March 2010

INFORMATION SECURITY

Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-237, a report to congressional requesters

Why GAO Did This Study

To reduce the threat to federal systems and operations posed by cyber attacks on the United States, the Office of Management and Budget (OMB) launched, in November 2007, the Trusted Internet Connections (TIC) initiative, and later, in 2008, the Department of Homeland Security's (DHS) National Cybersecurity Protection System (NCPS), operationally known as Einstein, became mandatory for federal agencies as part of TIC. For each of these initiatives, GAO was asked to (1) identify their goals, objectives, and requirements; (2) determine the status of actions federal agencies have taken, or plan to take, to implement the initiatives; and (3) identify any benefits, challenges, and lessons learned. To do this, GAO reviewed plans, reports, and other documents at 23 major executive branch agencies, interviewed officials, and reviewed OMB and DHS guidance.

What GAO Recommends

GAO is making recommendations to OMB to promptly communicate the number of approved connections for agencies, and to DHS aimed at improving communication and performance measures. OMB concurred with GAO's findings, conclusions, and recommendations. DHS concurred with GAO's recommendations and also provided technical comments.

View GAO-10-237 or key components.
For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The goals of TIC are to secure federal agencies' external network connections, including Internet connections, and improve the government's incident response capability by reducing the number of agencies' external network connections and implementing security controls over the connections that remain. In implementing TIC, agencies could either provide their own access points by becoming an access provider or seek service from these providers or an approved vendor. To achieve the initiative's goals, agencies were required to

- inventory external connections,
- establish a target number of TIC access points,
- develop and implement plans to reduce their connections,
- implement security capabilities (if they chose to be an access provider) addressing such issues as encryption and physical security, and
- demonstrate to DHS the consolidation of connections and compliance with the security capabilities (if they chose to be an access provider).

As of September 2009, none of the 23 agencies had met all of the requirements of the TIC initiative. Although most agencies reported that they have made progress toward reducing their external connections and implementing critical security capabilities, most agencies have also experienced delays in their implementation efforts. For example, the 16 agencies that chose to become access providers reported that they had reduced their number of external connections from 3,286 to approximately 1,753. Further, agencies have not demonstrated that they have fully implemented the required security capabilities. Throughout their reduction efforts, agencies have experienced benefits, such as improved security and network management. However, they have been challenged in implementing TIC because OMB did not promptly communicate the number of access points for which they had been approved and DHS did not always respond to agency queries on security capabilities in a timely manner. Agencies' experiences with implementing TIC offered OMB and DHS lessons learned, such as the need to define program requirements before establishing deadlines and the usefulness of sponsoring collaborative meetings for agencies' implementation efforts.

Einstein is intended to provide DHS with an increased awareness of activity, including possible security incidents, on federal networks by providing intrusion detection capabilities that allow DHS to monitor and analyze agencies' incoming and outgoing Internet traffic. As of September 2009, fewer than half of the 23 agencies had executed the required agreements with DHS, and Einstein 2 had been deployed to 6 agencies. Agencies that participated in Einstein 1 improved identification of incidents and mitigation of attacks, but DHS will continue to be challenged in understanding whether the initiative is meeting all of its objectives because it lacks performance measures that address how agencies respond to alerts.