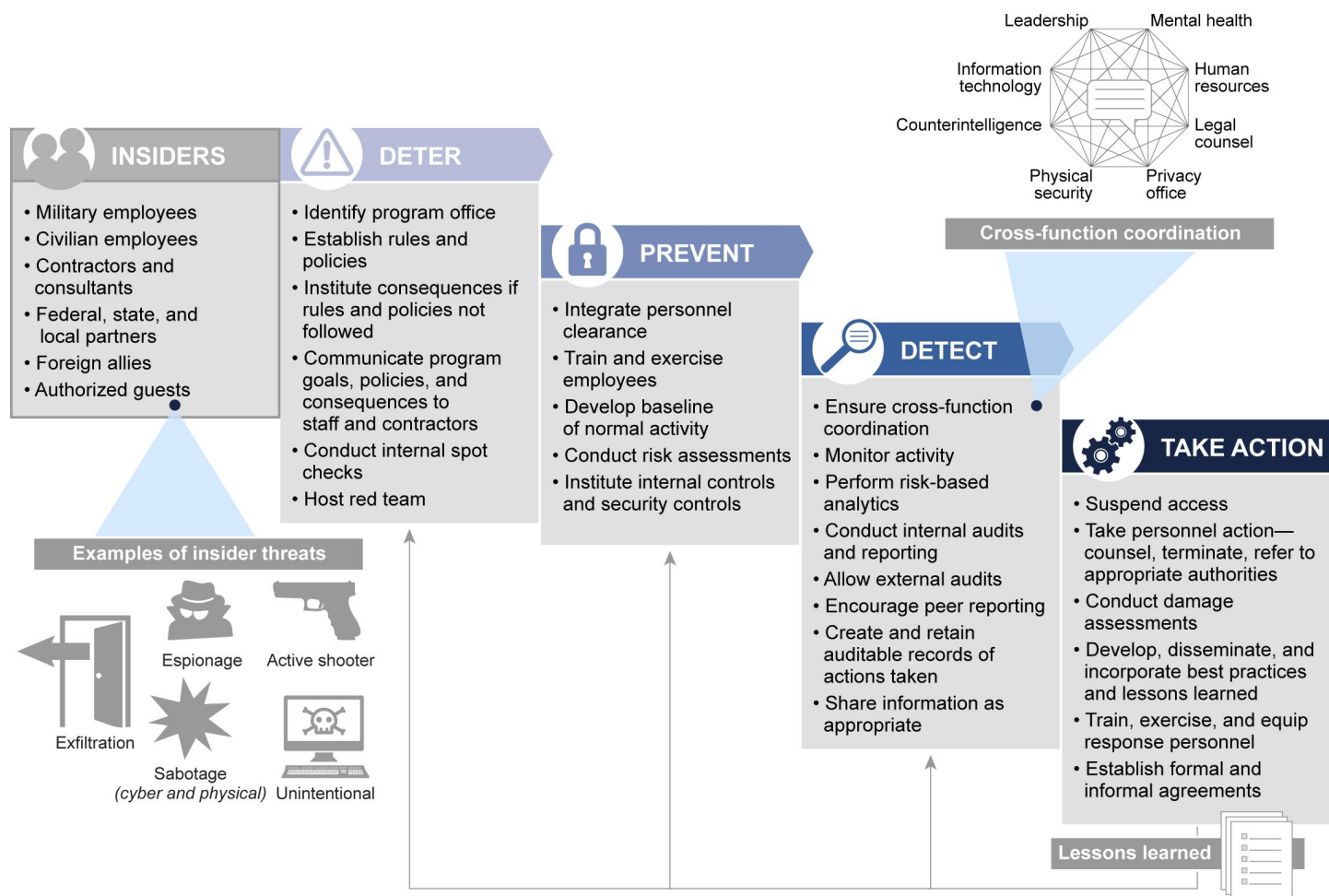
GAO Insider Threat Framework

We have previously reported that DOD should incorporate 25 key elements into DOD components' insider threat programs.¹⁴ We identified these key elements based on our analysis of the National Insider Threat Policy and Minimum Standards for Executive Agencies, DOD policy and guidance, executive-branch policy and reports, and independent studies to mitigate insider threats. As shown in figure 2 below, these key elements include training employees, issuing guidance, equipping response personnel, and establishing formal and informal agreements. While we developed the framework during our review of DOD's efforts to protect classified information and systems from insider threats, the framework is also applicable to DOD's efforts to protect U.S. installations from insider threats. For example, the following DOD policy and guidance documents and reviews support each of the phases of the framework: DOD Instruction 1438.06, *DOD Workplace Violence Prevention and Response Policy*; DOD Instruction 2000.12, *DOD Antiterrorism (AT) Program*; DOD Instruction 2000.16, *DOD Antiterrorism (AT) Standards*; DOD Instruction 2000.26, *Suspicious Activity Reporting*; DOD 5200.08-R, *Physical Security Program*; DOD Instruction 5525.15, *Law Enforcement (LE) Standards and Training in the DOD*; DOD Instruction 5240.22, *Counterintelligence Support to Force Protection*; DOD Instruction 6055.17, *Installation Emergency Management (IEM) Program*; Joint Publication 3-07.2, *Antiterrorism*; Directive Type Memorandum 09-012, *Interim Policy Guidance for DOD Physical Access Control*; and the findings and recommendations identified in the independent and internal reviews conducted in response to the 2009 Fort Hood and 2013 Washington Navy Yard shootings. In addition to these documents, our 2015 report, *Insider Threats: DOD Should Strengthen Management and Guidance to Protect Classified Information and Systems*, identifies documents that support the need to protect personnel and property on U.S. installations in addition to protecting classified information and systems. For example, DOD Directive 5240.06, *Counterintelligence Awareness and Reporting*, and DOD Instruction 5240.26, *Countering Espionage, International Terrorism, and the Counterintelligence (CI)*

¹⁴[GAO-15-544](#).

Insider Threat, identify procedures that would protect classified information, personnel, and real property from insider threats.

Figure 2: GAO’s Framework of Key Elements to Incorporate at Each Phase of DOD’s Insider-Threat Programs



Source: GAO analysis of Department of Defense (DOD), U.S. government, and private-sector guidance and reports. | GAO-15-543

Majority of DOD's Key Force Protection–Related Policy and Guidance Have Been Updated, but Some Guidance Do Not Yet Reflect Insider Threat Considerations

We found that 7 of 10 force protection–related DOD policy and guidance documents incorporated insider threat considerations; however, the 3 other documents do not reflect insider threat considerations.¹⁵ Specifically, we found that these 3 policy and other guidance documents did not cover all DOD employees that could become either an insider threat or a victim of such a threat, did not identify multiple types of insider threat scenarios, or did not incorporate insider threats into their training requirements. In addition, we identified a potential policy gap in providing information on reporting certain types of suspicious activities to base security personnel, which DOD officials acknowledged and were taking steps to address in light of our finding.

Seven DOD Key Force Protection–Related Policy and Guidance Documents Incorporate Insider Threat Considerations

We found that seven DOD policies and other guidance documents related to force protection incorporated insider threat considerations. Specifically, these seven DOD policies and other guidance address antiterrorism, security, and counterintelligence issues that are intended to protect the department's personnel, facilities, and resources.

- **Joint Publication 3-07.2, *Antiterrorism***, sets forth joint doctrine to provide the fundamental tenets for planning, executing, and assessing joint antiterrorism programs.¹⁶ In 2014, DOD updated the joint publication to identify active shooter and other insider threats as common terrorist tactics, techniques, and procedures, among other things. For example, the joint publication states that an insider threat can include active shooters and bombers that use improvised explosive devices to create additional victims or to impede first responders to the scene of the incident.
- **DOD Instruction 2000.12, *DOD Antiterrorism (AT) Program***, establishes and prescribes procedures for the DOD antiterrorism program.¹⁷ The instruction was updated in 2013 to clarify the geographic combatant commanders' authority to set force protection

¹⁵As noted in the independent review of the 2009 Fort Hood shooting, DOD does not have a single force protection policy. Therefore, we identified and verified with DOD officials 10 key force protection-related policy and guidance documents that could be used to address insider threats.

¹⁶Chairman of the Joint Chiefs of Staff, Joint Publication 3-07.2, *Antiterrorism* (Mar. 14, 2014).

¹⁷DOD Instruction 2000.12, *DOD Antiterrorism (AT) Program* (Mar. 1, 2012) (incorporating change 1, Sept. 9, 2013).

conditions in their areas of responsibility in response to recommendations from the 2009 Fort Hood shooting.

- **DOD Instruction 2000.26, *Suspicious Activity Reporting (SAR)***, establishes policy and procedures for implementing eGuardian as the DOD law enforcement suspicious activity reporting system.¹⁸ In addition, the instruction, which was updated in 2014, identifies responsibilities, such as the development of component-specific suspicious activity awareness campaigns, that DOD components should implement.¹⁹ The instruction refers to insider threats and also provides categories of suspicious activities. These categories include threats to DOD personnel, efforts to recruit personnel to collect information on DOD functions and procedures, and testing security measures at DOD installations in an effort to discover vulnerabilities.
- **DOD Directive 5200.43, *Management of the Defense Security Enterprise***, provides direction for a comprehensive Defense Security Enterprise policy, oversight framework, and governance structure to safeguard personnel and resources against harm, loss, or hostile acts and influences.²⁰ The directive requires the Defense Security Enterprise Executive Committee—which advises the Under Secretary of Defense for Intelligence—to, among other things, develop a Defense Security Enterprise framework that aligns with and is informed by insider threat initiatives and policy.
- **DOD Directive 5240.06, *Counterintelligence Awareness and Reporting (CIAR)***, establishes policy, assigns responsibilities, and provides procedures for counterintelligence awareness and reporting to include listing reportable indicators and behaviors associated with foreign intelligence entities.²¹ The directive includes specific references to counterintelligence insider threats and lists examples of reportable DOD employee behavior and activities such as advocating violence on behalf of a known or suspected international terrorist organization, advocating support for a known or suspected

¹⁸DOD Instruction 2000.26, *Suspicious Activity Reporting (SAR)* (Sept. 23, 2014). eGuardian is a Federal Bureau of Investigation system that DOD, among others, uses to manage, share, and store suspicious activity reports from law enforcement organizations and units.

¹⁹DOD Instruction 2000.26, enc. 2, § 5.j.

²⁰DOD Directive 5200.43, *Management of the Defense Security Enterprise* (Oct. 1, 2012) (incorporating change 1, Apr. 24, 2013).

²¹DOD Directive 5240.06, *Counterintelligence Awareness and Reporting (CIAR)* (May 17, 2011) (incorporating change 1, May 30, 2013).

international terrorist organization, or any attempt to recruit personnel for terrorist activities.²² The directive also incorporates insider threat awareness training into requirements for counterintelligence awareness training. For example, the directive states that the annual counterintelligence awareness training for all DOD employees should include instruction on the counterintelligence insider threat, methods of foreign intelligence entities, and reporting requirements on the list of indicators and behaviors.

- **DOD Instruction 5240.22, *Counterintelligence Support to Force Protection***, assigns responsibilities and lays out procedures for conducting and managing counterintelligence support to force protection programs of the DOD components and other supported elements within DOD.²³ While the instruction does not explicitly identify insider threats, it identifies the responsibilities and procedures for addressing international terrorist threats, terrorist-enabling individuals, and organizations threatening DOD interests—areas that could include individuals who are insider threats and are associated with foreign terrorist entities.
- **DOD Instruction 5240.26, *Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat***, establishes policy and assigns responsibilities for the counterintelligence insider threat program in support of other DOD insider threat programs.²⁴ The instruction includes specific references to counterintelligence insider threats and lays out procedures for reporting and processing threats from unidentified individuals affiliated with DOD who are believed to have a relationship with a foreign intelligence entity. The instruction directs the Director, Defense Intelligence Agency, to incorporate counterintelligence insider threat awareness into counterintelligence awareness and reporting training in accordance with DOD Directive 5240.06.

²²DOD defines a counterintelligence insider threat as a person who uses his or her authorized access to DOD facilities, personnel, systems, equipment, information, or infrastructure to damage and disrupt operations, compromise DOD information, or commit espionage on behalf of a foreign intelligence entity.

²³DOD Instruction 5240.22, *Counterintelligence Support to Force Protection* (Sept. 24, 2009) (incorporating change 1, Oct. 15, 2013).

²⁴DOD Instruction 5240.26, *Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat* (May 4, 2012) (incorporating change 1, Oct. 15, 2013).

DOD Is Updating Three Documents That Do Not Reflect Insider Threat Considerations and Addressing a Policy Gap for Reporting Someone Carrying a Weapon on an Installation

We found that, as of May 2015, three DOD policies and other guidance documents related to force protection did not incorporate insider threat considerations; additionally, DOD did not have a policy on when DOD military and contractor employees should report individuals observed carrying weapons on an installation. We found the following:

- **DOD Instruction 1438.06, *DOD Workplace Violence Prevention and Response Policy***, establishes policy and assigns responsibilities for workplace violence prevention and response regarding DOD civilian personnel.²⁵ The instruction, which was issued in 2014, does not explicitly identify insider threats but does direct the department to prevent and report incidents involving violence, threats, harassment, intimidation, and other disruptive behavior from civilian employees. These types of activities could be considered insider threat concerns. The instruction also requires all supervisors to immediately report threats of workplace violence to their management and appropriate military or civilian authorities as determined by local threat reporting protocols. However, the policy applies only to DOD civilian employees and does not apply to military and contractor personnel who could also become potential insider threats. DOD officials told us that the department is drafting a memorandum that will expand this instruction to cover all employees.
- **DOD Instruction 2000.16, *DOD Antiterrorism (AT) Standards***, identifies minimum antiterrorism standards, such as training standards, that DOD components must apply in the development of their individual antiterrorism programs and plans.²⁶ We found that the instruction, which has not been updated since either the 2009 Fort Hood or the 2013 Washington Navy Yard shootings, does not identify insider threats as one of the minimum antiterrorism awareness training requirements.²⁷ DOD is in the process of updating this instruction and has included “insider threat and active shooter attacks”

²⁵DOD Instruction 1438.06, *DOD Workplace Violence Prevention and Response Policy* (Jan. 16, 2014).

²⁶DOD Instruction 2000.16, *DOD Antiterrorism (AT) Standards* (Oct. 2, 2006).

²⁷DOD Instruction 2000.16 outlines the minimum training requirements for Level I Antiterrorism Awareness Training, including topics such as an introduction to terrorism, individual protective measures, improvised explosive device attacks, kidnapping and hostage survival, and an explanation of terrorism threat levels, among others. DOD provides Level I Antiterrorism Awareness Training in a classroom or computer-based setting or by viewing a video.

as a minimum training requirement in a draft version of the instruction.²⁸

- **DOD Instruction 6055.17, *DOD Installation Emergency Management (IEM) Program***, establishes policy and prescribes procedures for developing, implementing, and sustaining installation emergency management programs at DOD installations worldwide for all-hazards threats.²⁹ While the instruction, which has not been updated since 2010, does not explicitly reference insider threats, it highlights workplace violence and active shooter incidents as threats that have the potential to affect military installations and thus should be included in an installation's emergency management program. These threats could be considered insider threat concerns. However, the instruction does not identify other insider threat scenarios that have the potential to affect military installations, such as the use of a vehicle-borne improvised explosive device or a personal-borne improvised explosive device. DOD's joint guidance on antiterrorism recognizes that an insider threat could use improvised explosive devices to create additional victims, to impede first responders, or both. DOD is in the process of updating this instruction and included "improvised explosive device response" as a minimum capability assessment requirement in a draft version of the instruction.³⁰

In addition, we found that DOD does not have a policy in place for military personnel and DOD affiliated-contractors to provide guidance on when it would be appropriate to report to base security officials when an individual is observed carrying a weapon on an installation, especially into a work environment. Senior officials within OASD(HD&GS) acknowledged that the issue is not addressed in DOD policy for military personnel and DOD-affiliated contractors and told us that their intent is to incorporate such guidance into DOD Instruction 5200.08 on DOD's physical security

²⁸Officials within the Office of the Under Secretary of Defense for Policy told us they were in the process of updating this instruction and expect the revised version to be issued by June 2015.

²⁹DOD Instruction 6055.17, *DOD Installation Emergency Management (IEM) Program* (Jan. 13, 2009) (incorporating change 1, Nov. 19, 2010). DOD defines all hazards as any incident, natural or manmade, that warrants action to protect the life, property, health, and safety of military members, dependents, and civilians at risk, and minimize any disruptions of installation operations.

³⁰Officials within the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics told us they were in the process of updating this instruction, but could not provide an estimated time frame of when the instruction would be reissued.

program, which is currently under revision. If DOD addresses the policy gap on carrying weapons and issues updated policies on workplace violence prevention, antiterrorism standards, and installation emergency management to incorporate insider threats, the department will be better positioned to have clear and current policy and accurate procedures to prevent, detect, deter, and take actions in response to insider threats on U.S. installations.

Selected Installations Have Taken Actions to Protect against Insider Threats, but DOD Has Not Consistently Shared This Information

The eight installations we visited have taken actions to protect against insider threats. However, DOD has not consistently shared information about these actions throughout the department because DOD personnel have not consistently used existing mechanisms.

Installations Have Taken Actions to Protect against Insider Threats

During our visits to eight U.S. installations, we identified actions that installation officials had taken to protect against insider threats, as shown in table 2.

Table 2: Examples of Actions Taken by Selected Installations GAO Visited to Protect against Insider Threats

Categories of actions	Examples of actions taken
Establish rules and policies	<ul style="list-style-type: none"> Issued a handbook for installation supervisors on installation incident response plans Issued a handbook to share with local law enforcement to facilitate active shooter training and response Issued guidance on screening of non-DOD personnel accessing installation-controlled areas
Conduct internal spot checks	<ul style="list-style-type: none"> Used random antiterrorism measures
Train and exercise employees	<ul style="list-style-type: none"> Trained on suspicious activity and counterintelligence activity reporting Exercised to respond to active shooter scenarios
Conduct risk assessments	<ul style="list-style-type: none"> Implemented a workplace violence risk assessment pilot program
Ensure cross-function coordination	<ul style="list-style-type: none"> Established working groups with threat management capabilities

Categories of actions	Examples of actions taken
Train, exercise, and equip response personnel	<ul style="list-style-type: none"> • Trained and exercised response personnel on active shooter scenarios • Used vacant buildings on installation to facilitate active shooter training for law enforcement and security personnel • Provided body armor and rifles to installation security and law enforcement personnel • Upgraded installation radio systems to allow for interoperable communication for first responders
Establish formal and informal agreements	<ul style="list-style-type: none"> • Developed formal agreements with local law enforcement, fire, and medical emergency responders

Source: GAO analysis of DOD Information. | GAO-15-543

The following are some specific examples we found during our eight site visits:

- **Establish Rules and Policies.** Officials at four installations told us they issued guidance documents to protect against active shooters and other potential insider threats. For example, Peterson Air Force Base developed an active shooter response book that officials shared with local law enforcement to facilitate training and response to incidents. Rock Island Arsenal and Washington Navy Yard developed and issued handbooks that guide personnel to protect against active shooters and other insider threats. Specifically, Rock Island Arsenal issued a handbook for supervisory personnel on how to respond to on-base incidents. At Washington Navy Yard, officials told us they issued a handbook that guides law enforcement personnel by providing information about behavioral indicators of potential insider threats and actions when responding to an active shooter or a bomb threat.
- **Train and Exercise Employees.** All eight installations had trained and exercised personnel to report suspicious activities, report potential counterintelligence activities, and respond to active shooters, according to installation officials. To encourage suspicious activity and counterintelligence activity reporting, officials at Marine Corps Base Quantico told us they used media, briefings to new hires, and presentations to on-base school students to remind employees and military dependents about the base's suspicious activity program. Officials at Rock Island Arsenal told us they provide antiterrorism training that is tailored for each unit. In addition, officials at Fort Hood told us they encourage personnel to use a social media webpage to report suspicious activities. To facilitate response efforts, officials at

four installations told us they also use realistic training environments. For example, installation officials at Peterson Air Force Base and Naval Submarine Base New London told us they use buildings that contain cubicles to train installation security personnel on active shooter response. Officials at Naval Submarine Base New London and Marine Corps Base Quantico also told us they use blank and simulated ammunition to make training more realistic.

- **Train, Exercise, and Equip Response Personnel.** Officials at three installations we visited told us that additional equipment was provided to installation security forces personnel in order to respond to and protect against active shooters and insider threats. For example, officials at Fort Hood told us that after the 2009 Fort Hood shooting, they provided installation security personnel with supplemental weapons and body armor to respond to active shooters. Officials at Joint Base San Antonio also told us that they had procured upgrades on locks and doors for certain facilities to protect against active shooters. In addition, officials at Washington Navy Yard told us they upgraded their installation radio system to have interoperable communications for all first responders on the installation and within Naval District Washington.
- **Establish Formal and Informal Agreements.** Seven of the eight installations we visited have established formal agreements, such as memorandums of agreement or mutual aid agreements, with fire and medical emergency responders, and local law enforcement. Officials at three installations also told us they had developed informal relationships with local law enforcement and emergency responders. For example, officials at Fort Hood told us they regularly meet with local law enforcement officials. Also, officials at Rock Island Arsenal told us they participate in a monthly local area emergency management forum. Naval Criminal Investigative Service officials at Naval Submarine Base New London also told us they attend a monthly local and state law enforcement conference focused on both internal and external threats in the area. Officials at the Pentagon Force Protection Agency told us they have relationships with other organizations within the National Capital Region—such as the Naval Criminal Investigative Service—which helps facilitate information sharing on potential threats in the area.
- **Other Actions Taken.** Officials at the eight installations we visited also told us of other actions they had taken to protect against insider threats. Such actions include using random antiterrorism measures, installing installation mass notification systems, and piloting a workplace violence risk assessment program. For example, officials at Joint Base San Antonio told us about a pilot program they developed to assess the potential risk for workplace violence within units. At the

time of our visit, officials at Joint Base San Antonio had tested the pilot program on 17 units at the base with the goal to expand the pilot.

DOD Has Not Consistently Shared Actions to Protect against Insider Threats

While the U.S. installations we visited have taken actions to protect against insider threats, military services have not consistently shared this information across the department because DOD officials are not consistently using existing information sharing mechanisms. Such mechanisms include working groups, conferences, lessons-learned information systems, and antiterrorism web portals.

- **Working groups.** DOD officials told us that working groups are one mechanism used to share information across organizations and at installations. However, we found that some of the installations we visited were not consistently using working groups to share information. For example, we found that Air Force officials at Joint Base San Antonio were not aware and had not received a copy of an after-action report that an Army tenant on the installation had completed after an individual with access to the installation shot an employee on the installation. Air Force officials were not aware of this report and its recommendations even though they are responsible for security on the Joint Base because the installation command had not set up a working group with tenant officials where such information could have been shared.
- **Conferences.** DOD officials told us that leading practices and lessons learned formerly were exchanged at DOD antiterrorism conferences. However, DOD and two of the military services cancelled their annual antiterrorism conferences from 2013 to 2014 because of limited funding and increased scrutiny of conferences. The Army reinitiated its antiterrorism conference in 2015 and an Air Force official told us that the service is considering merging antiterrorism and other force protection issues into a mission assurance conference going forward.
- **Lessons-learned information systems.** The Joint Staff and each of the military services have established information systems to exchange information on lessons from training, exercises, and combat operations across the department. However, military service and installation officials told us they do not consistently use joint or military service lessons-learned information systems. Officials told us they do not use these systems because they believed the information within the systems focuses more on military combat operations, there is not a requirement to use the systems to share information on insider threats, and there is limited time or desire to use the systems. When we examined the joint lessons-learned information system, we found examples of information contained in the system that installations

could use to enhance their efforts to protect against insider threats. For example, we found two after-action reports that highlight lessons learned on active shooter exercises conducted at two installations within the United States.

- **Antiterrorism web-based portals.** The Joint Staff established an antiterrorism web-based, secure portal in 2003 to provide a collaborative environment for the DOD community to share antiterrorism and force protection information with the military services, combatant commands, and other DOD agencies. The portal contains links to various antiterrorism organizations, communities, and other force protection portals. However, service and installation officials told us they either were not aware of or did not use the Joint Staff's antiterrorism portal. Marine Corps and Army officials told us that they use their service-specific antiterrorism portals. When we examined the Army's antiterrorism enterprise portal we found examples of information contained in the system that installations could use to enhance their efforts to protect against insider threats. For example, the Army's antiterrorism enterprise portal contained documentation on mitigating insider threats and antiterrorism best practices.

DOD guidance and recommendations issued after the 2009 Fort Hood shooting state that DOD should identify and share leading practices to enhance the department's ability to protect the force. For example, DOD's joint guidance on antiterrorism states that after-action reports and lessons learned should be shared with other units and defense components.³¹ Also, in 2014, the Chairman of the Joint Chiefs of Staff recommended that the department share innovative measures to prevent and respond to attacks similar to those at Fort Hood and the Washington Navy Yard.³² Further, the independent review of the 2009 Fort Hood shooting encouraged the department to identify best practices to enhance the department's ability to protect the force. Similarly, in 2015, we reported that DOD components did not have or use a formalized process to develop, disseminate, and incorporate best practices and lessons learned in their insider-threat program.³³ According to federal internal control

³¹ Joint Publication 3-07.2, *Antiterrorism*.

³² Chairman of the Joint Chiefs of Staff Info Memo, *Results of CJCS-directed Internal Review of the 2 April 2014 Fort Hood Shooting Incident* (Washington, D.C.: Apr. 30, 2014).

³³ [GAO-15-544](#).

standards, communication and information sharing should occur in a broad sense with information flowing down, across, and up an organization with management ensuring there are adequate means of communicating with, and obtaining information from, external stakeholders who may have a significant effect on the achievement of goals.³⁴ Unless the military services share information across the department on insider threats by consistently using existing mechanisms, U.S. installations may miss opportunities to enhance the department's ability to protect the force against such threats.

DOD Is in the Process of Implementing Recommendations from the 2009 and 2013 Official Reviews, but Inconsistent Reporting and Limited Monitoring Prevent Status Assessment

DOD has taken actions to implement the recommendations from the official reviews of the 2009 Fort Hood and 2013 Washington Navy Yard shootings; however, we were unable to identify the number of Fort Hood recommendations fully implemented because DOD and the military services had inconsistently reported this information and have conducted limited monitoring of recommendation implementation. DOD, as well as the Navy and Marine Corps, have also taken initial actions towards implementing the recommendations that were tasked by the Secretary of Defense and the Secretary of the Navy in response to the official reviews of the 2013 Washington Navy Yard shooting. For example, DOD issued an implementation plan in June 2014 that stated it will take years to implement the recommendations approved by the Secretary of Defense.

DOD Has Taken Actions to Implement Fort Hood Recommendations

We found that DOD has taken a number of actions to implement recommendations from the DOD independent review of the 2009 Fort Hood shooting. For example, in response to recommendations stemming from the 2009 Fort Hood shooting, DOD revised policies in areas such as suspicious activity reporting, counterintelligence, and emergency management.³⁵ In September 2014, as part of its effort to address a

³⁴GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: Nov. 1999).

³⁵DOD Instruction 2000.26, *Suspicious Activity Reporting (SAR)*; DOD Directive 5240.06, *Counterintelligence Awareness and Reporting (CIAR)*; and DOD Instruction 6055.17, *DOD Installation Emergency Management (IEM) Program*.

recommendation that DOD integrate its disparate efforts to defend against internal threats, DOD established policy and assigned responsibilities for a DOD insider threat program.³⁶ Also, in response to a recommendation to examine the feasibility of advancing procurement and deployment of mass warning systems, military service officials informed us that they were provided with additional funding to install mass notification systems and enhanced 911 systems.³⁷ In response to our questionnaire provided to DOD and the services on the implementation of recommendations, DOD reported the Marine Corps installed mass notification systems at all of its installations, and the Navy and Air Force installed the systems at over 90 percent of their installations. DOD also reported that the Army fielded mass notification systems at locations that provide warning to over 80 percent of Army personnel. Likewise, DOD reported that all the services have installed enhanced 911 capabilities to varying degrees at their installations. For example, the Marine Corps installed enhanced 911 capabilities at all its installations, whereas the Army has completed fielding at 18 installations covering 54 percent of its population, and the Air Force has established enhanced 911 capabilities at 71 installations covering 64 percent of its population. The Navy reported that it has been hampered in fielding enhanced 911 systems at its installations because of aging infrastructure, among other factors, but expects to have enhanced 911 systems on its installations by September 2015.

In December 2014, the ASD(HD&GS) directed the Deputy Assistant Secretary of Defense for Defense Continuity & Mission Assurance to visit a sampling of installations to determine the effectiveness of policies issued since the 2009 Fort Hood shooting. In response to this tasking, the Deputy Assistant Secretary assembled key personnel from the Office of the Secretary of Defense staff, to include the Under Secretaries of Defense for Intelligence, for Personnel and Readiness, and for Acquisition, Technology, and Logistics; the Joint Staff; the military

³⁶DOD Directive 5205.16, *The DOD Insider Threat Program*.

³⁷Mass notification systems, also referred to as mass notification and warning systems, provide warning and response direction to all personnel within 10 minutes of an incident. Enhanced 911 is a capability that provides emergency responders with the location of, and callback number for, a person making a 911 emergency call. Prior to the 2009 Fort Hood shooting, DOD did not have a policy that required DOD bases to have an emergency contact system that identifies location and a callback number—a capability that is common for 911 systems outside of military installations.

services; and the Defense Threat Reduction Agency to conduct these courtesy visits. According to OASD(HD&GS) officials, the team completed visits to the four selected installations—Joint Base Andrews, Maryland; Marine Corps Base Quantico, Virginia; Fort Bragg, North Carolina; and Naval Station Mayport, Florida—by June 2015. In commenting on a draft of this report, DOD stated that the Mission Assurance Senior Steering Group plans to share best practices and lessons learned gathered from these site visits to strengthen DOD insider threat efforts and help prevent future tragedies such as the Fort Hood shootings.

Inconsistent Reporting of Information and Limited Monitoring Hampers an Assessment of Fort Hood Recommendation Implementation

DOD reported that, as of March 2015, the department had fully implemented 73 of the 79 recommendations identified in the Fort Hood independent review—and approved by the Secretary of Defense—and was taking actions on the other 6 recommendations.³⁸ However, we were unable to confirm the number of recommendations fully implemented because DOD and the military services were inconsistently reporting information and had conducted limited monitoring of recommendation implementation. Specifically, we found the following:

- **Inconsistent reporting of recommendation implementation.** Although DOD officials told us that as many as 73 of the 79 recommendations from the review of the 2009 Fort Hood shooting had been closed as implemented, we were unable to verify these had been implemented because DOD and the military services provided us inconsistent reporting of recommendations implemented. We identified the following two factors as potentially contributing to DOD's inconsistent reporting of recommendations implemented. First, the military services reported the status of recommendations based on service-level implementation rather than department-level implementation. For example, in response to a recommendation for the department to revise current policies and procedures to address preventing violence toward others in the workplace, DOD closed the recommendation as implemented by issuing a policy on workplace violence prevention and response in January 2014.³⁹ However, the Army and the Air Force reported that they were still taking action to

³⁸Secretary of Defense Memorandum, *Final Recommendations of the Ft. Hood Follow-on Review* (Aug. 18, 2010).

³⁹DOD Instruction 1438.06, *DOD Workplace Violence Prevention and Response Policy*.

address this recommendation based on the need to update their service-level implementing policies. Second, DOD reported that it closed recommendations that were partially under way, although the services reported such actions as in progress. DOD reported that it closed 10 recommendations that the military services were tasked to lead or support on behalf of the department even though all the military services reported they had not fully implemented the 10 recommendations. For example, DOD reported that it had closed a recommendation that the services were to review senior medical officers' requirements to optimize utilization and assignments. While three services reported to us that they had implemented this recommendation, one service reported that it had not completed implementation. Similarly, DOD reported closing a recommendation that the services were to update policies to reflect current DOD-level guidance on the release of protected health information. While two services reported to us that they had implemented this recommendation, the other two services reported that they had not completed implementation. Further, according to DOD officials, DOD reported closing recommendations based on preliminary rather than final actions taken by DOD. For example, in response to a recommendation to improve efforts for sharing access control information, DOD stated it was developing a new guidance document; however, this guidance document is still in draft form and has not gone through the Federal Register process, according to DOD officials. Therefore, this recommendation should not have been considered fully implemented by DOD.

The Army Audit Agency and the DOD Inspector General cited similar concerns in three recent reports about the reliability of the status of Fort Hood recommendation implementation. In December 2012, the Army Audit Agency issued a report that assessed the Army headquarters' progress in implementing recommendations from DOD's review of the 2009 Fort Hood shooting. The Army Audit Agency concluded that the intentions of 13 recommendations stemming from the 2009 Fort Hood shooting were not met by the Army, and recommended that the Army reopen the recommendations and continue to monitor implementation.⁴⁰ A February 2015 Army Audit Agency report, which examined whether nine selected Army installations had sufficiently implemented 18 selected Fort Hood

⁴⁰U.S. Army Audit Agency, *Army Headquarters-Level Actions to Implement Fort Hood Recommendations* (Dec. 18, 2012).

recommendations, also noted that the Army may have prematurely closed 4 recommendations in addition to the 13 recommendations identified in the 2012 audit.⁴¹ The Army Audit Agency also found only 1 of 18 selected recommendations from the review of the 2009 Fort Hood shooting was fully implemented at the nine Army installations that the agency visited even though 11 of the 18 recommendations had been closed by the Army. In discussions with officials from the DOD Office of Inspector General about their ongoing review of DOD's workplace violence prevention program, the DOD Inspector General found that DOD has not developed a comprehensive workplace violence prevention program, which resulted in the military services and the Defense Threat Reduction Agency using different approaches to address workplace violence. DOD Office of Inspector General officials told us this occurred, in part, because DOD did not exercise sufficient oversight to ensure the Fort Hood and Defense Science Board recommendations were properly addressed and closed.⁴²

- **Limited monitoring.** We also were unable to confirm the number of Fort Hood recommendations implemented because DOD and the military services have conducted limited monitoring of the status of recommendations from the review of the 2009 Fort Hood shooting. DOD has established a mechanism and process for reviewing the status of recommendations at the department level. Specifically, the Deputy Assistant Secretary of Defense for Defense Continuity and Mission Assurance has convened monthly meetings for the Mission Assurance Coordination Boards' Fort Hood Working Group to monitor implementation of the remaining Fort Hood recommendations. According to OASD(HD&GS) officials, the Fort Hood Working Group provides regular briefings to the Mission Assurance Coordination Boards' senior leaders and they discuss whether specific

⁴¹U.S. Army Audit Agency, *Army Installation-Level Actions to Address Fort Hood Report Recommendations* (Feb. 4, 2015). The Army Audit Agency did not make a recommendation in this matter because Army officials reopened the recommendations during the course of the audit.

⁴²Officials from the DOD Office of Inspector General told us that their review included an examination of recommendations resulting from the Fort Hood independent review related to workplace violence and focused on the military services; Defense Threat Reduction Agency; Joint Base Lewis-McChord, Washington; and Travis Air Force Base, California. This included recommendations 2.1a, 2.1c, 2.1d, 2.6a and 2.6b, 2.16, 3.1a, 3.2a through 3.2c, and 4.3a through 4.3d. For example, recommendation 2.6b from the Fort Hood independent review directs the department to integrate existing programs such as suicide, sexual assault, and family violence prevention with information on violence and self-radicalization to provide a comprehensive prevention and response program.

recommendations should be closed as implemented or remain open as an effort in continued progress. However, we found that DOD was not monitoring implementation of the Fort Hood recommendations at the military service and installation levels. Specifically, officials from OASD(HD&GS) told us that DOD—through the Mission Assurance Coordination Boards—has not been monitoring implementation of actions from military service follow-on reviews of the 2009 Fort Hood shooting. According to the 2013 DOD Mission Assurance Strategy Implementation Framework, the Mission Assurance Coordination Boards’ initial objectives included ensuring completion of all Fort Hood independent review activities as directed by the Secretary of Defense. In 2010, the Secretary of Defense issued a memorandum that tasked the ASD(HD&GS)—one of two key leaders of the Mission Assurance Coordination Boards—to report on progress made by the military services.⁴³ Officials from OASD(HD&GS) told us they did not monitor the progress of the military services’ efforts to take action based on their internal reviews of the 2009 Fort Hood shooting and that they believed the services were in the best position to report on their progress on implementing recommendations.⁴⁴ However, these officials acknowledged that the Assistant Secretary’s monitoring responsibility was never removed by the Secretary of Defense. Also, while OASD(HD&GS) officials believe that services are in the best position to report on their progress on implementing recommendations, we found that the services were not consistently monitoring the implementation of recommendations at their installation levels. For example, service headquarters officials from three services told us that they generally do not monitor implementation of the recommendations from the reviews of the 2009 Fort Hood shooting at the installation level. As previously stated, a February 2015 Army

⁴³Secretary of Defense Memorandum, *Final Recommendations of the Ft. Hood Follow-on Review*.

⁴⁴Department of the Army, *Fort Hood Army Internal Review Team: Final Report* (Washington, D.C.: Aug. 4, 2010); Headquarters US Marine Corps Memorandum, *Fort Hood Follow-On Internal Review (IR) Final Report* (Washington, D.C.: May 26, 2010); Office of the Chief of Naval Operations Memorandum, *Department of Navy Fort Hood Internal Review Report* (Washington, D.C.: May 28, 2010); Department of the Air Force, *Air Force Follow-On Review Protecting the Force: Lessons from Fort Hood* (Washington, D.C.: 2010). The Army and Air Force follow-on reviews also identified key actions and recommendations that those two services could respectively take to address findings from Fort Hood. All of the Army’s key actions and the vast majority of the Air Force’s recommendations were intended to further recommendations coming out of DOD’s independent review of the 2009 Fort Hood shooting.

Audit Agency report found that the Army had prematurely closed recommendations related to the 2009 Fort Hood shooting, based on the Army Audit Agency's review of implementation of 18 selected Fort Hood recommendations at nine selected installations. Officials from OASD(HD&GS) acknowledged that periodic reports from the military services would provide the Mission Assurance Coordination Boards with a more complete understanding of the extent to which the military services have implemented the recommendations from the 2009 Fort Hood shooting.

According to federal internal control standards, program managers need operational data to determine whether they are meeting their agencies' goals for accountability and such pertinent information should be identified, captured, and distributed in a form and time frame that permits people to perform their duties efficiently.⁴⁵ Internal control standards also state that monitoring of internal control should assess the quality of performance over time and ensure that the findings of reviews are promptly resolved. Until the military services provide the Mission Assurance Coordination Boards consistent reporting of information on the implementation of recommendations, DOD will not be able to ensure the reliability of its reporting on the status of the recommendations from the official review of the 2009 Fort Hood shooting. Further, until the Mission Assurance Coordination Boards and military services consistently monitor Fort Hood recommendation implementation at the service and installation level, DOD will be unable to know whether the deficiencies identified in the independent review of the 2009 Fort Hood shooting have been addressed on U.S. installations. In addition, by improving consistent reporting of information and monitoring—such as through developing criteria for consistent reporting on the progress of recommendations and having the military services provide periodic status reports—DOD will be better positioned to provide complete and accurate information in its report to Congress on Fort Hood recommendation implementation as required by the Carl Levin and Howard P. “Buck” McKeon National Defense Authorization Act for Fiscal Year 2015.⁴⁶

⁴⁵[GAO/AIMD-00-21.3.1](#).

⁴⁶See Pub. L. No. 113-291, § 2871 (2014) which requires the Secretary of Defense to submit a report to the congressional defense committees no later than April 30, 2015, on the status of the action taken by DOD in response to the recommendations of the reviews following the Fort Hood and Washington Navy Yard shootings. According to DOD officials, DOD is planning to submit the report in September 2015.

DOD Has Taken Initial Actions to Implement Washington Navy Yard Recommendations

In response to the official reviews from the 2013 Washington Navy Yard shootings,⁴⁷ the Secretary of Defense and the Secretary of the Navy issued memorandums directing DOD components to implement the recommendations and provide progress reports on the status of the recommendations.⁴⁸ The department has taken initial actions towards implementing the four recommendations that were tasked by the Secretary of Defense. For example, in June 2014, DOD issued an implementation plan that lays out major milestones, timelines, responsibilities, and resource requirements needed to address the findings and four recommendations.⁴⁹ According to the implementation plan, implementation of these four recommendations will take years to complete. For example, the plan calls for funding and fielding of an Identity Matching Engine for Security and Analysis system at DOD installations through fiscal year 2019 and beyond.⁵⁰ Nonetheless, DOD has begun to undertake actions identified in this plan. The following are examples of DOD's initial efforts:

- In response to a recommendation to field the Identity Matching Engine for Security and Analysis system, DOD installed the system at 127 Air Force and Defense Logistics Agency sites as of June 2015 with plans

⁴⁷DOD, *Security from Within: Independent Review of the Washington Navy Yard Shooting*; DOD, *Internal Review of the Washington Navy Yard Shooting, A Report to the Secretary of Defense*; Department of the Navy, Commander, U.S. Fleet Forces Command, and Commander, U.S. Marine Corps Forces Command, *Base, Station, and Installation Physical Security Assessment Report Part 2* (Oct. 31, 2013); and Department of the Navy, Office of the Chief of Naval Operations, *Investigation into the Fatal Shooting Incident at the Washington Navy Yard (WNY) on 16 September 2013 and Associated Security, Personnel, and Contracting Policies and Practices* (Nov. 8, 2013).

⁴⁸Secretary of Defense Memorandum, *Final Recommendations of the Washington Navy Yard Shooting Internal and Independent Reviews* (Mar. 18, 2014); Secretary of the Navy Memorandum, *Investigation into the Fatal Shooting Incident at the Washington Navy Yard on September 16, 2013* (Nov. 12, 2013); and Chief of Naval Operations Memorandum, *Base, Station, and Installation Physical Security Assessment Report* (Dec. 24, 2013).

⁴⁹This plan was completed by a task force that was established by the Under Secretary of Defense for Intelligence, with representatives from the Secretaries of the military departments, the Chairman of the Joint Chiefs of Staff, the DOD Inspector General, the Under Secretary of Defense for Personnel and Readiness, the DOD Comptroller, the Director of Cost Assessment and Program Evaluation, and the Director of Administration and Management.

⁵⁰The Identity Matching Engine for Security and Analysis is a system that supports physical access management activities including verifying credentials by drawing information from various data sources such as criminal databases.

to roll out the system to the rest of the department through fiscal year 2019 and beyond.

- In response to a recommendation to implement continuous evaluation, the Washington Navy Yard Task Force Implementation Plan stated that the department was going to meet this recommendation by enhancing the throughput capacity of DOD's existing first-generation Automated Continuing Evaluation System while concurrently developing the system's next generation. According to the Implementation Plan and DOD officials, the department is piloting the enhanced first-generation system and is developing a second generation of the system.⁵¹
- In response to a recommendation to create a DOD Insider Threat Management and Analysis Center, the Under Secretary of Defense for Intelligence has directed the Director of the Defense Security Service to establish the center. We previously reported in June 2015 that DOD had not issued a concept of operations and other planning documents that identify the center's actual functions, scope, level of involvement expected from DOD components, level of DOD involvement, depth of analysis to be completed at the center, and the relationship between the center and the services' existing threat-analysis centers.⁵² In response to a draft of this report, DOD provided a draft version of the concept of operations that the department plans to publish in the summer of 2015. According to DOD officials, the concept of operations, in combination with a DOD instruction on DOD Insider Threat Management and Analysis Center operations, will facilitate the analysis and response functions critical to identifying and mitigating the threat posed by insiders.
- DOD has initiated efforts to address a recommendation to centralize authority and accountability under the Under Secretary of Defense for Intelligence as the principal staff assistant to the Secretary of Defense for insider threat issues. Specifically, in 2014, DOD issued Directive

⁵¹The Automated Continuing Evaluation System is an automated system that facilitates assessments between formal investigations of whether individuals should continue to have access to classified information. The system has access to over 40 databases and is anticipated to assist DOD with earlier detection of insider threats when fully operational. In an April 2015 GAO report, we found that executive-branch agencies face challenges in implementing certain aspects of the 2012 Federal Investigative Standards, including establishing a continuous evaluation policy. GAO, *Personnel Security Clearances: Funding Estimates and Government-Wide Metrics Are Needed to Implement Long-Standing Reform Efforts*, GAO-15-179SU (Washington, D.C.: Apr. 23, 2015).

⁵²[GAO-15-544](#).

5205.16 that states that the Under Secretary of Defense for Intelligence serves as the senior official and principal civilian advisor to the Secretary of Defense on the DOD Insider Threat Program.

Similarly, the Navy and Marine Corps have taken actions toward implementing the 2013 Washington Navy Yard recommendations that were tasked by the Secretary of Navy. For example, the Navy has developed specific training material on the principles of its personnel security program and force protection. Also, according to Marine Corps officials, all Marine Corps installations are now conducting active shooter training as part of their annual exercises. While the services have taken these initial actions, as of March 2015, the Navy reported that it had implemented 12 (15 percent) of 79 recommendations from the internal base security report, the Marine Corps reported that it had fully implemented 9 (31 percent) of the 29 recommendations identified in the internal base security report, and we found that the Navy had fully implemented 13 (87 percent) of the 15 recommendations identified in the in-depth assessment of the events leading up to and during the Washington Navy Yard incident.⁵³

Conclusions

The insider attacks at Fort Hood in 2009 and the Washington Navy Yard in 2013 claimed the lives of 25 people and wounded 36 others, highlighting the need for DOD to address threats to U.S. installations by those personnel with authorized access. While we found that 3 of the 10 key force protection policy and guidance documents do not address insider threat considerations, DOD is taking steps to update these documents. Addressing gaps we identified in these 3 documents as well as addressing the policy gap we identified would provide DOD components with clearer and more comprehensive procedures for preventing, detecting, deterring, and taking actions in response to insider threats at U.S. installations.

Installations we visited have taken actions to protect against insider threats, such as training personnel on active shooter scenarios. However, until DOD more consistently shares leading practices and lessons learned on actions taken to protect against insider threats through the consistent

⁵³During DOD's review of a draft of this report, in June 2015, Navy officials reported taking additional actions on some recommendations including drafting policy and guidance, conducting a study of small-arms qualification, and establishing a process for coordination on more comprehensive installation local threat assessments.

use of existing information-sharing mechanisms, commanders and DOD leadership might miss opportunities to enhance force protection against insider threats at installations across the United States.

Finally, DOD has taken actions to implement recommendations in the wake of the 2009 Fort Hood and 2013 Washington Navy Yard shootings, such as establishing active shooter training. Because the military services have not provided the Mission Assurance Coordination Boards consistent information on the status of Fort Hood recommendation implementation, DOD is hampered in its ability to assess the extent to which it can deter, prevent, detect, and take action to counter insider threats where it matters most—at the installation level. Until the Mission Assurance Coordination Boards and the military services provide consistent reporting of information and conduct improved monitoring of recommendation implementation, the department will be unable to capitalize on the progress it has made and will be unable to assess whether efforts to mitigate the risk of insider threats to DOD personnel and installations in the United States have been achieved.

Recommendations for Executive Action

To assist U.S. installations in protecting against insider threats, we recommend that the Secretary of Defense direct the military services to share information about actions U.S. installations have taken to address insider threats by consistently using existing mechanisms—such as working groups, lessons-learned information systems, and antiterrorism web portals.

To assist DOD leadership in their oversight and decision-making process, we recommend that the Secretary of Defense direct the DOD leaders on the Mission Assurance Coordination Boards and the military services to take steps to improve the consistency of reporting and monitoring of the implementation of recommendations from the independent review of the 2009 Fort Hood shooting. Such steps could include DOD and the military services developing criteria for consistent reporting on the progress of recommendations and the military services providing periodic reports to the Mission Assurance Coordination Boards on the status of Fort Hood recommendations at the service level and installation level.

Agency Comments and Our Evaluation

We provided a draft of this report to DOD for comment. In its written comments, which are reprinted in appendix III, DOD concurred with the two recommendations and cited actions the department is currently taking to address the recommendations. The Departments of Homeland Security

and Justice reviewed a draft of this report but did not provide any comments.

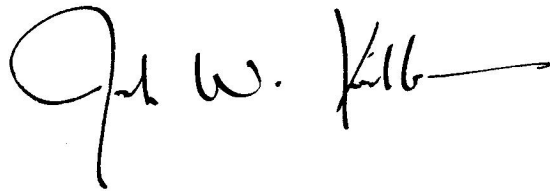
In response to our recommendation that the Secretary of Defense direct the military services to share information about actions U.S. installations have taken to address insider threats by consistently using existing mechanisms, DOD stated that the department has working groups in place within the Office of the Under Secretary of Defense for Intelligence and the Mission Assurance Senior Steering Group that act as venues for sharing best practices and lessons learned related to insider threats. DOD also stated that it conducted a series of site visits to installations and that the Mission Assurance Senior Steering Group will share the best practices and lessons learned from those visits with the DOD components. These are helpful steps toward identifying and sharing information to support the department's effort to address insider threats. However, the information-sharing actions that DOD identified in its comments are actions that are occurring at senior DOD levels and not at the installation level. In addition, DOD stated that it established a DOD insider threat website within the past year that is a potential source for components seeking the latest insider threat information. However, during our visits to selected installations, officials we spoke with did not mention this website. Therefore, we continue to believe that it is important for DOD to continue the progress it has made by increasing communication about the existence of the department's resources for sharing information on best practices and lessons learned, such as this website, down to the military services and installations.

In response to our recommendation that the Secretary of Defense direct the DOD leaders on the Mission Assurance Coordination Boards and the military services to take steps to improve the consistency of reporting and monitoring of the implementation of recommendations, DOD stated that the Mission Assurance Senior Steering Group will monitor the status of Fort Hood recommendations at the military service level to ensure full implementation. To the extent that the senior steering group monitors the military services, DOD will be better positioned to have situational awareness of the rate at which the services have implemented the recommendations. However, in its comments to the draft report, DOD did not state whether the military services will take steps to improve their monitoring of recommendation implementation at the installation level. We believe it remains important for the military services to extend efforts to monitor recommendation implementation at the installation level. This will better position the military services and DOD to know whether

problems or deficiencies associated with prior insider attacks have been addressed.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, the Secretary of Homeland Security, the Attorney General of the United States, and other interested parties. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff members have any questions about this report, please contact me at (202) 512-9971 or kirschbaumj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

A handwritten signature in black ink that reads "Joseph W. Kirschbaum" followed by a long horizontal flourish.

Joseph W. Kirschbaum
Director, Defense Capabilities and Management

Appendix I: Objectives, Scope, and Methodology

This report evaluates the extent to which the Department of Defense (DOD) has (1) reflected insider threat considerations in its force protection policies and other guidance, (2) shared actions that U.S. installations have taken to protect against insider threats, and (3) implemented recommendations from the official reviews of the 2009 Fort Hood and 2013 Washington Navy Yard shootings. As discussed with your committee, we focused our review on insider threats to force protection at U.S. installations and did not include DOD's overseas facilities.

To evaluate the extent to which DOD force protection policies and other guidance reflect insider threat considerations, we obtained and reviewed 10 key DOD policies and other guidance documents related to force protection. We selected the 10 key policies and other guidance documents by reviewing the DOD Directive 5205.16, *The DOD Insider Threat Program*, and the DOD independent and internal reviews of the 2009 Fort Hood and 2013 Washington Navy Yard shootings for references to policies and guidance related to force protection.¹ We verified these 10 policies and other guidance documents with officials within the Office of the Assistant Secretary of Defense for Homeland Defense and Global Security (OASD[HD&GS]) and the Office of the Under Secretary of Defense for Intelligence as key to addressing force protection across the department.

The 10 policies and other guidance documents we selected were

1. Chairman of the Joint Chiefs of Staff, Joint Publication 3-07.2, *Antiterrorism* (Mar. 14, 2014);
2. DOD Instruction 1438.06, *DOD Workplace Violence Prevention and Response Policy* (Jan. 16, 2014);
3. DOD Instruction 2000.12, *DOD Antiterrorism (AT) Program* (Mar. 1, 2012) (incorporating change 1, effective Sept. 9, 2013);

¹DOD Directive 5205.16, *The DOD Insider Threat Program* (Sept. 30, 2014); Department of Defense, *Draft DOD Insider Threat Implementation Plan* (Oct. 21, 2014); Department of Defense, *Protecting the Force: Lessons from Fort Hood, Report of the DOD Independent Review* (January 2010); Department of Defense, *Security from Within: Independent Review of the Washington Navy Yard Shooting* (November 2013); and Department of Defense, *Internal Review of the Washington Navy Yard Shooting, A Report to the Secretary of Defense* (Nov. 20, 2013).

4. DOD Instruction 2000.16, *DOD Antiterrorism (AT) Standards* (Oct. 2, 2006) (incorporating change 1, effective Dec. 8, 2006);
5. DOD Instruction 2000.26, *Suspicious Activity Reporting (SAR)* (Sept. 23, 2014);
6. DOD Directive 5200.43, *Management of the Defense Security Enterprise* (Oct. 1, 2012) (incorporating change 1, effective Apr. 24, 2013);
7. DOD Directive 5240.06, *Counterintelligence Awareness and Reporting (CIAR)* (May 17, 2011) (incorporating change 1, effective May 30, 2013);
8. DOD Instruction 5240.22, *Counterintelligence Support to Force Protection* (Sept. 24, 2009) (incorporating change 1, effective Oct. 15, 2013);
9. DOD Instruction 5240.26, *Countering Espionage, International Terrorism, and the Counterintelligence Insider (CI) Threat* (May 4, 2012) (incorporating change 1, effective Oct. 15, 2013); and
10. DOD Instruction 6055.17, *DOD Installation Emergency Management (IEM) Program* (Jan. 13, 2009) (incorporating change 1, effective Nov. 19, 2010).

We reviewed the key policies and other guidance documents to determine whether DOD had reviewed and updated them to incorporate

- recommendations from the independent review of the 2009 Fort Hood shooting that directed the department to integrate force protection efforts, such as developing policy and procedures to defend against insider threats;²
- insider threat considerations based on annual review requirements outlined in DOD Instruction 5025.01, *DOD Issuances Program*;³ and
- requirements for four minimum training topics addressing insider threat awareness: the importance of detecting potential insider threats by cleared employees and reporting suspected activity to insider threat personnel or other designated officials; methodologies of adversaries to recruit trusted insiders and collect classified

²Department of Defense, *Protecting the Force: Lessons from Fort Hood, Report of the DOD Independent Review*.

³DOD Instruction 5025.01, *DOD Issuances Program* (June 6, 2014) (incorporating change 1, effective Oct. 17, 2014).

information; indicators of insider threat behavior and procedures to report such behavior; and counterintelligence and security reporting requirements.⁴

We also interviewed officials within the Office of the Secretary of Defense and the military services (the Army, Navy, Marine Corps, and Air Force) to obtain their perspectives on DOD force protection policy and its application to addressing insider threats.

To evaluate the extent to which DOD has shared actions that U.S. installations have taken to protect against insider threats, we selected and conducted site visits at eight military installations located in the United States. Although findings from these eight installations are not generalizable to all installations, they provide context about the actions taken by these selected installations to protect against insider threats. In selecting installations to visit, we developed a methodology that included installations that experienced insider attacks since 2009—Fort Hood and Washington Navy Yard—as well as a selection of installations that have not had an attack during this period. We also included the Pentagon in our selection of installations to visit based on it being a high-value installation as the headquarters of the Department of Defense. We used the Department of Defense military installations website (www.militaryinstallations.dod.mil) as the source of information for the universe of military installations. We determined the list of installations on this website to be sufficiently reliable as a source of information on U.S. installations for each of the military services for the purposes of site selection. We based our selection of installations that have not had an insider attack since 2009 on proximity to Fort Hood and Washington Navy Yard and proximity to GAO office locations. In addition, we considered military service representation, joint basing, and geographic representation based on U.S. Census regions as additional selection criteria.⁵ Based on these considerations, we selected five additional installations—one from each military service and one joint base—to visit from our universe of installations. For the purpose of site selection, we focused on active-duty military installations and did not select Reserve and National Guard installations, military service depots, or recruiting

⁴White House, *Memorandum on the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* (Nov. 21, 2012).

⁵The U.S. Census Bureau divides the United States into four separate regions, which include the Northeast, Midwest, South, and West regions.

stations and commands as part of our review. In order to avoid duplication of effort with other ongoing DOD Inspector General work reviewing DOD's efforts to address workplace violence prevention, we did not include two installations—Joint Base Lewis-McChord and Travis Air Force Base. Based on this methodology, we selected the following installations to visit: Fort Hood, Texas; Rock Island Arsenal, Illinois; Washington Navy Yard, D.C.; Naval Submarine Base New London, Connecticut; Peterson Air Force Base, Colorado; Joint Base San Antonio, Texas; Marine Corps Base Quantico, Virginia; and the Pentagon, Virginia.

As part of our site visits, we reviewed installation exercise information and after-action reports provided to us by installation officials, as well as DOD policies and guidance on antiterrorism, force protection, and lessons learned. We compared information gathered from installation officials on actions taken at their respective installation to DOD guidance containing recommendations for promoting information sharing on measures to address insider threats, and to federal internal control standards for sharing information within an organization.⁶ We also conducted interviews with officials from the Office of the Under Secretary of Defense for Intelligence, OASD(HD&GS), and each military service headquarters to determine what actions the department and military services have taken to address insider threats, including the identification and sharing of any measures to address insider threats across the department. Further, we interviewed officials at the eight selected U.S. installations to discuss their knowledge of efforts to protect against insider threats at their respective installations.

To determine the extent to which DOD has implemented recommendations from the official reviews of the 2009 Fort Hood and 2013 Washington Navy Yard shootings, we evaluated the actions that DOD components had taken in response to reviews that either the Secretary of Defense or Secretary of Navy tasked appropriate DOD components to take as a result of the 2009 Fort Hood shooting and the 2013 Washington Navy Yard shooting. Specifically, for the 2009 Fort Hood shooting, we considered the DOD independent review commissioned by the Secretary of Defense and the service internal reviews that were directed by the Secretary of Defense as “official

⁶GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: November 1999).

reviews” for the 2009 Fort Hood shooting. Similarly, we considered the DOD internal review and the independent review—both of which were directed by the Secretary of Defense—and the two Navy internal reviews directed by the Secretary of the Navy as “official reviews” for the 2013 Washington Navy Yard shooting. In addition, we sent two separate questionnaires about the two shootings to OASD(HD&GS) and the Office of the Under Secretary of Defense for Intelligence. In addition, we sent the military services copies of the two questionnaires and requested information on the implementation status at the military service level of each recommendation from the Fort Hood and Washington Navy Yard reviews. For each of the Fort Hood and Washington Navy Yard recommendations, DOD and the military services were asked to state whether no actions had been taken; efforts had been taken, but the recommendation had not been fully implemented; the recommendation was fully implemented; or the recommendation was closed without implementation. We compared the questionnaire responses from OASD(HD&GS) to the responses from the military services and found that we were unable to confirm the number of recommendations fully implemented by DOD and the military services for the Fort Hood independent review because they were inconsistently reporting information and had conducted limited monitoring of recommendation implementation. For example, DOD officials reported that as many as 73 of the 79 recommendations from the review of the 2009 Fort Hood shooting had been closed as implemented, but this reporting was not consistent with responses from the military services. Further, although we reviewed these 79 recommendations and determined that the military services were tasked to lead or support at least 16 of the Fort Hood recommendations, DOD and military service officials provided differing questionnaire responses on the implementation status of 10 recommendations that the military services were tasked lead or support.

In addition to this analysis, we also reviewed the military services' internal reviews of the incidents.⁷ We analyzed documents from and interviewed military service officials to better understand the services' efforts to address insider threats and the recommendations from service internal reviews. We conducted interviews with officials from the Office of the Under Secretary of Defense for Intelligence, the OASD(HD&GS), the Department of the Navy, each military service headquarters, and eight selected U.S. installations to review the extent to which DOD has implemented recommendations from official reviews of the 2009 Fort Hood and 2013 Washington Navy Yard shootings. We also interviewed officials from the Department of Homeland Security and Federal Bureau of Investigation to understand the extent to which they supported DOD in implementing recommendations from the official reviews. Finally, we consulted with officials from the DOD Office of Inspector General and Army Audit Agency—both of whom were conducting similar reviews during our engagement—and obtained documents from those two agencies.

We conducted this performance audit from July 2014 to July 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

⁷Department of the Army, *Fort Hood Army Internal Review Team: Final Report* (Aug. 4, 2010); Department of the Navy, Headquarters U.S. Marine Corps Memorandum, *Fort Hood Follow-On Internal Review (IR) Final Report* (May 26, 2010); Department of the Navy, *Department of Navy Fort Hood Internal Review Report* (May 28, 2010); Department of the Air Force, *Air Force Follow-On Review Protecting the Force: Lessons from Fort Hood* (2010); Commander, U.S. Fleet Forces Command, and Commander, U.S. Marine Corps Forces Command, *Base, Station, and Installation Physical Security Assessment Report Part 2* (Oct. 31, 2013); Department of the Navy, *Investigation into the Fatal Shooting Incident at the Washington Navy Yard (WNY) on 16 September 2013 and Associated Security, Personnel, and Contracting Policies and Practices* (Washington, D.C.: Nov. 8, 2013).

Appendix II: Department of Defense (DOD) and Service Reviews of the 2009 Fort Hood and 2013 Washington Navy Yard Shootings

Independent Review of 2009 Fort Hood Shooting

In the wake of the 2009 Fort Hood shooting, the Secretary of Defense directed an independent review of the incident to determine whether there were programs, policies, and procedural weaknesses within DOD that created vulnerabilities to the health and safety of the department's employees and their families.¹ Specifically, the Secretary of Defense asked the independent review panel to identify and address (1) possible gaps, deficiencies, or both in DOD's programs, processes, and procedures related to identifying DOD employees who could potentially pose credible threats to themselves or others; (2) the sufficiency of DOD's force protection programs; (3) the sufficiency of DOD's emergency response to mass casualty situations at DOD facilities; and (4) the response to care for victims and families in the aftermath of a mass casualty situation. The results of the independent review, which were released in January 2010, identified 79 recommendations that the department should take to address findings associated with personnel policies, force protection, emergency and mass casualty response, and support to DOD healthcare providers.²

In January 2010, the Secretary of Defense directed the Assistant Secretary of Defense for Homeland Defense and Global Security (ASD[HD&GS]) to conduct a follow-on review to determine appropriate implementation of corrective actions recommended by the independent review.³ The Secretary of Defense also directed the Secretaries of the military departments, combatant commanders, and the heads of the other DOD components, informed by the report of the independent review panel, to initiate internal reviews in support of the follow-on review. These reviews were to assess their organization's ability below the headquarters level to identify internal threats and force protection and emergency response programs, policies, and procedures. As directed, the military services each produced a report based on their respective Fort Hood internal reviews and submitted them to the Secretary of Defense for his

¹Secretary of Defense memorandum, *Independent Panel for Department of Defense Review Related to Fort Hood* (Nov. 20, 2009).

²Department of Defense, *Protecting the Force: Lessons from Fort Hood, Report of the DOD Independent Review* (January 2010).

³Secretary of Defense memorandum, *Follow-on Action on the Findings and Recommendations of the DOD Independent Review Related to the Ft. Hood Incident* (Jan. 29, 2010).

consideration in determining which recommendations to implement from the independent review of the 2009 Fort Hood shooting.⁴

On August 18, 2010, the Secretary of Defense generally approved 79 recommendations identified in the independent review and directed the DOD components to take specific actions associated with those recommendations as identified in an attachment to the memorandum.⁵ The Secretary of Defense in his August 2010 memorandum also directed the ASD(HD&GS) to provide regular implementation progress reports to the Secretary of Defense, not only on those measures he approved, but also on progress by the military department Secretaries and combatant commanders to mitigate issues identified in their independent internal reviews. The Force Protection Senior Steering Group, which was established in August 2010, was responsible for monitoring implementation of the Fort Hood force protection-related recommendations. In October 2013, the Mission Assurance Coordination Boards assumed responsibility for monitoring recommendation implementation from the independent review of the 2009 Fort Hood shooting.⁶ The boards established a Fort Hood Working Group to track and monitor the status of implementation of the Fort Hood recommendations. The Mission Assurance Coordination Boards include representatives from the military departments, the offices of the Under Secretaries of Defense, the Office of the Director of Cost Assessment and

⁴Department of the Army, *Fort Hood Army Internal Review Team: Final Report* (Washington, D.C.: Aug. 4, 2010); Headquarters U.S. Marine Corps Memorandum, *Fort Hood Follow-On Internal Review (IR) Final Report* (Washington, D.C.: May 26, 2010); Office of the Chief of Naval Operations Memorandum, *Department of Navy Fort Hood Internal Review Report* (Washington, D.C.: May 28, 2010); Department of the Air Force, *Air Force Follow-On Review Protecting the Force: Lessons from Fort Hood* (Washington, D.C.: 2010). The Army and Air Force internal reviews also identified key actions and recommendations that those two services could respectively take to address findings from Fort Hood. All of the Army's key actions and the vast majority of the Air Force's recommendations were intended to further recommendations coming out of DOD's independent review of the 2009 Fort Hood shooting.

⁵Secretary of Defense Memorandum, *Final Recommendations of the Ft. Hood Follow-on Review* (Aug. 18, 2010).

⁶According to DOD's *Mission Assurance Strategy Implementation Framework* (October 2013), the Mission Assurance Coordination Boards are tasked with advocating for and overseeing alignment of mission assurance efforts on issues that cut across the department. Their responsibilities include incorporating those tasks previously overseen by the Force Protection Senior Steering Group to ensure completion of the Fort Hood recommendations, as directed by the Secretary of Defense.

Program Evaluation, the Office of the DOD Chief Information Officer, the Office of the Director of Administration and Management, the National Guard Bureau, the combatant commands, and the Office of the General Counsel.

DOD Internal Review and an Independent Review of the 2013 Washington Navy Yard Shooting

In response to the September 2013 Washington Navy Yard shooting, the Secretary of Defense directed an independent review and an internal review of the incident to identify and recommend actions to address gaps or deficiencies in DOD programs, policies, or procedures regarding security at DOD installations and the granting and renewing of security clearances for DOD employees and contractor personnel.⁷ Both the Washington Navy Yard independent review and internal review were released in November 2013 and identified actions that were intended to improve DOD's force protection posture from insider threats.⁸ In March 2014, the Secretary of Defense directed DOD to implement four key recommendations that were a compilation of a number of recommendations from the Washington Navy Yard independent review and internal review. The Secretary of Defense tasked the Under Secretary of Defense for Intelligence to lead a task force to develop and coordinate an implementation plan for the four key recommendations. The Secretary of Defense also directed the Under Secretary of Defense for Intelligence to study three additional recommendations from the Washington Navy Yard independent review.⁹ The Defense Security Enterprise Executive Committee—chaired by the Deputy Under Secretary of Defense for Intelligence and Security—assumed responsibility for

⁷Secretary of Defense Memorandum, *Department of Defense Independent Review of the Washington Navy Yard Shooting* (Sept. 30, 2013).

⁸Department of Defense, *Security from Within: Independent Review of the Washington Navy Yard Shooting* (November 2013); and Department of Defense, *Internal Review of the Washington Navy Yard Shooting, A Report to the Secretary of Defense* (Nov. 20, 2013). The independent review made 30 recommendations while the internal review made 73 recommendations.

⁹Secretary of Defense Memorandum, *Final Recommendations of the Washington Navy Yard Shooting Internal and Independent Reviews* (Mar. 18, 2014).

monitoring progress of actions taken to implement the four approved recommendations from the Washington Navy Yard implementation plan.¹⁰

Internal Service Reviews of the 2013 Washington Navy Yard Shooting

In addition, the Department of the Navy conducted two internal service reviews in response to the Washington Navy Yard shootings. Specifically, in a September 2013 memorandum, the Secretary of the Navy directed Admiral John M. Richardson to conduct an in-depth investigation into the full range of security, contractor, personnel, and other factors related to the Washington Navy Yard shootings.¹¹ As a result of this in-depth investigation, Admiral Richardson issued a report that identified 15 recommendations to the Department of the Navy addressing contractor security; personnel security management; and additional actions to improve force protection, antiterrorism, and emergency management.¹² Additionally, in an October 11, 2013, memorandum, the Secretary of the Navy directed the Chief of Naval Operations and the Commandant of the Marine Corps to conduct a thorough ongoing review of physical security on naval installations that, among other things, assessed military service access control policy and procedures and risk mitigation measures; evaluated training and education programs to identify contributing factors and behavioral indicators of potentially violent actors; and identified barriers to physical security and access control policy implementation.¹³ On October 31, 2013, the commanders of U.S. Fleet Forces Command and U.S. Marine Corps Forces Command issued a consolidated report that identified 79 recommendations for the Navy to implement and 29

¹⁰The Defense Security Enterprise is the organization, infrastructure, and measures in place to safeguard DOD personnel, information, operations, resources, technologies, and facilities against harm, loss, hostile acts, or hostile influences. The Defense Security Enterprise Executive Committee includes representatives from the Offices of the Under Secretaries of Defense, the DOD Chief Information Officer, the Director of Administration and Management, the military departments, the Chairman of the Joint Chiefs of Staff, and the General Counsel of the department.

¹¹Secretary of the Navy memorandum, *Investigation Into the Fatal Shooting Incident at the Washington Navy Yard (WNY) on 16 September 2013 and Associated Security, Personnel, and Contracting Policies and Practices* (Sept. 25, 2013).

¹²Department of the Navy, *Report of the Investigation into the Fatal Shooting Incident at the Washington Navy Yard (WNY) on 16 September 2013 and Associated Security, Personnel, and Contracting Policies and Practices* (Nov. 8, 2013).

¹³Secretary of the Navy memorandum, *Base, Station, and Installation Physical Security Assessment* (Oct. 11, 2013).

recommendations for the Marine Corps to implement. The recommendations focused on a range of topics, such as assessments of behavioral indicators, an insider threat analysis entity within the Marine Corps, and improved training for commanders and security personnel on violence prevention and active shooter response.¹⁴

¹⁴Department of the Navy, Commander, U.S. Fleet Forces Command, and Commander, U.S. Marine Corps Forces Command *Base, Station, and Installation Physical Security Assessment Report, Part 2* (Oct. 31, 2013). The report made 79 recommendations to the Navy and 29 to the Marine Corps.

Appendix III: Comments from the Department of Defense



POLICY

PRINCIPAL DEPUTY UNDER SECRETARY
OF DEFENSE
2100 DEFENSE PENTAGON
WASHINGTON, DC 20301-2100

JUN 23 2015

Mr. Joseph Kirschbaum
Director, Defense Capabilities Management
U.S. Government Accountability Office
441 G Street, NW
Washington DC 20548

Dear Mr. Kirschbaum:

This letter provides the Department of Defense (DoD) response to the GAO Draft Report GAO-15-543, "INSIDER THREATS: DOD Should Improve Information Sharing and Oversight to Protect U.S. Installations," dated May 27, 2015 (GAO Code 351950).

My point of contact is Deputy Assistant Secretary of Defense for Defense Continuity and Mission Assurance Chuck Kosak, who can be reached at 571-256-8352 or charles.p.kosak.civ@mail.mil.

Sincerely,

A handwritten signature in blue ink that reads "Brent P. McKeen".

Attachment:
DoD Response



GAO DRAFT REPORT DATED MAY 27, 2015
GAO-15-543 (GAO CODE 351950)

“INSIDER THREATS: DOD SHOULD IMPROVE INFORMATION SHARING AND
OVERSIGHT TO PROTECT U.S. INSTALLATIONS”

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATION

RECOMMENDATION 1: To assist U.S. installations in protecting against insider threats, GAO recommends that the Secretary of Defense direct the military services to share information about actions U.S. installations have taken to address insider threats by consistently using existing mechanisms – such as working groups, lessons-learned information systems, and antiterrorism web portals.

DoD RESPONSE: We concur in the GAO’s recommendation to seek opportunities to improve information sharing about actions taken to address insider threats through existing mechanisms. The Office of the Under Secretary of Defense for Intelligence (OUSD(I)) has established and chairs working groups today that share best practices and lessons learned as DoD Components counter threats associated with insiders. For the past several years, separate working groups have been actively supporting security initiatives for personnel, industrial and physical security domains. Each working group routinely shares information associated with actions taken to strengthen the security of DoD resources, including military installations and remote DoD facilities. Concurrently, OUSD(I) has been active in establishing and enhancing web sites as information portals to share evolving security practices and policy changes that impact insider threat issues. The DoD insider threat website, like other information portals, evolves as new information is shared and posted. Although it is only a year old, it possesses exceptional potential as a source for Components seeking the latest insider threat information. Furthermore, the establishment and growth of the Defense Security Enterprise (DSE) and its vast governance structure has been extremely effective in forging and disseminating security information across all segments of the Department. As security issues and challenges arise in the Components, these issues are quickly shared and resolved in the DSE Advisory Group or the DSE Executive Committee. In summary, OUSD(I) believes these existing efforts, as well as those planned for the future, are in alignment with and supportive of Recommendation #1.

In March 2015, the Mission Assurance Senior Steering Group (MA SSG) discussed two benchmark insider threat programs - the Navy’s Threat Management Unit concept and the Pentagon Force Protection Agency’s Threat Duty Desk program. Additionally, the Department recently renamed the Fort Hood Working Group as the Antiterrorism Force Protection (AT/FP) Working Group and expanded its scope to address protection issues beyond the Fort Hood recommendations. The AT/FP Working Group is another venue to share best practices and lessons related to insider threat.

From March to May 2015, the Assistant Secretary of Defense for Homeland Defense and Global Security conducted a series of site visits to ensure implementation of the Fort Hood

recommendations. The MA SSG will share the best practices and lessons learned garnered from these visits to strengthen DoD Insider Threat efforts and help prevent future tragedies such as the Fort Hood shootings.

RECOMMENDATION 2: To assist DoD leadership in their oversight and decision-making process, GAO recommends that the Secretary of Defense direct the DoD leaders on the Mission Assurance Coordination Boards and the military services to take steps to improve the consistency of reporting and monitoring of the implementation of recommendations from the independent review of the 2009 Fort Hood shootings. Such steps could include DoD and the military services developing criteria for consistent reporting on the progress of recommendations and the military services providing periodic reports to the Mission Assurance Coordination Boards on the status of Fort Hood recommendations at the service level and installation level.

DoD RESPONSE: We concur in the recommendation that the Office of the Secretary of Defense and the Military Departments/Services take steps to improve the consistency of the monitoring and reporting of the implementation of recommendations from the January 2010 Report of the DoD Independent Review, Protecting the Force: Lessons from Fort Hood. Many of the report's recommendations are functional in nature and require the Military Departments/Services and other DoD Components to oversee the recommendations through mission-appropriate supplemental policy and guidance at the installation level.

The Department has made significant progress in its ability to respond to insider threats and acts of targeted violence. As of June 2015, 73 of the 79 recommendations from the DoD Independent Review and 8 of the 11 recommendations from the Defense Science Board Report of the Task Force on Predicting Violent Behavior have been implemented.

Although the GAO reported discrepancies between the Military Departments/Services and the Office of the Secretary of Defense (OSD) about the status of the implementation of the Fort Hood recommendations, the MA SSG determined that OSD and Joint Staff completed their actions directing the Services to implement the recommendations. In some cases, however, the Military Services needed to do some additional work to ensure full implementation at the individual Military Department/Service level. For example, the DoD Workplace Violence Policy was published in January 2014; however, the Army and Air Force reported that the implementation of the recommendation was still underway based on their need to update their respective internal policies. Consistent with the GAO recommendations, the MA SSG will continue to monitor the status of Fort Hood Recommendations at the Military Service level to ensure full implementation.

The Department remains committed to improving insider threat information sharing while maintaining oversight and ensuring the recommendations from the Fort Hood review are fully implemented.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Joseph W. Kirschbaum, (202) 512-9971 or kirschbaumj@gao.gov

Staff Acknowledgments

In addition to the individual named above, Tommy Baril, Assistant Director; Ashley Hess; Amber Lopez Roberts; Michael Pose; and Edwin Yuen made key contributions to this report. Tracy Barnes, Richard Powelson, Terry Richardson, Monica Savoy, and Amie Steele also made important contributions.

Appendix V: Accessible Data

Accessible Text

Accessible Text for Figure 1: Timeline of 2009 Fort Hood and 2013 Washington Navy Yard Shootings and Official Reviews and Related Tasking Memorandums

November 5, 2009: Fort Hood Shooting [Pictured: Bernie Beck Gate entrance sign];

November 20, 2009: Secretary of Defense memorandum, *Independent Panel for Department of Defense (DOD) Review Related to Fort Hood*;

January 2010:

- *Protecting the Force: Lessons from Fort Hood, Report of the DOD Independent Review*;
- Department of the Air Force, *Air Force Follow-On Review, Protecting the Force: Lessons from Fort Hood*.

May 2010:

- Headquarters U.S. Marine Corps memorandum, *Fort Hood Follow-On Internal Review (IR) Final Report*;
- Office of the Chief of Naval Operations memorandum, *Department of Navy Fort Hood Internal Review Report*.

August 2010:

- Department of the Army, *Fort Hood Army Internal Review Team: Final Report*;
- Secretary of Defense memorandum, *Final Recommendations of the Ft. Hood Follow-on Review*.

September 16, 2013: Washington Navy Yard shooting [Pictured: Washington Navy Yard entrance sign].

October 2013: Commander, U.S. Fleet Forces Command, and Commander, U.S. Marine Corps Forces Command, *Base, Station, and Installation Physical Security Assessment Report Part 2*.

November 2013:

- Navy Memorandum, *Investigation into the Fatal Shooting Incident at the Washington Navy Yard (WNY) on 16 September 2013, and Associated Security, Personnel, and Contracting Policies and Practices*;
- *Security from Within, Independent Review of the Washington Navy Yard Shooting*;
- *Department of Defense Internal Review of the Washington Navy Yard Shooting, A Report to the Secretary of Defense*.

March 2014: Secretary of Defense memorandum, *Final Recommendations of the Washington Navy Yard Shooting Internal and Independent Reviews*.

Source: GAO analysis of DOD information. | GAO-15-543

Accessible Text for Figure 2: GAO's Framework of Key Elements to Incorporate at Each Phase of DOD's Insider-Threat Programs

- **INSIDERS:**
 - Military employees;
 - Civilian employees;
 - Contractors and consultants;

- Federal, state, and local partners;
- Foreign allies;
- Authorized guests:
 - Active shooter;
 - Exfiltration;
 - Espionage
 - Sabotage (cyber and physical);
 - Unintentional.
- **DETER:**
 - Identify program office;
 - Establish rules and policies;
 - Institute consequences if rules and policies not followed;
 - Communicate program goals, policies, and consequences to staff and contractors;
 - Conduct internal spot checks;
 - Host red team.
- **PREVENT:**
 - Integrate personnel clearance;
 - Train and exercise employees;
 - Develop baseline of normal activity;
 - Conduct risk assessments;
 - Institute internal controls and security controls.
- **DETECT:**
 - Ensure cross-function coordination:
 - Cross-function coordination:
 - Leadership;
 - Mental health;
 - Information technology;
 - Human resources;
 - Counterintelligence;
 - Legal counsel;
 - Physical security;
 - Privacy office.
 - Monitor activity;
 - Perform risk-based analytics;
 - Conduct internal audits and reporting;
 - Allow external audits;
 - Encourage peer reporting;
 - Create and retain auditable records of actions taken;
 - Share information as appropriate.

• **TAKE ACTION:**

- Suspend access;
- Take personnel action—counsel, terminate, refer to appropriate authorities;
- Conduct damage assessments;
- Develop, disseminate, and incorporate best practices and lessons learned;
- Train, exercise, and equip response personnel;
- Establish formal and informal agreements.

Source: GAO analysis of Department of Defense (DOD), U.S. government, and private-sector guidance and reports. | GAO-15-543

Agency Comments

Department of Defense

Page 1

Accessible Text for Appendix III: Comments from the Department of Defense

PRINCIPAL DEPUTY UNDER SECRETARY OF DEFENSE

2100 DEFENSE PENTAGON
WASHINGTON, DC 20301-2100

POLICY

June 23, 2015

Mr. Joseph Kirschbaum
Director, Defense Capabilities Management
U.S. Government Accountability Office
441 G Street, NW
Washington DC 20548

Dear Mr. Kirschbaum:

This letter provides the Department of Defense (DoD) response to the GAO Draft Report GAO-15-543, "INSIDER THREATS: DOD Should Improve Information Sharing and Oversight to Protect U.S. Installations," dated May 27, 2015 (GAO Code 351950).

My point of contact is Deputy Assistant Secretary of Defense for Defense Continuity and Mission Assurance Chuck Kosak, who can be reached at 571-256-8352 or charles.p.kosak.civ@mail.mil.

Sincerely,

Signed by
Brian P. McKeon

Attachment: DoD Response

Page 2

GAO DRAFT REPORT DATED MAY 27, 2015 GA0-15-543 (GAO CODE 351950)

"INSIDER THREATS: DOD SHOULD IMPROVE INFORMATION SHARING AND OVERSIGHT TO PROTECT U.S. INSTALLATIONS"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION 1: To assist U.S. installations in protecting against insider threats, GAO recommends that the Secretary of Defense direct the military services to share information about actions U.S. installations have taken to address insider threats by consistently using existing mechanisms - such as working groups, lessons-learned information systems, and antiterrorism web portals.

DoD RESPONSE: We concur in the GAO's recommendation to seek opportunities to improve information sharing about actions taken to address insider threats through existing mechanisms. The Office of the Under Secretary of Defense for Intelligence (OUSD(I)) has established and chairs working groups today that share best practices and lessons learned as DoD Components counter threats associated with insiders. For the past several years, separate working groups have been actively supporting security initiatives for personnel, industrial and physical security domains. Each working group routinely shares information associated with actions taken to strengthen the security of DoD resources, including military installations and remote DoD facilities. Concurrently, OUSD(I) has been active in establishing and enhancing web sites as information portals to share evolving security practices and policy changes that impact insider threat issues. The DoD insider threat website, like other information portals, evolves as new information is shared and posted. Although it is only a year old, it possesses exceptional potential as a source for Components seeking the latest insider threat information. Furthermore, the establishment and growth of the Defense Security Enterprise (DSE) and its vast governance structure has been extremely effective in forging and disseminating security information across all segments of the Department. As security issues and challenges arise in the Components, these issues are quickly shared and resolved in the DSE Advisory Group or the DSE Executive Committee. In summary, OUSD(I) believes these existing efforts, as well as those planned for the future, are in alignment with and supportive of Recommendation # 1.

In March 2015, the Mission Assurance Senior Steering Group (MA SSG) discussed two benchmark insider threat programs - the Navy's Threat Management Unit concept and the Pentagon Force Protection Agency's Threat Duty Desk program. Additionally, the Department recently renamed the Fort Hood Working Group as the Antiterrorism Force Protection (AT/FP) Working Group and expanded its scope to address protection issues beyond the Fort Hood recommendations. The AT/FP Working Group is another venue to share best practices and lessons related to insider threat.

From March to May 2015, the Assistant Secretary of Defense for Homeland Defense and Global Security conducted a series of site visits to ensure implementation of the Fort Hood recommendations. The MA SSG will share the best practices and lessons learned garnered from these visits to strengthen DoD Insider Threat efforts and help prevent future tragedies such as the Fort Hood shootings.

RECOMMENDATION 2: To assist DoD leadership in their oversight and decision-making process, GAO recommends that the Secretary of Defense direct the DoD leaders on the Mission Assurance Coordination Boards and the military services to take steps to improve the consistency of reporting and monitoring of the implementation of recommendations from the independent review of the 2009 Fort Hood shootings. Such steps could include DoD and the military services developing criteria for consistent reporting on the progress of recommendations and the military services providing periodic reports to the Mission Assurance Coordination Boards on the status of Fort Hood recommendations at the service level and installation level.

DoD RESPONSE: We concur in the recommendation that the Office of the Secretary of Defense and the Military Departments/Services take steps to improve the consistency of the monitoring and reporting of the implementation of recommendations from the January 2010 Report of the DoD Independent Review, Protecting the Force: Lessons from Fort Hood. Many of the report's recommendations are functional in nature and require the Military Departments/Services and other DoD Components to oversee the recommendations through mission-appropriate supplemental policy and guidance at the installation level.

The Department has made significant progress in its ability to respond to insider threats and acts of targeted violence. As of June 2015, 73 of the 79 recommendations from the DoD Independent Review and 8 of the 11 recommendations from the Defense Science Board Report of the Task Force on Predicting Violent Behavior have been implemented.

Although the GAO reported discrepancies between the Military Departments/Services and the Office of the Secretary of Defense (OSD) about the status of the implementation of the Fort Hood recommendations, the MA SSG determined that OSD and Joint Staff completed their actions directing the Services to implement the recommendations. In some cases, however, the Military Services needed to do some additional work to ensure full implementation at the individual Military Department/Service level. For example, the DoD Workplace Violence Policy was published in January 2014; however, the Army and Air Force reported that the implementation of the recommendation was still underway based on their need to update their respective internal policies. Consistent with the GAO recommendations, the MA SSG will continue to monitor the status of Fort Hood Recommendations at the Military Service level to ensure full implementation.

The Department remains committed to improving insider threat information sharing while maintaining oversight and ensuring the recommendations from the Fort Hood review are fully implemented.

Related GAO Reports

Insider Threats: DOD Should Strengthen Management and Guidance to Protect Classified Information and Systems. [GAO-15-544](#). Washington, D.C.: June 2, 2015.

Personnel Security Clearances: Funding Estimates and Governmentwide Metrics Are Needed to Implement Long-Standing Reform Efforts. [GAO-15-179SU](#). Washington, D.C.: April 23, 2015.

Military Personnel: DOD Needs to Take Further Actions to Prevent Sexual Assault during Initial Military Training. [GAO-14-806](#). Washington, D.C.: September 9, 2014.

Personnel Security Clearances: Additional Guidance and Oversight Needed at DHS and DOD to Ensure Consistent Application of Revocation Process. [GAO-14-640](#). Washington, D.C.: September 8, 2014.

Federal Facility Security: Additional Actions Needed to Help Agencies Comply with Risk Assessment Methodology Standards. [GAO-14-86](#). Washington, D.C.: March 5, 2014.

Personnel Security Clearances: Actions Needed to Ensure Quality of Background Investigations and Resulting Decisions. [GAO-14-138T](#). Washington, D.C.: February 11, 2014.

Personnel Security Clearances: Opportunities Exist to Improve Quality Throughout the Process. [GAO-14-186T](#). Washington, D.C.: November 13, 2013.

Personnel Security Clearances: Full Development and Implementation of Metrics Needed to Measure Quality of Process. [GAO-14-157T](#). Washington, D.C., October 31, 2013.

Afghanistan Security: New Steps Taken to Address Insider Attacks, but DOD Has Not Always Ensured That Personnel Are Prepared for Casualty Assessment Teams. [GAO-13-838SU](#). Washington, D.C.: September 30, 2013.

Information Sharing: Additional Actions Could Help Ensure That Efforts to Share Terrorism-Related Suspicious Activity Reports Are Effective. [GAO-13-233](#). Washington, D.C.: March 13, 2013.

Afghanistan Security: Renewed Sharing of Biometric Data Could Strengthen U.S. Efforts to Protect U.S. Personnel from Afghan Security Force Attacks. GAO-12-471SU. Washington, D.C.: April 20, 2012.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548