October 2010

CYBERSPACE POLICY

Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-11-24, a report to congressional requesters

Why GAO Did This Study

To address pervasive computer-based (cyber) attacks against the United States that posed potentially devastating impacts to systems and operations, the federal government has developed policies and strategies intended to combat these threats. A recent key development was in February 2009, when President Obama initiated a review of the government's overall strategy and supporting activities with the aim of assessing U.S. policies and structures for cybersecurity. The resulting policy review report—issued by the President in May 2009—provided 24 near- and mid-term recommendations to address these threats.

GAO was asked to assess the implementation status of the 24 recommendations. In doing so, GAO, among other things, analyzed the policy review report and assessed agency documentation and interviewed agency officials.

What GAO Recommends

GAO recommends that the national Cybersecurity Coordinator designates roles and responsibilities and develops milestones and plans for the recommendations that lacked these key planning elements. The Cybersecurity Coordinator's office provided no comments on the conclusions and recommendations in this report; the office did cite recent progress being made on cybersecurity research and development and education that is consistent with GAO's report.

View GAO-11-24 or key components.
For more information, contact David A. Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

Of the 24 recommendations in the President's May 2009 cyber policy review report, 2 have been fully implemented, and 22 have been partially implemented. The two fully implemented recommendations involve appointing within the National Security Council a cybersecurity policy official (Special Assistant to the President and Cybersecurity Coordinator) responsible for coordinating the nation's cybersecurity policies and activities, and a privacy and civil liberties official. Examples of partially implemented recommendations include:

- Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties, leveraging privacy-enhancing technologies for the nation: In June 2010, the administration released a draft strategy (entitled National Strategy for Trusted Identities in Cyberspace) that seeks to increase trust associated with the identities of individuals, organizations, services, and devices involved in financial and other types of online transactions, as well as address privacy and civil liberty issues associated with identity management. It plans to finalize the strategy in October 2010.
- Develop a framework for research and development strategies: The administration's Office of Science and Technology Policy (which is within the Executive Office of the President) has efforts under way to develop a framework for research and development strategies, which as currently envisioned includes three key cybersecurity research and development themes, but is not expected to be finalized until 2011.

Officials from key agencies involved in these cybersecurity efforts, (e.g., the Departments of Defense and Homeland Security and the Office of Management and Budget) attribute the partial implementation status of the 22 recommendations in part to the fact that agencies are moving slowly because they have not been assigned roles and responsibilities with regard to recommendation implementation. Specifically, although the policy review report calls for the cybersecurity policy official to assign roles and responsibilities, agency officials stated they have yet to receive this tasking and attribute this to the fact that the cybersecurity policy official position was vacant for 7 months. In addition, officials stated that several mid-term recommendations are broad in nature, and agencies state they will require action over multiple years before they are fully implemented. This notwithstanding, federal agencies reported they have efforts planned or under way that are aimed toward implementing the 22 partially implemented recommendations. While these efforts appear to be steps forward, agencies were largely not able to provide milestones and plans that showed when and how implementation of the recommendations was to occur. Specifically, 16 of the 22 near- and mid-term recommendations did not have milestones and plans for implementation. Consequently, until roles and responsibilities are made clear and the schedule and planning shortfalls identified above are adequately addressed, there is increased risk the recommendations will not be successfully completed, which would unnecessarily place the country's cyber infrastructure at risk.