United States Government Accountability Office

Report to Congressional Committees

June 2015

INSIDER THREATS

DOD Should Strengthen Management and Guidance to Protect Classified Information and Systems

GAO-15-544

GAO Highlights

Highlights of GAO-15-544, a report to congressional committees.

June 2015

INSIDER THREATS

DOD Should Strengthen Management and Guidance to Protect Classified Information and Systems

Why GAO Did This Study

Since 2010, the United States has suffered grave damage to national security and an increased risk to the lives of U.S. personnel due to unauthorized disclosures of classified information by individuals with authorized access to defense information systems. Congress and the President have issued requirements for structural reforms and a new program to address insider threats.

A 2014 House Committee on Armed Services report included a provision that GAO assess DOD's efforts to protect its information and systems. This report evaluates the extent to which (1) DOD has implemented an insider-threat program that incorporates minimum standards and key elements, (2) DOD and others have assessed DOD's insider-threat program, and (3) DOD has identified any technical and policy changes needed to protect against future insider threats. GAO reviewed studies, guidance, and other documents; and interviewed officials regarding actions that DOD and a nonprobability sample of six DOD components have taken to address insider threats.

What GAO Recommends

GAO recommends that DOD issue guidance to incorporate key elements into insider-threat programs, evaluate the extent to which programs address capability gaps, issue risk-assessment guidance, and identify a program office to manage and oversee insider-threat programs. DOD agreed or partially agreed with all of the recommendations, and described actions it plans to take. However, DOD's actions may not fully address the issues as discussed in the report.

View GAO-15-544. For more information, contact Joseph W. Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The Department of Defense (DOD) components GAO selected for review have begun implementing insider-threat programs that incorporate the six minimum standards called for in Executive Order 13587 to protect classified information and systems. For example, the components have begun to provide insider-threat awareness training to all personnel with security clearances. In addition, the components have incorporated some of the actions associated with a framework of key elements that GAO developed from a White House report, an executive order, DOD guidance and reports, national security systems guidance, and leading practices recommended by the National Insider Threat Task Force. However, the components have not consistently incorporated all recommended key elements. For example, three of the six components have developed a baseline of normal activity—a key element that could mitigate insider threats. DOD components have not consistently incorporated these key elements because DOD has not issued guidance that identifies recommended actions beyond the minimum standards that components should take to enhance their insider-threat programs. Such guidance would assist DOD and its components in developing and strengthening insider-threat programs and better position the department to safeguard classified information and systems.

DOD and others, such as the National Insider Threat Task Force, have assessed the department's insider-threat program, but DOD has not analyzed gaps or incorporated risk assessments into the program. DOD officials believe that current assessments meet the intent of the statute that requires DOD to implement a continuing gap analysis. However, DOD has not evaluated and documented the extent to which the current assessments describe existing insider-threat program capabilities, as is required by the law. Without such a documented evaluation, the department will not know whether its capabilities to address insider threats are adequate and address statutory requirements. Further, national-level security guidance states that agencies, including DOD, should assess risk posture as part of insider-threat programs. GAO found that DOD components had not incorporated risk assessments because DOD had not provided guidance on how to incorporate risk assessments into components' programs. Until DOD issues guidance on incorporating risk assessments, DOD components may not conduct such assessments and thus not be able to determine whether security measures are adequate.

DOD components have identified technical and policy changes to help protect classified information and systems from insider threats in the future, but DOD is not consistently collecting this information to support management and oversight responsibilities. According to Office of the Under Secretary of Defense for Intelligence officials, they do not consistently collect this information because DOD has not identified a program office that is focused on overseeing the insider-threat program. Without an identified program office dedicated to oversight of insider-threat programs, DOD may not be able to ensure the collection of all needed information and could face challenges in establishing goals and in recommending resources and improvements to address insider threats.

This is an unclassified version of a classified report GAO issued in April 2015.

Contents

Tables

Figures

Abbreviations

DOD	Department of Defense
DOD CIO	Department of Defense Chief Information Officer
E.O.	Executive Order
OUSD (Intelligence)	Office of the Under Secretary of Defense for Intelligence

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

June 2, 2015

Congressional Committees

According to U.S. intelligence-community leaders, unauthorized disclosures of classified information by individuals with authorized access to Department of Defense (DOD) information and systems have resulted in grave damage to national security and potentially placed the lives of military service members at risk, highlighting the threat insiders can pose to government organizations.[1] Disclosures by an Army service member in 2010 and a National Security Agency contractor in 2013 are among the largest known leaks of classified information in U.S. history, according to DOD and U.S intelligence-community leaders. In January 2014, the U.S. intelligence community's Worldwide Threat Assessment[2] cited the persistent challenge and continuing critical threat that insiders pose.[3] Insiders have an advantage over others who may want to harm an organization because insiders may have an awareness of their organization's vulnerabilities, such as loosely enforced policies and procedures, or exploitable technical flaws. Even insiders who do not intend to cause harm may inadvertently do so through human error. Insiders with access to DOD information and systems may be able to conduct far more malicious activity—wittingly or unwittingly—than outsiders, with potentially devastating consequences for DOD. DOD's April 2015 cyber strategy stressed the importance of mitigating insider threats, stating that DOD's work to mitigate these threats extends beyond

[1]Statements of James Clapper, Director of National Intelligence, and Lieutenant General Michael Flynn, Director of the Defense Intelligence Agency, Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence (Jan. 29, 2014); and statement of James Clapper, Director of National Intelligence, Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence (Feb. 16, 2011).

[2]Statement for the Record of James Clapper, Director of National Intelligence, Worldwide Threat Assessment of the U.S. Intelligence Community (Jan. 29, 2014).

[3]An insider is any person with authorized access to any U.S. government resource to include personnel, facilities, information, equipment, networks, or systems. See White House, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, memorandum (Nov. 21, 2012).

technological solutions and includes personnel, reliability, leadership, and accountability matters.[4]

Since the 2010 disclosures, Congress and the President have taken actions to try to prevent additional unauthorized disclosures of classified information by insiders. In 2011, Congress—citing damage to national security, the effect on military operations, and harm to the reputation and credibility of the United States resulting from the 2010 disclosures—called for DOD to establish an insider-threat program.[5] In 2011, the President issued Executive Order 13587 (E.O. 13587) that directed structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks consistent with appropriate protections for privacy and civil liberties.[6] In 2012, the President issued the national insider-threat policy that required agencies to implement insider-threat programs by May 2013.[7] The President also directed each agency's insider-threat program to include six minimum standards: (1) designation of senior official(s); (2) information integration, analysis, and response; (3) insider-threat program personnel; (4) access to information; (5) monitoring user activity on networks; and (6) employee training and awareness.

A 2014 House Committee on Armed Services report included a provision that GAO assess DOD's efforts to protect information and systems from insider threats.[8] This report evaluates the extent to which (1) DOD has implemented an insider-threat program that incorporates minimum standards and key elements to protect classified information and

[4]Department of Defense, *The Department of Defense Cyber Strategy* (April 2015).

[5]See National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112–81, § 922 (2011) and H.R. Rep. 112-78 at 184-185 (2011).

[6]Executive 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). (Hereinafter cited as E.O. 13587.)

[7]See White House, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, memorandum (Nov. 21, 2012), which defines insider threat as the threat that an individual with authorized access will use that access, wittingly or unwittingly, to harm the security of the United States.

[8]See H. R. Rep. No. 113-446 at 287–288 (2014) accompanying H.R. 4435, a proposed bill for the National Defense Authorization Act for Fiscal Year 2015. The House report also included a provision for us to evaluate DOD's efforts to protect U.S. installations from insider threats. That report is due to be issued in summer 2015.

systems, (2) DOD and others have assessed DOD's insider-threat program to protect classified information and systems, and (3) DOD has identified any technical and policy changes it needs to protect its classified information and systems from insider threats in the future. Although this report is about protection of classified information and systems from insider threats, we have previously completed a body of work on other security issues, such as defense cybersecurity, information security, and personnel security. This is an unclassified version of a classified report that we issued in April 2015. This report does not identify specific DOD components or the results of DOD and independent assessments of DOD insider-threat programs—information that DOD deemed to be classified or sensitive. Although the information provided in this report is less detailed, it addresses the same objectives as our classified report. Also, the overall methodology used for both reports is the same.

To evaluate the extent to which DOD has implemented an insider-threat program that incorporates minimum standards and key elements to protect classified information and systems, we evaluated initiatives that DOD had established and policy and guidance that identify responsibilities within the department to address the threat that insiders pose to classified information and systems. We selected a nonprobability sample of six DOD components to assess implementation efforts at the component level.[9] The six components include three combat support agencies; one military service; one combatant command; and one service sub-command. We selected these six components based on several factors including their specific roles in supporting DOD networks, prior insider-threat incidents, and reported progress in implementing insider-threat programs. In order to avoid duplication with an ongoing DOD Inspector General evaluation, we included only one military service.[10] While not generalizable, the information we obtained from these selected components provided insight about the steps that different types of components (i.e., service, combatant command, combat support agency)

[9]DOD defines "DOD components" to include the Office of the Secretary of Defense, the military departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the combatant commands, DOD Office of Inspector General, the defense agencies, the DOD field activities, and all other entities within DOD.

[10]In April 2014, the DOD Inspector General initiated work assessing the implementation of insider-threat programs at the four military services. According to the DOD Inspector General office, it plans to issue its report in mid-2015.

are taking and challenges they are encountering. We developed a questionnaire based on our research objectives, the minimum standards called for in E.O. 13587, and industry leading practices for insider-threat programs. We administered the questionnaire and collected responses from all six components, and conducted follow-up meetings as needed based on responses. We also collected responses from the Office of the Under Secretary of Defense for Intelligence (OUSD [Intelligence]) about the implementation of the department's insider-threat program because the Under Secretary of Defense for Intelligence is the DOD senior official responsible for the department's program. We used the questionnaire responses and information obtained from meetings and document reviews to assess each component's insider-threat program implementation and content. Using a scorecard methodology, two analysts independently rated the collective data sources against the minimum standards to score and provide an overall rating. The two analysts then compared their independent scores, discussed any differences, and determined the final ratings.

In addition to minimum standards, we identified key elements of insider-threat programs by reviewing and analyzing a range of documents including E.O. 13587, DOD guidance and reports, Committee on National Security Systems guidance, a set of leading practices that the National Insider Threat Task Force recommends, practices that other federal agencies and private industry use, and a list of essential principles developed by a group of private-sector and U.S. government analysts. We then organized this information into a framework of 25 key elements. We based these elements upon the principles that we identified, but this framework is not necessarily a comprehensive list of all elements since other principles may exist that could benefit insider-threat programs. We discussed this framework with DOD and private-sector officials and incorporated their comments and changes as appropriate. In order to assess how insider-threat programs incorporated these key elements, we collected and analyzed information from the selected components and OUSD (Intelligence) and interviewed relevant officials.

To evaluate the extent to which DOD and others have assessed DOD's insider-threat program to protect classified information and systems, we compared DOD assessment efforts occurring during the course of our review to those described in E.O. 13587. We reviewed copies of DOD's quarterly self-assessments from December 2013 through February 2015, in which DOD reported its progress in complying with minimum standards, and we interviewed OUSD (Intelligence) and DOD Chief Information Officer (DOD CIO) officials about their self-assessment

process and results. We did not independently verify the accuracy of the self-assessments since it was beyond the scope of this review. We also met with officials from the National Security Agency and National Insider Threat Task Force involved in conducting independent assessments, confirmed that they have assessed some DOD components, and obtained and reviewed copies of the assessments. To determine the extent to which DOD conducted the continuing analysis of gaps in its insider-threat program required by the National Defense Authorization Act for Fiscal Year 2012, we obtained and reviewed DOD's 2013 report to Congress, which described the department's plan for conducting a continuing analysis, and interviewed OUSD (Intelligence) officials about the current status of the analysis.[11] To determine the extent to which DOD incorporated risk assessments in its insider-threat program, we reviewed DOD, Committee on National Security Systems, and National Insider Threat Task Force guidance, and asked OUSD (Intelligence), DOD CIO, and component officials about the extent to which DOD conducted risk assessments related to insider-threat programs.

To evaluate the extent to which DOD has identified any technical or policy changes it needs to protect its classified information and systems from insider threats in the future, we focused on initiatives to be implemented beginning in 2015 and those initiatives not included in DOD's existing insider-threat guidance. We collected information about initiatives through our questionnaire and interviews with component officials, discussed above. We also asked component, OUSD (Intelligence), and DOD CIO officials about their process for prioritizing and planning for initiatives, as well as how the department is collecting information about these initiatives. We compared their responses to DOD guidance on responsibilities for insider-threat programs and the defense security enterprise, federal standards for internal control,[12] and Office of the Director of National Intelligence guidance. We did not evaluate the initiatives themselves or assess each initiative's relative priority or efficacy. A more-detailed explanation of our scope and methodology can be found in appendix I.

[11]Department of Defense, *Report to Congress: Insider Threat Detection* (Washington, D.C.: March 2013).

[12]GAO/AIMD-00.21.3.1.

We conducted this performance audit from May 2014 to June 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

Policies and Plans to Address Insider Threats

DOD reported on the potential threats that insiders could pose in April 2000 when the department issued an integrated process team report with 59 recommendations for action to mitigate insider threats to DOD information systems.[13] After the unauthorized, massive disclosures of classified information in 2010, Congress required the Secretary of Defense to establish a program for information sharing protection and insider-threat mitigation for DOD information systems.[14] Additionally, the President in October 2011 ordered structural reforms to safeguard classified information and improve security of classified networks that were to be consistent with appropriate protections for privacy and civil liberties.[15] E.O. 13587, among other things, established an interagency Insider Threat Task Force, known as the National Insider Threat Task Force, discussed below.

In November 2012, the President issued the *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, which identified six minimum standards that executive-branch agencies were required to include in their insider-threat programs. These standards include (1) designation of senior official(s); (2) information

[13]Department of Defense, *Insider Threat Mitigation: Final Report of the Insider Threat Integrated Process Team* (Apr. 24, 2000). The Senior Civilian Official of the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) established the Insider Threat Integrated Process Team to foster the effective development of interdependent technical and procedural safeguards to reduce malicious behavior by insiders.

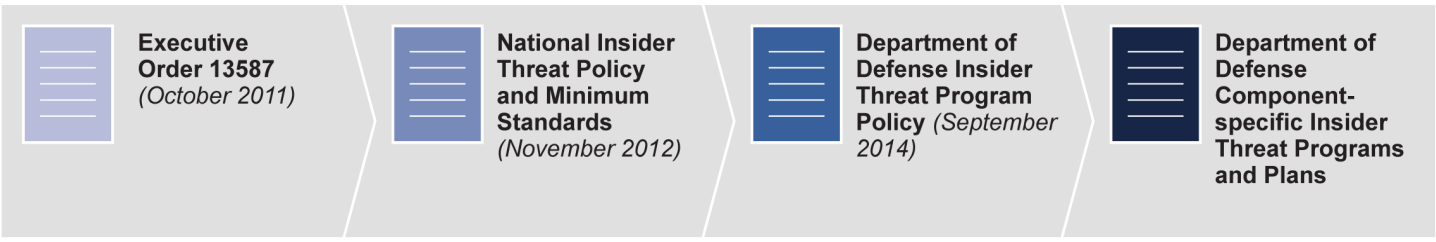
[14]Pub. L. No. 112–81, § 922 (2011).

[15]E.O. 13587.

integration, analysis, and response; (3) insider-threat program personnel; (4) access to information; (5) monitoring user activity on networks; and (6) employee training and awareness.[16] Each minimum standard has multiple associated tasks. For more information on these minimum standards and associated tasks, see appendix II.

As part of the minimum standards, departments and agencies were required to issue their own insider-threat policies and plans. DOD issued its insider-threat program policy in September 2014.[17] DOD's insider-threat program policy requires each of the department's components to issue respective insider-threat policies and implementation plans. Figure 1 shows the relationship between the White House, DOD, and DOD component actions to issue policies or plans.

Figure 1: Insider-Threat Policies and Plans for the Department of Defense



Source: GAO analysis of executive order, national policy, and Department of Defense (DOD) information. | GAO-15-544

Roles and Responsibilities Related to Insider Threats

As part of the President's 2011 reforms, E.O. 13587 assigned various executive-branch organizations responsibilities and oversight related to insider threats.

- National Insider Threat Task Force (co-chaired by the Attorney General of the United States and the Director of National Intelligence and includes representatives from numerous federal entities, including DOD) developed six minimum standards for executive-branch insider-threat programs and a guide to assist agencies as they establish and

[16]See White House, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*.

[17]DOD Directive 5205.16, *The DOD Insider Threat Program* (Sept. 30, 2014).

tailor programs to meet their particular needs.[18] In addition, according to task-force officials, the task force conducts independent assessments of agency programs as required by E.O. 13587.

- Senior Information Sharing and Safeguarding Steering Committee (co-chaired by the National Security Staff and the Office of Management and Budget and includes representatives from executive departments and agencies, including DOD) is to coordinate priorities for sharing and safeguarding classified information on computer networks. According to E.O. 13587, the committee is to receive copies of the self-assessments that each agency is to conduct—commonly referred to as the Key Information Sharing and Safeguarding Indicators assessment—and copies of the independent assessments that the National Insider Threat Task Force and National Security Agency are to conduct.
- National Security Agency, as co-Executive Agent for Safeguarding Classified Information on Computer Networks, is to conduct independent assessments of agency compliance with safeguarding policies and standards as required by E.O. 13587.
- Departments and agencies, including DOD, are to establish insider-threat programs and perform self-assessments of compliance with established standards and priorities.

Various DOD organizations, as described in table 1, have responsibilities related to insider threats, specifically the protection of DOD classified information and systems.

[18]National Insider Threat Task Force, *2014 Guide to Accompany the National Insider Threat Task Force Policy and Minimum Standards* (Sept. 2014).

Table 1: Department of Defense (DOD) Roles and Responsibilities for Insider Threats

Component	Responsibilities
Under Secretary of Defense for Intelligence	Serves as the senior official for the DOD insider-threat program; provides management, accountability, and oversight of the DOD program; and develops department-wide policy to counter insider threats.
DOD Chief Information Officer	Works with the Under Secretary of Defense for Intelligence to issue department-wide policy to safeguard against and mitigate insider-threat risks to DOD information and systems, based upon interagency priorities.
U.S. Cyber Command	Defends DOD information networks, including issuing detailed direction to DOD components on actions to counter insider-threat risks.
Defense Intelligence Agency	Ensures that the cybersecurity program associated with the Joint Worldwide Intelligence Communications System, a top-secret-level network, provides effective security against insider threats.
Defense Information Systems Agency	Supports unclassified and classified networks, including the secret-level network, throughout DOD by designing and deploying proactive protections to help address insider threats and performing other necessary security functions.
Defense Security Service	Conducts counterintelligence functions for cleared defense-industrial-base critical assets and incorporates insider-threat education and awareness material into training programs for DOD components and contractors.
DOD components[a]	Implement individual insider-threat programs in accordance with minimum standards and relevant DOD policies.

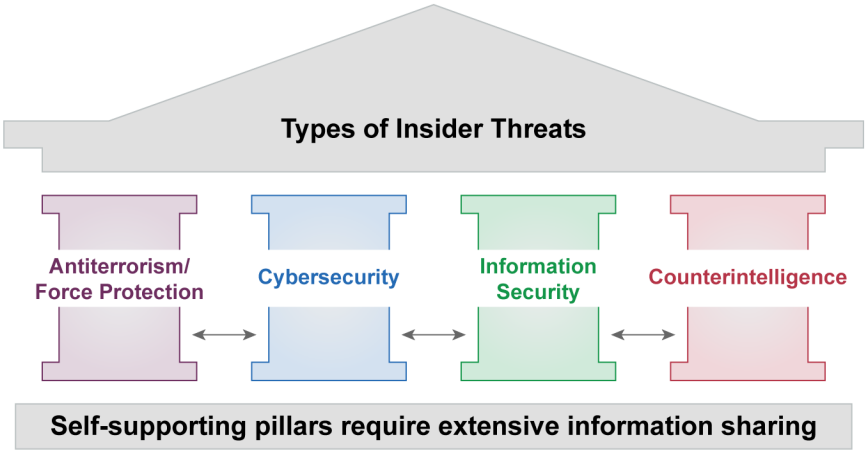
Source: GAO summary of DOD guidance. | GAO-15-544

[a]DOD components include collectively the Office of the Secretary of Defense, the military departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the combatant commands, the DOD Office of Inspector General, the defense agencies, the DOD field activities, and all other entities within DOD.

DOD's Program to Address Insider Threats

DOD has structured its insider-threat program to include four broad types of insider threats, including cyber threats. According to an OUSD (Intelligence) insider-threat program briefing, the DOD organizations responsible for each of these threat areas are to share information to help prevent and mitigate insider threats (see fig. 2).

Figure 2: Types of Threats Included in the Department of Defense's Insider-Threat Program



Source: GAO analysis of Department of Defense (DOD) information. | GAO-15-544

DOD and Selected Components Have Taken Steps to Implement Insider-Threat Programs, but DOD Has Not Issued Supplemental Guidance

DOD and Selected Components Have Begun Implementing Insider-Threat Programs That Incorporate Minimum Standards

DOD and the six selected components we reviewed have begun incorporating the minimum standards called for in E.O. 13587 into insider-threat programs to varying degrees to protect classified information and systems. Specifically, two components have established insider-threat programs that incorporate all six of the minimum standards. Conversely, the other components have taken action but have not addressed all tasks associated with the six minimum standards. For example, one insider-threat program has addressed six of the seven tasks associated with the minimum standard of "Designation of Senior Official(s)." However, that program has not completed the task that requires their senior official to submit to the agency head an implementation plan and an annual report

that identifies annual accomplishments, resources allocated, insider-threat risks to the agency, recommendations and goals for program improvement, and major impediments or challenges.

Similarly, all of the components we reviewed reported that they had addressed the task included in the "Monitoring User Activity on Networks" standard that states that insider-threat programs should include the technical capability to monitor user activity on classified networks. However, the means by which the selected components addressed this task varied. Specifically, according to component officials, one component was conducting more enhanced user activity monitoring for a small pilot group, and two components were conducting widespread enhanced monitoring of user activity. Two components reported that they were using an application that provides network activity information to inform user activity monitoring.[19] According to the National Insider Threat Task Force, this application contributes to insider-threat programs but does not provide full user activity-monitoring capability. Table 2 describes our evaluation of the extent to which DOD and the six selected components had incorporated minimum standards into insider-threat programs as of January 2015.

[19]This commercial application provides network administrators and security personnel with mechanisms to prevent, detect, track, report, and remediate malicious computer-related activities and incidents across networks and systems.

Table 2: GAO's Assessment of Department of Defense (DOD) and Six Selected Components' Incorporation of Minimum Standards into Insider-Threat Programs as of January 2015

Minimum standard	DOD and Components[a]						
	1	2	3	4	5	6	7
Designation of senior official(s)[b]	◐	◐	◐	●	●	●	◐
Information integration, analysis, and response	◐	◐	◐	●	●	●	◐
Insider-threat program personnel	◐	◐	●	●	●	●	◐
Access to information	◐	●	●	●	●	●	○
Monitoring user activity on networks	◐	◐	◐	◐	●	●	◐
Employee training and awareness	●	◐	◐	●	●	●	◐

Legend

● Addressed all tasks associated with minimum standard

◐ Addressed at least one of the tasks associated with minimum standard

○ Has not addressed any tasks associated with minimum standard

Source: GAO analysis of DOD information. | GAO-15-544.

[a]We have removed identifying references to DOD and specific components in this unclassified version of our assessment.

[b]This minimum standard requires each agency to designate a senior official who shall complete the following seven tasks: (1) program management and oversight; (2) issuing policy; (3) submitting implementation plans and annual reports to the agency head; (4) ensuring legal and civil liberties consultation during development of program; (5) establishing oversight for proper handling of records; (6) ensuring proper retention of records as defined in Executive Order 13587; and (7) facilitating oversight review to ensure compliance. While six components have designated a senior official for their insider-threat programs, some have not addressed all of the tasks associated with this standard. Therefore, most components were rated as having addressed at least one of the tasks associated with this minimum standard.

As of January 2015, DOD officials indicated that the selected components continue to take steps to develop their programs and incorporate the minimum standards into their programs. For example, DOD has drafted an implementation plan—a task in the "Designation of Senior Official(s)" minimum standard—that identifies the key milestones to incorporate the minimum standards into the department's insider-threat program. The implementation plan also requires the components to issue their own implementation plans as they establish insider-threat programs that incorporate all minimum standards in accordance with DOD's insider-threat program directive.[20] According to DOD officials, DOD plans to issue the department's implementation plan in spring 2015. Additionally, according to National Insider Threat Task Force officials, the Senior

[20]DOD Directive 5205.16, *The DOD Insider Threat Program*.

Information Sharing and Safeguarding Steering Committee has decided to adopt a risk-based approach to how departments and agencies incorporate the minimum standards. Lower-risk organizations, which could include some DOD components, will not be required to incorporate the minimum standards to the same extent as higher-risk organizations. The officials told us that they have not yet determined which DOD components might be characterized as lower-risk, and the committee is continuing to study the standards to determine what will be required of lower-risk organizations.

Selected Components Have Not Incorporated Key Elements of Insider-Threat Programs That Are Cited in DOD Guidance

In addition to the minimum standards issued by the President, DOD guidance and reports identify elements that could enhance DOD's efforts to protect classified information and systems. These elements—which are required to support DOD's broader efforts in areas such as cybersecurity, counterintelligence, and information security—are also identified in executive-branch policy and recommended in DOD and independent studies related to insider threats.[21] For example, DOD Instruction 5240.26, DOD's 2000 insider-threat mitigation report, and Carnegie Mellon Software Engineering Institute's insider-threat guide state that DOD components should develop a baseline of normal users' activities.[22] Also, Carnegie Mellon Software Engineering Institute[23] and a White

[21]We identified 25 key elements from DOD, executive-branch, government, and private-sector policies, guidance, and reports that could be included as a part of a framework of key elements of insider-threat programs. However, we did not perform a detailed analysis of all existing policies and guidance that could relate to insider threats. Therefore, agencies may be able to identify elements for inclusion in insider-threat programs in addition to the 25.

[22]DOD Instruction 5240.26, *Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat* (May 4, 2012) (incorporating change 1, Oct. 15, 2013); DOD, *Insider Threat Mitigation: Final Report of the Insider Threat Integrated Process Team*; and Carnegie Mellon Software Engineering Institute, *Common Sense Guide to Mitigating Insider Threats* 4th ed. (December 2012). The National Insider Threat Task Force cites Carnegie Mellon Software Engineering Institute's guide as a useful reference with practices that can help agencies formulate their own insider-threat programs.

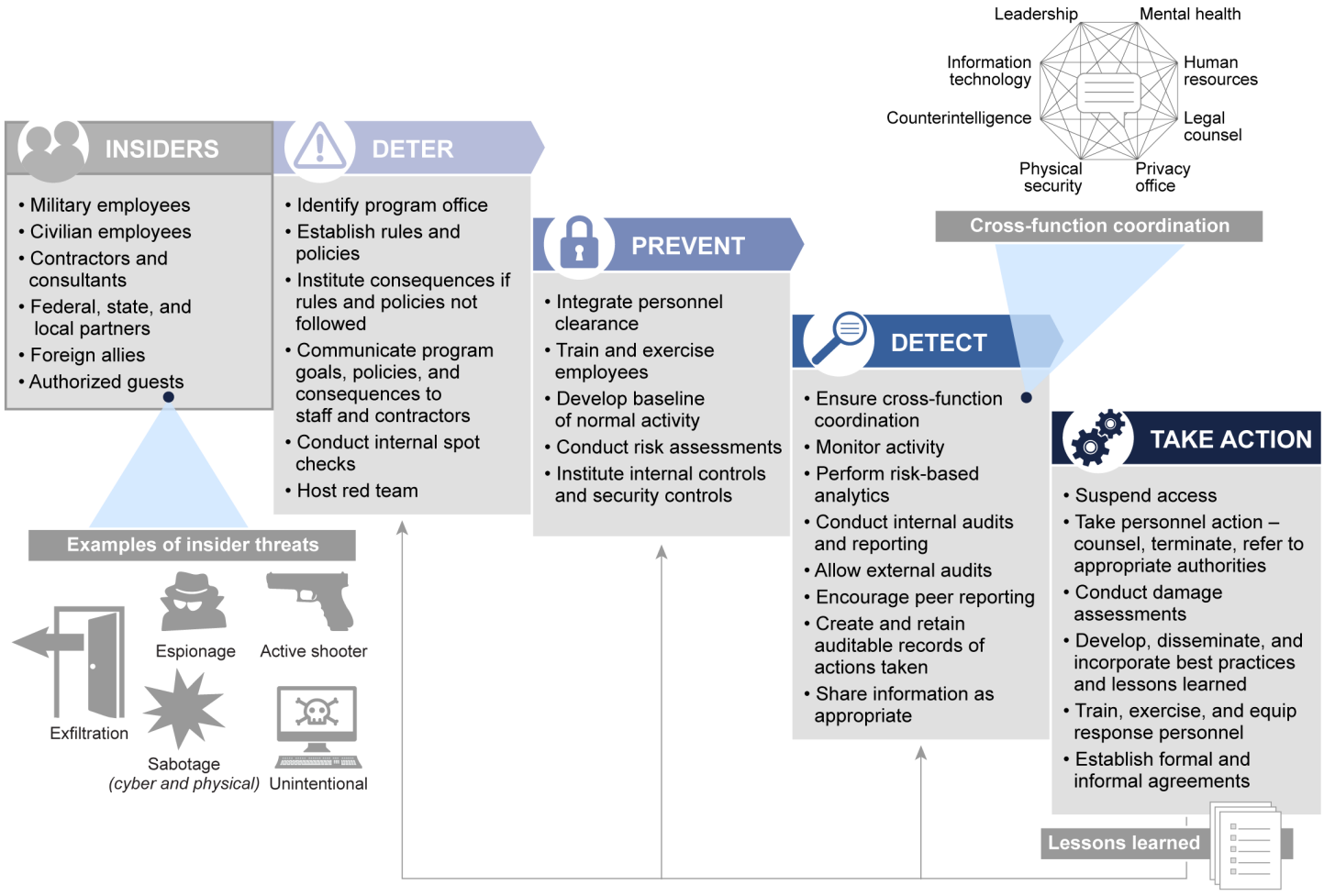
[23]Carnegie Mellon Software Engineering Institute, *Common Sense Guide to Mitigating Insider Threats*.

House review group[24]—both of whom have recommended actions to address insider threats—stated that agencies, such as DOD, should develop risk-based analytics to detect insider-threat activity. As shown in figure 3, we developed a framework of these key elements by program phase based on our analysis of the minimum standards, DOD guidance, executive-branch policy and reports, and other guidance.[25]

[24]After the 2013 disclosures of classified information by a National Security Agency contractor, the President created the Review Group on Intelligence and Communications Technologies to review practices for safeguarding liberty and security. The group's final report included 46 recommendations, including recommendations for protecting classified information and systems. *Liberty and Security in a Changing World* (The President's Review Group on Intelligence and Communications Technologies: Washington, D.C., Dec. 12, 2013).

[25]For a detailed list of all documents used to develop each key element, see appendix III.

Figure 3: 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-15-544

DOD and the six components we reviewed have incorporated some of the 25 recommended key elements we identified from DOD guidance and reports and independent studies to mitigate insider threats. Specifically, we found that some components have incorporated key elements such as

conducting internal spot checks; instituting internal controls and security controls; performing risk-based analytics; and taking personnel action.[26]

However, DOD and the six components have not incorporated all of the 25 key elements and for the ones they have incorporated, they have not done so consistently. For example:

- *Institute and communicate consequences.* DOD Instruction 8500.01 directs DOD components to ensure personnel are considered for sanctions if they compromise, damage, or place at risk DOD information.[27] Additionally, Carnegie Mellon Software Engineering Institute's insider-threat guide states that agencies should have policies and procedures in place that specify the consequences of particular policy violations.[28] We found that one component published a table of penalties, which is a guide for assessing the appropriate penalty for misconduct. A second component's policy had procedures for communicating the consequences of disciplinary actions to insider-threat personnel; however, the other components we reviewed did not have similar information in their insider-threat program policies. Further, two components reported that their program processes and procedures were not fully documented, and officials from another component cited an example of component officials not instituting consequences when an incident occurred.
- *Develop a baseline of normal activity*.[29] DOD Instruction 5240.26 directs DOD components to report anomalies, such as changes in user behavior.[30] DOD's 2000 insider-threat mitigation report recommended that DOD create a list of system and user behavior attributes to develop a baseline of normal activity patterns.[31]

[26]For a list of documents identifying actions associated each of these elements, see appendix III.

[27]DOD Instruction 8500.01, *Cybersecurity* (Mar. 14, 2014).

[28]Carnegie Mellon Software Engineering Institute, *Common Sense Guide to Mitigating Insider Threats*.

[29]A baseline of normal activity identifies a user's normal network activity.

[30]DOD Instruction 5240.26, *Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat*.

[31]DOD, *Insider Threat Mitigation: Final Report of the Insider Threat Integrated Process Team*.

Additionally, according to Carnegie Mellon Software Engineering Institute's insider-threat guide, to detect anomalies in network activity, an organization must first create a baseline of normal network activity.[32] Three components have taken action to identify a baseline of normal user activity, but the others have not.

- *Share information as appropriate.* E.O. 13587 states that agencies should provide policies for sharing information both within and outside of the federal government. Component officials stated there are informal processes for sharing information within DOD; however, the component officials stated that they were unaware of a process for sharing information outside of DOD.
- *Develop, disseminate, and incorporate best practices and lessons learned.* DOD Instruction 5240.26 calls for the identification and dissemination of best practices across DOD in support of DOD insider-threat programs.[33] Additionally, DOD's 2000 insider-threat mitigation report recommended that DOD develop a database of lessons learned from insider-threat incidents.[34] The report stated that not having such information severely hampers understanding of the magnitude of the insider-threat problem and the development of solution strategies. Officials at five components stated that while they sometimes develop and share best practices and lessons learned as a matter of practice, they do not have or use a formalized process of developing, disseminating, and incorporating best practices and lessons learned, such as solutions to vulnerabilities, in their insider-threat programs.

When we discussed the key elements framework with DOD officials, researchers specializing in insider threats, and a private sector insider-threat program official, they agreed that it identified elements that would help DOD components develop and strengthen their insider-threat programs. However, DOD officials stated that they would need supplemental planning guidance that helps them identify actions, such as the key elements, beyond the minimum standards that they should take to

[32]Carnegie Mellon Software Engineering Institute, *Common Sense Guide to Mitigating Insider Threats*.

[33]DOD Instruction 5240.26, *Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat*.

[34]DOD, *Insider Threat Mitigation: Final Report of the Insider Threat Integrated Process Team*.

enhance their insider-threat programs. The current DOD directive does not contain additional guidance for implementing key elements of an insider-threat program beyond the minimum standards.[35] According to DOD component officials, the directive repeats the minimum standards but does not provide DOD component officials with sufficient guidance for incorporating recommended key elements to enhance their insider-threat programs. Additionally, the draft DOD implementation plan provides guidance on the minimum standards but not recommended key elements. In January 2015, DOD officials stated that they planned to issue supplemental guidance to assist components in implementing insider-threat programs. Issuing such guidance would be consistent with federal standards for internal control, which state that organizations need information to achieve objectives, and that information should be communicated to those who need it within a time frame that enables them to carry out their responsibilities.[36] Guidance identifying actions beyond the minimum standards could assist components in enhancing their insider-threat programs and further enhance the department's efforts to protect its classified information and systems.

DOD Has Assessed Its Insider-Threat Program but Has Not Analyzed Gaps or Incorporated Risk Assessments into the Program

DOD and Other Entities Have Assessed the Department's Insider-Threat Program

DOD has conducted self-assessments of its insider-threat program; additionally, independent entities have assessed DOD components' compliance with relevant policies and standards. E.O. 13587 and the national insider-threat policy require agencies to perform self-assessments that evaluate their level of organizational compliance with

[35]DOD Directive 5205.16, *The DOD Insider Threat Program*.

[36]GAO/AIMD-00.21.3.1.

the national insider-threat policy and minimum standards.[37] To meet this requirement, DOD conducts quarterly self-assessments—commonly referred to as the Key Information Sharing and Safeguarding Indicators assessment—and evaluates the extent to which the department is addressing 63 key performance indicators. These 63 key performance indicators address topics such as the implementation of the department's insider-threat program, the management and monitoring of removable media, and the implementation of a public-key infrastructure to reduce user anonymity on classified networks.[38] In its February 2015 quarterly self-assessment, DOD reported that it addressed all of the management and monitoring indicators for removable media. For example, DOD reported that it monitors computer systems and uses a tool to alert appropriate officials when individuals try to write to removable media such as CDs or USB devices. However, DOD also reported that it had not fully addressed other indicators, including those associated with the department's insider-threat program. For example, DOD reported that it had not issued its program-implementation plan. DOD officials acknowledged that the department had not completed the tasks associated with the 63 key performance indicators and told us that the department will continue to focus on these efforts until they have been addressed.

DOD has conducted these self-assessments for the department, as required. However, we found that these assessments reflect either the department's overall progress or limited information regarding actions taken by individual DOD components. This information is limited because the current assessments do not reflect the extent to which the components have accomplished tasks associated with the 63 key performance indicators. According to the draft DOD insider threat program implementation plan, DOD components will be expected to submit self-assessments to the Under Secretary of Defense for Intelligence in 2015.

[37]E.O. 13587 and White House, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*.

[38]Public-key infrastructure is a system of hardware, software, policies, and people that, when fully and properly implemented, can provide a suite of information security assurances—including confidentiality, data integrity, authentication, and non-repudiation—that are important in protecting sensitive communications and transactions.

In addition to its self-assessments, in 2013 DOD updated its Command Cyber Readiness Inspections[39] to evaluate whether units had incorporated insider-threat security measures identified in a 2013 U.S. Cyber Command tasking order.[40] U.S. Cyber Command officials indicated that the command selects units for inspection according to risk factors such as threat information and inspection histories. As of July 2014, DOD had inspected one of the six components included in the scope of our review. According to the inspection report, this component was complying with the security measures cited in the 2013 tasking order.[41] U.S. Cyber Command officials stated that DOD intends to update the inspections in 2015 to include additional security measures developed in response to a 2014 U.S. Cyber Command tasking order.[42]

In addition to DOD's internal assessments, the National Security Agency and the National Insider Threat Task Force separately conduct independent assessments of DOD's protection of classified information and systems, as required by E.O. 13587.[43] DOD officials stated that as of January 2015, the National Security Agency had assessed one DOD component since E.O. 13587 was issued in 2011. The focus of the assessment was to identify vulnerabilities, assess compliance, and assist the component with the implementation of safeguarding policies and standards in support of E.O. 13587. The assessment report identified best practices, vulnerabilities, and recommendations to resolve technical security issues.

[39]Command Cyber Readiness Inspections are intended to assess compliance, validation, and readiness of components and individual units. U.S. Cyber Command is in charge of the Command Cyber Readiness Inspection process, but the Defense Information Systems Agency executes these inspections to include evaluations of readiness to mitigate insider threats.

[40]U.S. Cyber Command, *United States Cyber Command Operation Gladiator Shield Tasking Order 13-0651 Insider Threat Mitigation Amplifying Direction* (July 2013). This tasking order directed DOD components to implement specific short-term technical and procedural safeguards to prevent, deter, and detect insider threats.

[41]As of July 2014, U.S. Cyber Command reported that nearly all of the 89 units that it had assessed from October 1, 2013, through June 6, 2014, were complying with the security measures cited in the 2013 task order.

[42]U.S. Cyber Command, *United States Cyber Command Tasking Order 14-0185 Insider Threat Mitigation* (July 2014).

[43]The National Security Agency conducts these assessments in its independent role as co-executive agent for safeguarding classified information on computer networks.

In accordance with the executive order, the National Insider Threat Task Force has assessed four DOD components' compliance with insider-threat policies and minimum standards. According to these assessments, the task force compares the component's policies and practices with the minimum standards. The assessments note where the component has taken action to address minimum standards and associated tasks, and also make recommendations to help the components develop their programs and address the standards. For example, in its assessment of one component, the National Insider Threat Task Force complimented the component's system to centralize access to unclassified employee records, but recommended that the component begin issuing an annual report to its director, which is a task associated with the "Designation of Senior Official(s)" standard.

DOD Has Not Completed a Required Continuing Analysis of Gaps

Section 922 of the National Defense Authorization Act for Fiscal Year 2012 requires that DOD complete a continuing analysis of gaps in security measures and of technology, policies, and processes that are needed to increase the capability of its insider-threat program to address these gaps, and that DOD report to Congress on implementation of the requirement.[44] Although DOD reported to Congress in March 2013 that OUSD (Intelligence) was conducting a survey to serve as a baseline foundation for a continuing analysis of gaps, in October 2014 DOD officials told us that they suspended this baseline survey and did not otherwise complete a continuing analysis of gaps.[45] This survey would have allowed DOD to define existing insider-threat program capabilities; identify gaps in security measures; and advocate for the technology, policies, and processes necessary to increase capabilities in the future. According to the officials, after consulting DOD's Cost Assessment and Program Evaluation office about the process for conducting such a survey across the department, the department believed such an effort would not be feasible due to financial and personnel limitations. The department has not taken action to fulfill this statutory requirement since then.

OUSD (Intelligence) officials stated that they believe the department has addressed the intent of the statutory requirement through the previously discussed assessments—DOD's quarterly self-assessments, DOD's

[44]Pub. L. No. 112–81, § 922 (2011).

[45]DOD, *Report to Congress: Insider Threat Detection*.

Command Cyber Readiness Inspections, and the National Security Agency's independent assessments. However, DOD has not evaluated and documented the extent to which these assessments define existing insider-threat program capabilities; identify gaps in security measures; and advocate for the technology, policies, and processes necessary to increase capabilities in the future, as is required by law. Similarly, DOD officials stated that the department has not informed Congress that it did not complete the actions identified in its 2013 report to Congress, because they believed the legislation required only the 2013 report. Further, officials from OUSD (Intelligence)—which supports DOD's senior official overseeing insider-threat programs—told us they do not review the results of the National Security Agency assessments or Command Cyber Readiness Inspection reports, though DOD Directive 5205.16 directs the senior official to monitor insider-threat program implementation progress.[46] Without evaluating and documenting the extent to which current assessments provide a continuing analysis of gaps, reporting to Congress on the results of this evaluation, and OUSD (Intelligence) reviewing the overall results of these self- and independent assessments, the department will not know whether their capabilities for insider-threat detection and analysis are adequate and fully address the statutory requirements.

DOD and the Six Components Have Not Incorporated Risk Assessments into Insider-Threat Programs

National-level security guidance states that agencies should assess their risk posture as a part of their insider-threat programs.[47] For example, the National Insider Threat Task Force's guide states that agencies should identify their critical assets and then assess the risk to those assets. Also, the Committee on National Security Systems' Directive on Protecting National Security Systems from Insider Threat requires the alignment of departments and agencies' cybersecurity protections—which are part of an insider-threat program's protective capabilities—with the assets,

[46]DOD Directive 5205.16. *The DOD Insider Threat Program*.

[47]National Insider Threat Task Force, *2014 Guide to Accompany the National Insider Threat Policy and Minimum Standards*; and Committee on National Security Systems Directive 504, *Directive on Protecting National Security Systems from Insider Threat* (Feb. 4, 2014).

threats, and vulnerability assessments as determined by risk assessments.[48]

We found that DOD has not incorporated risk assessments into its insider-threat programs. DOD officials stated that they include insider threats in other risk assessments; however, these assessments are technical in nature and focus on the vulnerabilities of individual systems. These individual system risk assessments do not provide insider-threat program officials with complete information to make informed risk and resource decisions about how to align cybersecurity protections. For example, the individual system risk assessments do not identify or consider the different types of insider threats (e.g., foreign intelligence collection, individuals with a personal agenda, or unintentional actions); insider-threat vulnerabilities; or different levels of consequence that each component or organization could suffer if an insider were to exploit the vulnerability; nor do they address the overall risk to the insider-threat program. Rather than conducting a formal risk assessment for the insider-threat program, DOD CIO officials stated that they reach out to DOD component officials in an effort to maintain awareness of the department's overall insider-threat capabilities. We found that this communication provides OUSD (Intelligence) and DOD CIO a status update of the component's progress in achieving key performance indicators for the insider-threat program but does not include identification of component's critical assets and risks to them, as described in the National Insider Threat Task Force's guide.[49] For example, agencies should identify elements of their mission that are essential to national security and that, if damaged, stolen, or otherwise exploited, would have a damaging effect on the agency, its mission, and national security.

[48]Risk assessments are a means of providing decision makers with information needed to understand factors that can negatively influence operations and outcomes and make informed judgments concerning the extent of actions needed to reduce risk. They provide a basis for establishing appropriate policies and selecting cost-effective techniques to implement these policies. Risk assessments generally include the tasks of identifying threats and vulnerabilities, and determining consequences. GAO, *Information Security Risk Assessment: Practices of Leading Organizations*, GAO/AIMD-00-33 (Washington, D.C.: Nov. 1, 1999); and National Institute of Standards and Technology, *Guide for Conducting Risk Assessments*, Special Publication 800-30 Revision 1 (Gaithersburg, Md.: September 2012).

[49]National Insider Threat Task Force, *2014 Guide to Accompany the National Insider Threat Task Force Policy and Minimum Standards*.

DOD officials stated that they believe the department has addressed the intent of a risk assessment by other means, including the Command Cyber Readiness Inspections and the National Security Agency's independent assessments of DOD components. Officials of the Command Cyber Readiness Inspection program told us that the inspection process currently includes threat assessments, a risk-indicator matrix, and a risk assessment to prompt organizations to consider threats and risk to their missions and operations resulting from vulnerabilities found on their networks. However, these inspections do not focus on the overall component but rather on specific units within a component. Additionally, the National Security Agency told us that its independent assessments would not include all information needed for a true risk assessment. Finally, OUSD (Intelligence) officials stated that they do not currently review the results of the National Security Agency assessments or Command Cyber Readiness Inspection reports, as previously discussed. Therefore, the senior-level official does not know which specific types of risk the department is incurring.

DOD officials stated that the department and its components have not incorporated risk assessments as part of their insider-threat programs in part because they have not fully implemented the department's insider-threat program. We also found that the DOD components we reviewed have not assessed risks because DOD has not provided guidance directing components to incorporate risk assessments into their respective insider-threat programs. Until DOD provides supplemental guidance directing components to incorporate risk assessments into their insider-threat programs, components may not assess risk and DOD will not be able to determine whether current security measures are adequate or whether proposed security measures would address a component's level of risk. Also, if DOD and its components do not align insider-threat security measures with threats, as required by the directive on national security systems, decision makers may lack information needed to make informed judgments.[50]

[50]Committee on National Security Systems Directive 504, *Directive on Protecting National Security Systems from Insider Threat*.

DOD Identified Technical and Policy Changes to Protect against Insider Threats in the Future but Does Not Consistently Collect Information for Oversight and Recommendations

Selected DOD Components Identified Technical and Policy Changes for Future Action

To help protect classified information and systems from future insider threats, in the technical area, officials from three of the six DOD components we reviewed told us that they are hoping to obtain or improve analytic tools that allow the component to identify anomalous behavior that could indicate insider-threat activities.[51] These analytic tools would obtain data through monitoring of user activity. Specifically, officials from two DOD components told us that they currently do not have these tools, but hope to obtain them in the future. Officials from another DOD component that does have such a tool told us that the component hopes to obtain an enhanced version that will allow the tool to analyze user behavior across systems of different classification levels (i.e., across the unclassified network, secret network, and top-secret network). According to National Insider Threat Task Force officials, these tools can also merge user activity-monitoring data with other sources of data to provide analysts with additional information.

In the policy area, component officials we interviewed also identified several actions to better protect against insider threats.

[51]Anomalous activities are network activities that are inconsistent with the expected norms. These activities, such as network activity outside of normal work hours or changes in typical data download patterns, could indicate the exploitation of cyber vulnerabilities, among other things.

- DOD Insider Threat Management and Analysis Center. Officials from three of the six DOD components we reviewed told us that they need DOD to make additional decisions regarding the proposed Defense Insider Threat Management and Analysis Center. According to an OUSD (Intelligence) briefing, DOD developed the concept for such a center based on a common recommendation that was identified in a 2012 Defense Science Board report and a 2013 Washington Navy Yard shooting after-action report; a similar recommendation was also identified in a 2010 Fort Hood shooting after-action report.[52] According to DOD's Washington Navy Yard Task Force Implementation Plan, the center will consist of cross-functional representatives that assess risk, recommend intervention or mitigation, and oversee the completion of case action on threats that insiders may pose to DOD personnel, DOD missions and resources, or both.[53] While this implementation plan identifies general efforts that the center could take, DOD has not issued a concept of operations and other planning documents that identify the center's actual functions, scope, level of involvement expected from the components, level of DOD involvement, and depth of analysis to be completed at the center, and the relationship between the center and the services' existing threat-analysis centers.
- Information sharing. Officials from two of the six components we reviewed cited the need for clear policies on when and how components can share information about individuals who are suspected or confirmed of being an insider threat. Similarly, officials said that the components need clear policy about sharing suspicious information that could be occurring across DOD components and other federal agencies.
- Continuous evaluation. Officials from one of the six components we reviewed told us that the components need policy that addresses continuous evaluation. Continuous evaluation is the practice of reviewing background information at any time during an individual's period of eligibility for access to classified information to determine

[52]Department of Defense, *Protecting the Force: Lessons from Fort Hood* (Washington, D.C.: January 2010); Defense Science Board, *Task Force Report: Predicting Violent Behavior* (Washington, D.C.: August 2012); and Department of Defense, *Security from Within: Independent Review of the Washington Navy Yard Shooting* (Washington, D.C.: November 2013).

[53]Under Secretary of Defense for Intelligence, *Washington Navy Yard Task Force Implementation Plan* (June 16, 2014).

whether the individual continues to meet the requirement for eligibility. According to DOD's Washington Navy Yard Task Force Implementation Plan, continuous evaluation will leverage automated records checks of personnel with access to DOD facilities or classified information. These automated records checks of authoritative commercial and government data sources (e.g., criminal, financial, or credit records) will flag issues of personnel security concern. These checks are to supplement existing security processes, such as self-reporting, to more quickly identify and prioritize information of adjudicative relevance or adverse events that occur between periodic reinvestigations. According to DOD's draft insider-threat program implementation plan, as of October 2014 DOD was still defining the organizational construct and concept of operations for continuous evaluation. DOD plans to provide this information in 2015.

DOD Is Not Consistently Collecting Information for Providing Oversight and Recommendations

DOD is not consistently collecting the information to manage and oversee insider-threat programs that could assist the Under Secretary of Defense for Intelligence in providing oversight and making recommendations to counter insider threats, such as the technical and policy changes identified above. DOD's insider-threat program directive requires that the Under Secretary of Defense for Intelligence provide management, accountability, and oversight of the department's insider-threat program, which includes the components' programs.[54] As part of these responsibilities, the Under Secretary of Defense for Intelligence is to oversee departmental capabilities and resources to counter insider threats, and make recommendations on program improvements and resources.[55] Additionally, DOD's defense security enterprise directive requires that the Under Secretary of Defense for Intelligence coordinate with the DOD CIO to establish enterprise investment goals informed by security-related efforts such as insider-threat initiatives.[56] OUSD (Intelligence) officials stated that they reach out to components on an as-

[54]DOD Directive 5205.16. *The DOD Insider Threat Program*.

[55]Specifically, the directive requires the Under Secretary of Defense for Intelligence to (1) recommend improvements on DOD insider-threat activities; (2) oversee strategy, programs, capabilities, and resources to counter insider threats; and (3) coordinate with the DOD CIO and the components to make resource recommendations in support of insider-threat activities.

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

needed basis to obtain information about insider-threat resources. However, according to the officials, they do not have a process to consistently collect information that identifies components prioritized needs, such as technical and policy needs for the future, and as a result face difficulties identifying component needs and comparing them against overall goals and strategy. Without collecting information from DOD components, the Under Secretary of Defense for Intelligence may face challenges fulfilling these management responsibilities. OUSD (Intelligence) and DOD CIO officials acknowledged that information from the components' about technical and policy needs would help the Under Secretary of Defense for Intelligence establish investment goals and make recommendations on program improvements and resources.

According to OUSD (Intelligence) officials, they do not have a process to collect information from the components to support management and oversight duties and inform resource recommendations and investment goals because DOD has not dedicated a program office that is focused on oversight of the insider-threat program. Specifically, while DOD has designated the Under Secretary of Defense for Intelligence as the department's senior insider-threat program official, officials stated that DOD has not identified a program office to execute the day-to-day responsibilities associated with this position and the program is instead currently supported within an office whose mission is policy, rather than management, oriented. Identification of a program office is consistent with federal standards for internal control and Office of the Director of National Intelligence guidance.[57] For example, federal standards for internal control call for an organizational structure that provides a framework to achieve agency objectives, including delegation of authority and responsibility for operating activities.[58] Additionally, the Office of the

[57]GAO/AIMD-00-21.3.1 and Office of the Director of National Intelligence, Office of the National Counterintelligence Executive, *Protecting Key Assets: A Corporate Counterintelligence Guide*.

[58]Per GAO's Standards for Internal Control in the Federal Government, another factor affecting the environment is the agency's organizational structure. It provides management's framework for planning, directing, and controlling operations to achieve agency objectives. A good internal-control environment requires that the agency's organizational structure clearly defines key areas of authority and responsibility and establishes appropriate lines of reporting. The environment is also affected by the manner in which the agency delegates authority and responsibility throughout the organization. These delegations cover authority and responsibility for operating activities, reporting relationships, and authorization protocols.

Director of National Intelligence guidance states that fully functional headquarters-level counterintelligence programs should include at least a program manager and supporting program staff. Without identifying a program office to support the Under Secretary of Defense for Intelligence's responsibilities in managing and overseeing DOD and components' insider-threat programs, DOD may not be able to collect all information about DOD components' technical and policy needs and could face challenges in establishing goals, and recommending resources and improvements to address insider threats.

Conclusions

The recent disclosures of classified information by insiders have damaged national security, potentially placed the lives of military service members at risk, and highlighted the importance of preventing or mitigating future threats to DOD's classified information and systems. DOD's April 2015 cyber strategy reflects the importance of mitigating insider threats to achieve the department's goal of defending DOD's information network, securing DOD data, and mitigating the risk to DOD missions.[59] DOD and its components are taking steps to address these threats by implementing programs that incorporate minimum standards. However, DOD components have not taken action to incorporate other key elements into their insider-threat programs because DOD has not issued guidance that identifies actions beyond the minimum standards that components should take to enhance their insider-threat programs. Such guidance would assist components in developing and strengthening insider-threat programs and better position the department to safeguard classified information and systems.

Gap and risk assessments allow DOD components to regularly assess the dynamic threat, vulnerability, and consequences associated with protecting classified information and systems from insider threats. While DOD has assessed aspects of its insider-threat program, it has not evaluated or documented the extent to which these assessments provide a continuing analysis of gaps as required by statute and has not incorporated risk assessments into insider-threat programs; nor have the results of the existing assessments been provided to DOD's senior insider-threat official. Without such an analysis of gaps and risk assessments—and without the Under Secretary of Defense for

[59]DOD, *The Department of Defense Cyber Strategy*.

Intelligence reviewing the results—DOD will face challenges understanding the extent to which its mitigations address current and evolving threats that insiders pose, and will be hampered in making more-informed management and resource decisions.

In addition, as the threat evolves, DOD will need to address future technical and policy changes. However, DOD is not consistently collecting information about future technical and policy changes because it has not established an insider-threat program office. Without designating a program office dedicated to the oversight role, DOD may not ensure the collection of all information about components' needs and could face challenges in establishing goals, and recommending resources and improvements to address insider threats.

Recommendations for Executive Action

To further enhance the department's efforts to protect its classified information and systems from insider threats, we recommend that the Secretary of Defense take the following four actions.

We recommend that the Secretary of Defense direct the Under Secretary of Defense for Intelligence to take the following actions:

- In planned supplemental planning guidance to be developed, identify actions beyond the minimum standards that components should take to enhance their insider-threat programs.
- Evaluate and document the extent to which current assessments provide a continuing analysis of gaps for all DOD components; report to Congress on the results of this evaluation; and direct that the overall results of these self- and independent assessments be reviewed by the Office of the Under Secretary of Defense for Intelligence.
- Provide DOD components supplemental guidance that directs them to incorporate risk assessments into their insider-threat programs.

We also recommend that the Secretary of Defense take action to do the following:

- Identify an insider-threat program office to support the Under Secretary of Defense for Intelligence's responsibilities in managing and overseeing DOD and components' insider-threat programs.

Agency Comments and Our Evaluation

DOD provided written comments on a draft of this report and these comments are reproduced in appendix IV. DOD concurred or partially concurred with all four of our recommendations. The Departments of Homeland Security and Justice and the Office of the Director of National Intelligence reviewed a draft of this report but did not provide any comments.

DOD agreed with our recommendation to identify in supplemental guidance actions beyond the minimum standards that components should take to enhance their insider-threat programs. DOD stated that it will publish a detailed implementation plan in 2015 to assist components in implementing multiple actions required in all insider-threat programs. Issuing an implementation plan is a positive step and one required by the minimum standards. However, as stated in our report, the draft implementation plan that we reviewed focused on actions that DOD would take to implement the minimum standards and did not provide DOD components additional information about other key elements that component officials told us would be helpful. We therefore believe that DOD needs to update its draft implementation plan before it is issued to include guidance beyond the minimum standards, or issue this guidance in another form. This will ensure that DOD components will be better positioned to enhance their insider-threat programs and the department will be better positioned to protect its classified information and systems.

DOD partially agreed with our recommendation to evaluate and document the extent to which current assessments provide a continuing analysis of gaps for all DOD components, report to Congress on the results of this evaluation, and direct that the overall results of these assessments be reviewed by OUSD (Intelligence). In its comments, DOD first stated that it analyzes security gaps each quarter through its self-assessments, which identify gaps in program capabilities. While these assessments can provide DOD and its components information required under E.O. 13587, DOD did not indicate whether it would evaluate and document whether those assessments provide a continuing analysis of gaps as identified in Section 922 of the National Defense Authorization Act for Fiscal Year 2012. Such an evaluation is necessary to determine whether DOD is meeting the statutory requirement to complete a continuing analysis of gaps in security measures and of technology, policies, and processes that are needed to increase the capability of DOD's insider-threat program to address these gaps. We believe such an evaluation is prudent since, as we stated in the report, the information from the self-assessments and independent assessments cited by DOD is sometimes limited. Therefore, we continue to believe that DOD should take steps to evaluate and

document the extent to which these current assessments provide the same information as the statutorily-required analysis of gaps in order to determine the adequacy of DOD's insider-threat detection and analysis capabilities. Second, DOD stated that it met the congressional reporting requirement with its 2013 report, which did not require additional reporting. However, as we stated in the report, DOD did not complete the actions it described in the 2013 report and thus has not provided Congress with current information that would assist it in making informed decisions about funding to address gaps in security measures. Therefore, we continue to believe that the department should report to Congress on the results of its evaluation of current assessments, which identify gaps in security measures under its program for information-sharing protection and insider-threat mitigation. DOD also stated that the self-assessments and independent assessments of component insider-threat programs have begun, and agreed that these assessments will be provided to OUSD (Intelligence) for review upon completion.

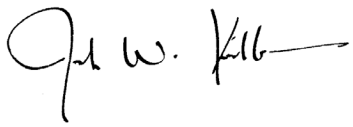
DOD agreed with our recommendation to provide components with supplemental guidance directing them to incorporate risk assessments into their insider-threat programs. DOD stated that its forthcoming implementation plan will require components to employ a process to identify critical assets and assess the components' risk posture. DOD also stated that other risk assessments will be considered and integrated with insider-threat risks. We agree that incorporating risk assessments will assist component leadership in making informed judgments and better enable them to align security measures with threats.

DOD partially agreed with our recommendation to identify an insider-threat program office to support the Under Secretary of Defense for Intelligence's responsibilities in managing and overseeing insider-threat programs. DOD stated that it has chartered a study to examine the feasibility and associated requirements for establishing a separate DOD insider-threat program office. DOD expects to complete this study by July 2016. Our recommendation does not state that DOD needs to establish a separate program office, but rather that DOD should identify a program office to support the Under Secretary's responsibilities. Therefore we would hope that as part of its study DOD would assign responsibility for this oversight to a program office. In its comments, DOD also referred to steps it has taken to establish the Defense Insider Threat Management and Analysis Center and described some of the center's future capabilities. However, as we note in our report, DOD components described their need for policy about the center, and DOD has not yet issued a concept of operations and other planning documents that identify

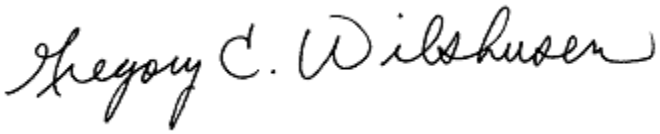
the center's actual functions, scope, and relationships with existing service threat-analysis centers. Once DOD implements our recommendation and identifies an insider-threat program office, the Under Secretary of Defense for Intelligence will be better positioned to collect information from the components about their prioritized technical and policy needs for the future, such as policy regarding the Defense Insider Threat Management and Analysis Center.

We are sending copies of this report to the appropriate congressional committees, the Secretaries of Defense and Homeland Security; the Attorney General of the United States; and the Director of National Intelligence. In addition, this report will also be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions concerning this report, please contact Joseph W. Kirschbaum at (202) 512-9971 or KirschbaumJ@gao.gov or Gregory C. Wilshusen at (202) 512-6244 or WilshusenG@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 V.



Joseph W. Kirschbaum
Director
Defense Capabilities and Management



Gregory C. Wilshusen
Director, Information Security Issues
Information Technology

List of Committees

The Honorable John McCain
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Thad Cochran
Chairman
The Honorable Richard Durbin
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

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

The Honorable Rodney Frelinghuysen
Chairman
The Honorable Pete Visclosky
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Scope and Methodology

To evaluate the extent to which the Department of Defense (DOD) has implemented an insider-threat program that incorporates minimum standards and key elements to protect classified information and systems, we evaluated initiatives that DOD had established and policy and guidance that identify responsibilities within the department to address the threat that insiders pose to classified information and systems. We selected a nonprobability sample of six DOD components to assess implementation efforts at the component level.[1] These six components include three combat support agencies; one military service; one combatant command; and one service sub-command. We selected these six components based on several factors including their specific roles in supporting DOD networks, prior insider-threat incidents, and reported progress in implementing insider-threat programs. In order to avoid duplication with an ongoing DOD Inspector General evaluation, we included only one military service.[2] While not generalizable, the information we obtained from these selected components provided insight about steps components are taking and challenges they are encountering.

We developed a questionnaire based on our research objectives, the six minimum standards issued in 2012 by the President, and industry leading practices, and solicited responses from the six selected components. We administered the questionnaire and collected responses from all six selected components and the Office of the Under Secretary of Defense for Intelligence (OUSD [Intelligence]), and conducted follow-up meetings as needed. We also collected policies and guidance related to the responses and programs. We then used the questionnaire responses and information obtained from meetings and document reviews to assess each component's insider-threat program implementation and content. We reviewed the questionnaire responses to ensure the responses were consistent with the information we obtained. Any discrepancies were documented and follow up was conducted as necessary. Using a scorecard methodology, we developed a rating system to assess the

[1]DOD defines "DOD components" to include the Office of the Secretary of Defense, the military departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the combatant commands, the DOD Office of Inspector General, the defense agencies, the DOD field activities, and all other entities within DOD.

[2]In April 2014, the DOD Inspector General initiated work assessing the implementation of insider-threat programs at the four military services. According to the DOD Inspector General, it plans to issue its report in mid-2015.

components against the minimum standards to determine the extent to which the minimum standards were incorporated into component insider-threat programs. We used three ratings for assessing the incorporation of each minimum standard: addressed all tasks associated with minimum standard, addressed at least one task, and did not address tasks. We rated components that answered yes to all questions related to that minimum standard and its associated tasks as addressed all tasks. We rated components that answered yes to one or more question related to that minimum standard and its associated tasks as addressed at least one task. We rated components that did not answer yes to at least one question related to a minimum standard and its associated tasks as having not addressed any of the tasks. Two analysts independently assessed and assigned a rating to each standard and then compared their independent ratings, discussed any differences, and determined a final rating. We then compiled the final ratings into a scorecard graphic. An independent analyst reviewed our analysis and ratings for accuracy and consistency.

Additionally, to identify 25 key elements for a framework applicable to insider-threat programs, we analyzed Executive Order 13587 (E.O. 13587), the national insider-threat policy and minimum standards, DOD guidance and reports, Committee on National Security Systems guidance, a set of leading practices that the National Insider Threat Task Force recommends, practices that other federal agencies and private industry use, and a list of essential elements that a group of private-sector

and U.S. government analysts created.[3] For a list of the resources we consulted by key element, see appendix III. We then organized this information into a framework of 25 key elements. We based these elements upon the principles that we identified, but note that this framework is not necessarily a comprehensive list since other principles may exist that did not surface based on our inquiry that could benefit insider-threat programs. We discussed the framework with DOD and

[3]We analyzed information from Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (July 2011); DOD Directive 5105.42, *Defense Security Service (DSS)* (Aug. 3, 2010) (incorporating change 1, Mar. 31, 2011); DOD Directive 5200.43, *Management of the Defense Security Enterprise* (Oct. 1, 2012) (incorporating change 1, Apr. 24, 2013); DOD Directive 5240.06, *Counterintelligence Awareness and Reporting (CIAR)* (May 17, 2011) (incorporating change 1, May 30, 2013); DOD Directive-Type Memorandum 09-0912, *Interim Policy Guidance for DOD Physical Access Control* (Dec. 8, 2009) (incorporating change 5, Mar. 3, 2015); DOD Instruction 1438.06, *DOD Workplace Violence Prevention and Response Policy* (Jan. 16, 2014); DOD Instruction 2000.12, *DOD Antiterrorism (AT) Program* (Mar. 1, 2012) (incorporating change 1, Sept. 9, 2013); DOD Instruction 2000.16, *DOD Antiterrorism (AT) Standards* (Oct. 2, 2006) (incorporating change 2, Dec. 8, 2006); DOD Instruction 2000.26, *Suspicious Activity Reporting (SAR)* (Sept. 23, 2014); DOD Instruction 5240.22, *Counterintelligence Support to Force Protection* (Sept. 24, 2009) (incorporating change 1, Oct. 15, 2013); DOD Instruction 5240.26, *Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat* (May 4, 2012) (incorporating change 1, Oct. 15, 2013); DOD Instruction 5525.15, *Law Enforcement (LE) Standards and Training in the DOD* (Apr. 27, 2012); DOD Instruction 6055.17, *DOD Installation Emergency Management (IEM) Program* (Jan. 13, 2009) (incorporating change 1, Nov. 19, 2010); DOD Instruction 8500.01, *Cybersecurity* (Mar. 14, 2014); DOD 5200.2-R, *Personnel Security Program* (January 1987) (incorporating change 3, Feb. 23, 1996); DOD 5200.8-R, *Physical Security Program* (Apr. 9, 2007) (incorporating change 1, May 27, 2009); DOD Manual 5200.01, *DOD Information Security Program: Protection of Classified Information*, vol. 3 (Feb. 24, 2012) (incorporating change 2, Mar. 19, 2013)*;* Department of Defense, *Insider Threat Mitigation: Final Report of the Insider Threat Integrated Process Team* (Apr. 24, 2000); Joint Chiefs of Staff, Joint Pub. 3-07.2, *Antiterrorism* (Mar. 14, 2014); Secretary of Defense, *Final Recommendations of the Fort Hood Follow-on Review*, memorandum (Aug. 18, 2010); Committee on National Security Systems Directive 504, *Directive on Protecting National Security Systems from Insider Threat* (Feb. 4, 2014); E.O. 13587; White House, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*; Office of Management and Budget, *Suitability and Security Processes Review: Report to the President* (February 2014); *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies* (Dec. 12, 2013); GAO*, Standards for Internal Control in the Federal Government*, GAO/AIMD-00.21.3.1 (Washington, D.C.: Nov. 1, 1999); Office of the Director of National Intelligence, Office of the National Counterintelligence Executive, *Protecting Key Assets: A Corporate Counterintelligence Guide* (11137482 ID 6-11); Carnegie Mellon Software Engineering Institute, *Common Sense Guide to Mitigating Insider Threats,* 4th ed. (December 2012); and the Intelligence and National Security Alliance, *Insider Threat Resource Directory*. In addition, we consulted officials from DOD, the Department of Homeland Security, Department of Justice, Federal Bureau of Investigation, and Lockheed Martin.

private-sector officials and incorporated comments and changes as appropriate. We also met with officials from the Department of Homeland Security and Department of Justice and obtained information about their insider-threat programs because E.O. 13587 assigns them roles for insider threats. While not generalizable, the information we obtained provided insight about the implementation of insider-threat programs at federal agencies other than DOD.

To evaluate the extent to which DOD and others have assessed DOD's insider-threat program to protect classified information and systems, we obtained copies of DOD's quarterly self-assessments from December 2013 through February 2015, in which DOD reported its progress in complying with minimum standards. We compared the current DOD assessment efforts to those described in E.O. 13587 and national policy, and we interviewed officials from DOD and its components about their self-assessment process and results. We did not independently verify the accuracy of the self-assessments since it was beyond the scope of this review. We met with U.S. Cyber Command and obtained information about Command Cyber Readiness Inspections, including a list of organizations inspected and the overall results related to insider threat. We did not independently verify the accuracy of this information since it was beyond the scope of this review. We also met with officials from the National Insider Threat Task Force and National Security Agency who are involved in conducting independent assessments, confirmed that they have assessed some DOD components, and obtained and reviewed copies of the assessments. To determine the extent to which DOD conducted the continuing analysis of gaps in its insider-threat program required by National Defense Authorization Act for Fiscal Year 2012, we obtained and reviewed DOD's 2013 report to Congress in which it described its plan for conducting a continuing analysis, and interviewed officials about the current status of the analysis. To determine the extent to which DOD incorporated risk assessments in its insider-threat program, we reviewed DOD, Committee on National Security Systems, and National Insider Threat Task Force guidance related to the assessment of an agency's risk posture. We interviewed OUSD (Intelligence) and DOD Chief Information Officer (DOD CIO) officials about the extent to which DOD conducted risk assessments related to insider-threat programs, and asked components about the extent to which they conducted risk assessments that would inform insider-threat programs.

To evaluate the extent to which DOD has identified any technical or policy changes to protect its classified information and systems from insider threats in the future, we focused on initiatives to be implemented

beginning in 2015 and those initiatives not included in DOD's existing insider-threat guidance. We did not include initiatives that are being assessed in-depth by a related GAO engagement.[4] We collected information about initiatives through the questionnaire we developed for the six selected components, and through interviews with component officials. The questionnaire and interviews were used to identify any future technical and policy changes to address threats to component information and information systems. We also asked component officials about their process for prioritizing and planning for initiatives. We then interviewed officials from OUSD (Intelligence) and DOD CIO about how the department is collecting information about these initiatives and using the information to inform resource recommendations and program improvements. We compared these responses to DOD guidance on responsibilities for insider-threat programs and the defense security enterprise, federal standards for internal control,[5] and Office of the Director of National Counterintelligence guidance. We did not evaluate the initiatives themselves or assess each initiative's relative priority or efficacy.

We obtained relevant data and documentation and interviewed officials from components within the Department of Defense, Department of Homeland Security, Department of Justice, and the Office of the Director of National Intelligence's National Insider Threat Task Force. We also met with representatives from Carnegie Mellon University Software Engineering Institute – CERT Insider Threat Center and Lockheed Martin.

We conducted this performance audit from May 2014 to June 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.

[4]We are currently conducting an engagement assessing DOD's force-protection efforts to address insider threats at U.S. installations. We anticipate issuing a product in summer 2015.

[5]GAO, *Standards for Internal Control in the Federal Government,* GAO/AIMD-00-21.3.1 (Washington, D.C.: Nov. 1, 1999).

Appendix II: Minimum Standards for Executive Branch Insider-Threat Programs

DESIGNATION OF SENIOR OFFICIAL(S): Each agency head shall designate a senior official or officials, who shall be principally responsible for establishing a process to gather, integrate, and centrally analyze, and respond to Counterintelligence (CI), Security, Information Assurance (IA), Human Resources (HR), Law Enforcement (LE), and other relevant information indicative of a potential insider threat. Senior Official(s) shall:	1. Provide management and oversight of the insider threat program and provide resource recommendations to the agency head. 2. Develop and promulgate a comprehensive agency insider threat policy to be approved by the agency head within 180 days of the effective date of the National Insider Threat Policy. Agency policies shall include internal guidelines and procedures for the implementation of the standards contained herein. 3. Submit to the agency head an implementation plan for establishing an insider threat program and annually thereafter a report regarding progress and/or status within that agency. At a minimum, the annual reports shall document annual accomplishments, resources allocated, insider threat risks to the agency, recommendations and goals for program improvement, and major impediments or challenges. 4. Ensure the agency's insider threat program is developed and implemented in consultation with that agency's Office of General Counsel and civil liberties and privacy officials so that all insider threat program activities to include training are conducted in accordance with applicable laws, whistleblower protections, and civil liberties and privacy policies. 5. Establish oversight mechanisms or procedures to ensure proper handling and use of records and data described below, and ensure that access to such records and data is restricted to insider threat personnel who require the information to perform their authorized functions. 6. Ensure the establishment of guidelines and procedures for the retention of records and documents necessary to complete assessments required by Executive Order 13587. 7. Facilitate oversight reviews by cleared officials designated by the agency head to ensure compliance with insider threat policy guidelines, as well as applicable legal, privacy and civil liberty protections.
INFORMATION INTEGRATION, ANALYSIS AND RESPONSE: Agency heads shall:	1. Build and maintain an insider threat analytic and response capability to manually and/or electronically gather, integrate, review, assess, and respond to information derived from CI, Security, IA, HR, LE, the monitoring of user activity, and other sources as necessary and appropriate. 2. Establish procedures for insider threat response action(s), such as inquiries, to clarify or resolve insider threat matters while ensuring that such response action(s) are centrally managed by the insider threat program within the agency or one of its subordinate entities. 3. Develop guidelines and procedures for documenting each insider threat matter reported and response action(s) taken, and ensure the timely resolution of each matter.
INSIDER THREAT PROGRAM PERSONNEL: Agency heads shall ensure personnel assigned to the insider threat program are fully trained in:	1. Counterintelligence and security fundamentals to include applicable legal issues; 2. Agency procedures for conducting insider threat response action(s); 3. Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information; 4. Applicable civil liberties and privacy laws, regulations, and policies; and 5. Investigative referral requirements of Section 811 of the Intelligence Authorization Act for FY 1995, as well as other policy or statutory requirements that require referrals to an internal entity, such as a security office or Office of Inspector General, or external investigative entities such as the Federal Bureau of Investigation, the Department of Justice, or military investigative services

ACCESS TO INFORMATION: Agency heads shall:	1. Direct CI, Security, IA, HR, and other relevant organizational components to securely provide insider threat program personnel regular, timely, and, if possible, electronic access to the information necessary to identify, analyze, and resolve insider threat matters. Such access and information includes, but is not limited to, the following: a. Counterintelligence and Security. All relevant databases and files to include, but not limited to, personnel security files, polygraph examination reports, facility access records, security violation files, travel records, foreign contact reports, and financial disclosure filings. b. Information Assurance. All relevant unclassified and classified network information generated by IA elements to include, but not limited to, personnel usernames and aliases, levels of network access, audit data, unauthorized use of removable media, print logs, and other data needed for clarification or resolution of an insider threat concern. c. Human Resources. All relevant HR databases and files to include, but not limited to, personnel files, payroll and voucher files, outside work and activities requests, disciplinary files, and personal contact records, as may be necessary for resolving or clarifying insider threat matters. 2. Establish procedures for access requests by the insider threat program involving particularly sensitive or protected information, such as information held by special access, law enforcement, inspector general, or other investigative sources or programs, which may require that access be obtained upon request of the Senior Official(s). 3. Establish reporting guidelines for CI, Security, IA, HR, and other relevant organizational components to refer relevant insider threat information directly to the insider threat program. 4. Ensure insider threat programs have timely access, as otherwise permitted, to available United States Government intelligence and counterintelligence reporting information and analytic products pertaining to adversarial threats.
MONITORING USER ACTIVITY ON NETWORKS: Agency heads shall ensure insider threat programs include:	1. Either internally or via agreement with external agencies, the technical capability, subject to appropriate approvals, to monitor user activity on all classified networks in order to detect activity indicative of insider threat behavior. When necessary, Service Level Agreements (SLAs) shall be executed with all other agencies that operate or provide classified network connectivity or systems. SLAs shall outline the capabilities the provider will employ to identify suspicious user behavior and how that information shall be reported to the subscriber's insider threat personnel. 2. Policies and procedures for properly protecting, interpreting, storing, and limiting access to user activity monitoring methods and results to authorized personnel. 3. Agreements signed by all cleared employees acknowledging that their activity on any agency classified or unclassified network, to include portable electronic devices, is subject to monitoring and could be used against them in a criminal, security, or administrative proceeding. Agreement language shall be approved by the Senior Official(s) in consultation with legal counsel. 4. Classified and unclassified network banners informing users that their activity on the network is being monitored for lawful United States Government-authorized purposes and can result in criminal or administrative actions against the user. Banner language shall be approved by the Senior Official(s) in consultation with legal counsel.

EMPLOYEE TRAINING AND AWARENESS: Agency heads shall ensure insider threat programs:	1. Provide insider threat awareness training, either in-person or computer-based, to all cleared employees within 30 days of initial employment, entry-on-duty (EOD), or following the granting of access to classified information, and annually thereafter. Training shall address current and potential threats in the work and personal environment, and shall include, at a minimum, the following topics: a. The importance of detecting potential insider threats by cleared employees and reporting suspected activity to insider threat personnel or other designated officials; b. Methodologies of adversaries to recruit trusted insiders and collect classified information; c. Indicators of insider threat behavior and procedures to report such behavior; and d. Counterintelligence and security reporting requirements, as applicable. 2. Verify that all cleared employees have completed the required insider threat awareness training contained in these standards. ‘ 3. Establish and promote an internal network site accessible to all cleared employees to provide insider threat reference material, including indicators of insider threat behavior, applicable reporting requirements and procedures, and provide a secure electronic means of reporting matters to the insider threat program.

Source: The White House. | GAO-15-544.

Note: Data are from the White House, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (Washington, D.C.: Nov. 12, 2012).

Appendix III: Sources for Key Elements of Insider-Threat Programs GAO Identified

Program phase	Program element	Source
Deter	Identify program office	GAO, *Standards for Internal Control in the Federal Government,* GAO/AIMD-00.21.3.1 (Washington, D.C.: Nov. 1, 1999); Office of the Director of National Intelligence, Office of the National Counterintelligence Executive, *Protecting Key Assets*: *A Corporate Counterintelligence Guide* (11137482 ID 6-11)
	Establish rules and policies	Department of Defense (DOD) Instruction 5240.26 (*Countering Espionage, International Terrorism, and the Counterintelligence Insider Threat*); DOD Instruction 2000.12 (DOD *Antiterrorism [AT] Programs*); DOD Instruction 2000.16 (DOD *Antiterrorism [AT] Standards)*; DOD Directive 5105.42 (*Defense Security Service*); DOD Directive 5200.43 (*Management of the Defense Security Enterprise*); DOD, *Insider Threat Mitigation: Final Report of the Insider Threat Integrated Process Team*; Committee on National Security Systems Directive 504 (*Directive on Protecting National Security Systems from Insider Threat*); *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*; Carnegie Mellon Software Engineering Institute, *Common Sense Guide to Mitigating Insider Threats*
	Institute consequences if rules and policies not followed	DOD Instruction 8500.01 (*Cybersecurity*); DOD Instruction 2000.12; DOD 5200.08-R (*Physical Security Program*); DOD, Insider Threat Mitigation: Final Report; Carnegie Mellon, *Common Sense Guide*
	Communicate program goals, policies, and consequences to staff and contractors	DODI 8500.01; DODD 5105.42; DOD Instruction 1438.06 (DOD *Workplace Violence Prevention and Response Policy*); DODI 2000.12; DOD, *Insider Threat Mitigation: Final Report;* Carnegie Mellon, *Common Sense Guide*
	Conduct internal spot checks	DOD 5200.08-R; DODI 2000.16; DOD, *Insider Threat Mitigation: Final Report*; Carnegie Mellon, *Common Sense Guide*
	Host red team	DOD, *Department of Defense Strategy for Operating in Cyberspace*; DODI 8500.01; Joint Chiefs of Staff, Joint Pub. 3-07.2 (*Antiterrorism*); *Liberty and Security in a Changing World*: *Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*
Prevent	Integrate personnel clearance	DODI 8500.01; DODI 5240.26; DOD 5200.2-R (DOD *Personnel Security Program*); DODD 5105.42; DOD, *Insider Threat Mitigation: Final Report*; Office of Management and Budget, *Suitability and Security Processes Review* (February 2014); *Liberty and Security in a Changing World;* Carnegie Mellon, *Common Sense Guide*
	Train and exercise employees	DODI 5240.26; DODI 8500.01; DODI 1438.06; DODI 2000.12; DODI 2000.16; Joint Pub. 3-07.2; DOD Directive 5240.06 (*Counterintelligence Awareness and Reporting)*; DODD 5105.42; CNSSD 504; *National Insider Threat Policy and Minimum Standards*; Carnegie Mellon, *Common Sense Guide*
	Develop a baseline of normal activity	DODI 5240.26; Joint Pub. 3-07.2; DOD, *Insider Threat Mitigation: Final Report*; CNSSD 504; Carnegie Mellon, *Common Sense Guide*
	Conduct risk assessments	DODI 8500.01; DODI 2000.16; Joint Pub. 3-07.2; DOD, *Insider Threat Mitigation: Final Report*; CNSSD 504; Carnegie Mellon, *Common Sense Guide*
	Institute internal controls and security controls	DODI 5240.26; DODI 8500.01; DODI 2000.12; CNSSD 504; DOD Instruction 2000.26 (*Suspicious Activity Reporting*); Carnegie Mellon, *Common Sense Guide*

Program phase	Program element	Source
Detect	Ensure cross-function coordination	DODI 5240.26; DODI 8500.01; DODI 1438.06; DODI 2000.12; DODI 2000.16; CNSSD 504; *National Insider Threat Policy and Minimum Standards*; Carnegie Mellon, *Common Sense Guide*
	Monitor activity	DODI 5240.26; DODI 8500.01; CNSSD 504; Directive-Type Memorandum 09-012 *(Interim Policy Guidance for DOD Physical Access Control)*; *National Insider Threat Policy and Minimum Standards*; *Liberty and Security in a Changing World*; Carnegie Mellon, *Common Sense Guide*
	Perform risk-based analytics	DODI 5240.26; CNSSD 504; Joint Pub. 3-07.2; *Liberty and Security in a Changing World*; Carnegie Mellon, *Common Sense Guide*
	Conduct internal audits and reporting	DODI 5240.26; DODI 8500.01; DODI 2000.12; DODI 2000.16; DOD Manual 5200.01, vol. 3 (*DOD Information Security Program: Protection of Classified Information*); DODD 5105.42; DOD, *Insider Threat Mitigation: Final Report*; CNSSD 504; Joint Pub. 3-07.2; *National Insider Threat Policy and Minimum Standards*; Carnegie Mellon, *Common Sense Guide*
	Allow external audits	DODI 5240.26; DODI 2000.16; Joint Pub. 3-07.2; *National Insider Threat Policy and Minimum Standards*
	Encourage peer reporting	DODI 5240.26; DODI 8500.01; DODI 1438.06; DODD 5240.06; DODM 5200.01, vol. 3; Joint Pub. 3-07.2; *National Insider Threat Policy and Minimum Standards*; Carnegie Mellon, *Common Sense Guide*
	Create and retain auditable records of actions taken	DODI 8500.01; DODI 1438.06; DOD, *Insider Threat Mitigation: Final Report*; CNSSD 504; DTM 09-012; Carnegie Mellon, *Common Sense Guide*
	Share information as appropriate	DODI 5240.26; DODI 8500.01; DODI 5240.22; DODD 5105.42; DTM 09-012; Joint Pub. 3-07.2; E.O. 13587; Carnegie Mellon, *Common Sense Guide*
Take Action	Suspend access	DOD 5200.2-R; DTM 09-012; DOD, *Insider Threat Mitigation: Final Report*; Carnegie Mellon, *Common Sense Guide*
	Take personnel action—counsel, terminate, refer to appropriate authorities	DODI 5240.26; DODI 8500.01; DODI 2000.26; DODI 2000.12; DODI 2000.16; DODI 6055.17; Joint Pub. 3-07.2; DODM 5200.01, vol. 3; Carnegie Mellon, *Common Sense Guide*
	Conduct damage assessments	DODI 8500.01; DODI 2000.16; DODI 6055.17; DODM 5200.01, vol. 3; DOD, *Insider Threat Mitigation: Final Report*; Intelligence and National Security Alliance, *Insider Threat Resource Directory*
	Develop, disseminate, and incorporate best practices and lessons learned	DODI 5240.26; DODI 2000.12; DODI 2000.16; DODI 6055.17; Joint Pub. 3-07.2; DOD, *Insider Threat Mitigation: Final Report*; *Intelligence and National Security Alliance, Insider Threat Resource Directory*
	Train, exercise, and equip response personnel	DOD 5200.8-R; DODI 2000.12; DODI 2000.16; DOD Instruction 5525.15 (*Law Enforcement [LE*] *Standards and Training in the DOD*); DODI 6055.17
	Establish formal and informal agreements	DOD 5200.8-R; DODI 2000.16; DODI 6055.17; Joint Pub. 3-07.2; Secretary of Defense, *Final Recommendations of the Fort Hood Follow-on Review, memorandum* (Aug. 18, 2010)

Source: GAO analysis of Department of Defense, Office of the Director of National Intelligence, Carnegie Mellon, and Intelligence and National Security Alliance data. | GAO-15-544

Appendix IV: Comments from the Department of Defense

Note: Since the recommendations in this report are the same as in the classified report, which DOD responded to in a letter we received on April 7, 2015 (see letter to the right), we did not send this version of the report out for agency comment.

UNACLASSIFIED WHEN NOT INCLUDED IN CLASSIFIED REPORT

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

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

Dear Mr. Kirschbaum:

(U) This is the Department of Defense (DoD) response to the General Accountability Office (GAO) Draft Report, [redacted], "INSIDER THREATS: DoD Should Strengthen Management and Guidance to Protect Classified Information and Systems," dated February 19, 2015 (GAO Code 351927).

(U) The Department's comments to the draft report are attached. Overall lead for this effort in the Department of Defense is the Under Secretary of Defense for Intelligence (USD(I)). The point of contact for USD(I) is Mr. Don Hopkins, at email: Don.r.hopkins.civ@mail.mil, (703) 604-1114. The alternate POC for this response is Ms. Carmen Santos-Logan, at email: Carmen.j.santoslogan.civ@mail.mil, (571) 372-4692.

Sincerely,
DE VRIES.DAVID.LEE.1093968235
Digitally signed by DE VRIES.DAVID.LEE.1093968235
DN: c=US, o=U.S. Government, ou=NSS, ou=DoD, ou=OSD, cn=DE VRIES.DAVID.LEE.1093968235
Date: 2015.04.07 15:10:04 -04'00'
David L. De Vries
Principal Deputy

Attachment:
As stated

UNACLASSIFIED WHEN NOT INCLUDED IN CLASSIFIED REPORT

UNCLASSIFIED

GAO DRAFT REPORT DATED FEBRUARY 19, 2015
[redacted] (GAO Code 351927)

INSIDER THREATS: DoD Should Strengthen Management and Guidance to Protect Classified Information and Systems

(U) RECOMMENDATION 1: To further enhance the department's efforts to protect its classified information and systems from insider threats, GAO recommends that the Secretary of Defense direct the Under Secretary of Defense for Intelligence to take the following action. In planned supplemental planning guidance to be developed, identify actions beyond the minimum standards that Components should take to enhance their insider threat programs.

(U) DOD RESPONSE: Concur. DoD will publish a detailed plan in 2015 to assist Components implement the multiple actions required in all insider threat programs.

(U) RECOMMENDATION 2: To further enhance the department's efforts to protect its classified information and systems from insider threats, GAO recommends that the Secretary of Defense direct the Under Secretary of Defense for Intelligence to take the following action. Evaluate and document the extent to which current assessments provide a continuing gap analysis for all DoD Components; report to Congress on the results of this evaluation; and direct that the overall results of these self and independent assessments be reviewed by the Office of the Under Secretary of Defense for Intelligence.

(U) DOD RESPONSE: Partially Concur. DoD performs analysis of insider threat security gaps each quarter through the compilation of Key Information Sharing and Safeguarding Indicators. This data identifies the strengths and weaknesses of insider threat programs in the Department, and when jointly assessed, identifies gaps in program capabilities. Self and independent assessments of the Component insider threat programs have begun and will continue to evaluate the state of programs as they mature. When completed, these reports will be provided to the OUSD(I) for review. Lastly, the statutory issue cited by GAO requiring DoD to provide congressional defense committees a report within 90 days of the statute's enactment was met in March 2013 and Public Law 112-81 did not direct DoD to submit follow-up reports.

(U) RECOMMENDATION 3: To further enhance the department's efforts to protect its classified information and systems from insider threats, GAO recommends that the Secretary of Defense direct the Under Secretary of Defense for Intelligence to take the following action. Provide DoD Components supplemental guidance that directs them to incorporate risk assessments into their insider threat programs.

(U) DOD RESPONSE: Concur. The forthcoming DoD insider threat implementation plan will require DoD Component programs to employ a process which identifies its critical assets and assesses its risk posture. Furthermore, the risk assessments inherent with information systems, physical security, operations security, and personnel security today will be considered and integrated with the insider threat risks.

UNCLASSIFIED

UNCLASSIFIED

(U) RECOMMENDATION 4: GAO recommends that the Secretary of Defense take action to identify an insider threat program office to support the Under Secretary of Defense for Intelligence's responsibilities in managing and overseeing DoD and Component's insider threat programs.

(U) DOD RESPONSE: Partially Concur. The Office of the Under Secretary of Defense (Intelligence) (OUSD(I)) has chartered a study to examine the feasibility and associated requirements for establishing a separate DoD insider threat program office. The study is projected to be completed by July 2016 and will inform a final decision on the necessity for a separate program office. Nevertheless, the Office of the Secretary of Defense (OSD) has taken actions to strengthen the Department's insider threat capabilities. On December 12, 2014, the Under Secretary of Defense for Intelligence directed the Director, Defense Security Service, to incubate the Defense Insider Threat Management and Analysis Center (DITMAC). The DITMAC's specified responsibilities include an enterprise-level management capability enabling OSD-level oversight of DoD Components' insider threat responsibilities while ensuring Department-wide awareness for specific threshold-level insider threat events. DITMAC operations, metrics and case studies will inform, support and enable OUSD(I)'s management and oversight of DoD's insider threat program.

UNCLASSIFIED

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contacts

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

Gregory C. Wilshusen, (202) 512-6244 or WilshusenG@gao.gov

Staff Acknowledgments

In addition to the individuals named above, Tommy Baril, Assistant Director; Jeffrey Knott, Assistant Director; Tracy Barnes; Lon Chin; Grace Coleman; Nicole Collier; Kristi Dorsey; Ashley Houston; Amie Lesser; Richard Powelson; Terry Richardson; Monica Savoy; and Jennifer Spence made key contributions to this report.

Related Unclassified GAO Products

Department of Defense Cybersecurity

Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates. GAO-11-695R. Washington, D.C.: July 29, 2011.

Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities. GAO-11-75. Washington, D.C.: July 25, 2011.

Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities. GAO-11-421. Washington, D.C.: May 20, 2011.

Cybersecurity

Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems. GAO-15-6. Washington, D.C.: December 12, 2014.

Information Security: Agencies Need to Improve Oversight of Contractor Controls. GAO-14-612. Washington, D.C.: August 8, 2014.

Information Security: Agencies Need to Improve Cyber Incident Response Practices. GAO-14-354. Washington, D.C.: April 30, 2014.

Critical Infrastructure Protection: More Comprehensive Planning Would Enhance the Cybersecurity of Public Safety Entities' Emerging Technology. GAO-14-125. Washington, D.C.: January 28, 2014.

Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent. GAO-14-34. Washington, D.C.: December 9, 2013.

Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness. GAO-13-776. Washington, D.C.: September 26, 2013.

Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented. GAO-13-187. Washington, D.C.: February 14, 2013.

Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged. GAO-12-757. Washington, D.C.: September 18, 2012.

Cybersecurity: Challenges in Securing the Electricity Grid. GAO-12-926T. Washington, D.C.: July 17, 2012.

Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage. GAO-12-876T. Washington, D.C.: June 28, 2012.

Cybersecurity: Threats Impacting the Nation. GAO-12-666T. Washington, D.C.: April 24, 2012.

Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can be Done to Promote Its Use. GAO-12-92. Washington, D.C. December 9, 2011.

Personnel Security

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

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

Personnel Security Clearances: Further Actions Needed to Improve the Process and Realize Efficiencies. GAO-13-728T. Washington, D.C.: June 20, 2013.

Security Clearances: Agencies Need Clearly Defined Policy for Determining Civilian Position Requirements. GAO-12-800. Washington, D.C.: July 12, 2012.