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.