April 2014

INFORMATION SECURITY

Agencies Need to Improve Cyber Incident Response Practices

GAO Highlights

Highlights of GAO-14-354, a report to congressional requesters

Why GAO Did This Study

The number of cyber incidents reported by federal agencies increased in fiscal year 2013 significantly over the prior 3 years (see figure). An effective response to a cyber incident is essential to minimize any damage that might be caused. DHS and US-CERT have a role in helping agencies detect, report, and respond to cyber incidents.

GAO was asked to review federal agencies' ability to respond to cyber incidents. To do this, GAO reviewed the extent to which (1) federal agencies are effectively responding to cyber incidents and (2) DHS is providing cybersecurity incident assistance to agencies. To do this, GAO used a statistical sample of cyber incidents reported in fiscal year 2012 to project whether 24 major federal agencies demonstrated effective response activities. In addition, GAO evaluated incident response policies, plans, and procedures at 6 randomly-selected federal agencies to determine adherence to federal guidance. GAO also examined DHS and US-CERT policies, procedures, and practices, and surveyed officials from the 24 federal agencies on their experience receiving incident assistance from DHS.

What GAO Recommends

GAO is making recommendations to OMB and DHS to address incident response practices governmentwide, particularly in CyberStat meetings with agencies; to the heads of six agencies to strengthen their incident response policies, plans, and procedures; and to DHS to establish measures of effectiveness for the assistance US-CERT provides to agencies. The agencies generally concurred with GAO's recommendations.

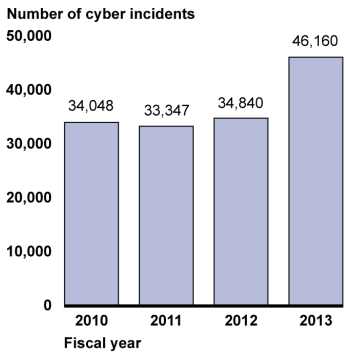
View GAO-14-354. For more information, contact Gregory C.Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Twenty-four major federal agencies did not consistently demonstrate that they are effectively responding to cyber incidents (a security breach of a computerized system and information). Based on a statistical sample of cyber incidents reported in fiscal year 2012, GAO projects that these agencies did not completely document actions taken in response to detected incidents in about 65 percent of cases (with 95 percent confidence that the estimate falls between 58 and 72 percent). For example, agencies identified the scope of an incident in the majority of cases, but frequently did not demonstrate that they had determined the impact of an incident. In addition, agencies did not consistently demonstrate how they had handled other key activities, such as whether preventive actions to prevent the reoccurrence of an incident were taken. Although all 6 selected agencies that GAO reviewed in depth had developed parts of policies, plans, and procedures to guide their incident response activities, their efforts were not comprehensive or fully consistent with federal requirements. In addition, the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) conduct CyberStat reviews, which are intended to help federal agencies improve their information security posture, but the reviews have not addressed agencies' cyber incident response practices. Without complete policies, plans, and procedures, along with appropriate oversight of response activities, agencies face reduced assurance that they can effectively respond to cyber incidents.

DHS and a component, the United States Computer Emergency Readiness Team (US-CERT), offer services that assist agencies in preparing to handle cyber incidents, maintain awareness of the current threat environment, and deal with ongoing incidents. Officials from the 24 agencies GAO surveyed said that they were generally satisfied with the assistance provided, and made suggestions to make the services more useful, such as improving reporting requirements. Although US-CERT receives feedback from agencies to improve its services, it has not yet developed performance measures for evaluating the effectiveness of the assistance it provides to agencies. Without results-oriented performance measures, US-CERT will face challenges in ensuring it is effectively assisting federal agencies with preparing for and responding to cyber incidents.

Cyber Incidents Reported by All Federal Agencies to US-CERT, Fiscal Years 2010-2013



Source: GAO analysis of US-CERT data for fiscal years 2010-2013.