March 2010

# CYBERSECURITY

## Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative

GAO Highlights

Accountability • Integrity • Reliability

Highlights of GAO-10-338, a report to congressional requesters

### Why GAO Did This Study

In response to the ongoing threats to federal systems and operations posed by cyber attacks, President Bush established the Comprehensive National Cybersecurity Initiative (CNCI) in 2008. This initiative consists of a set of projects aimed at reducing vulnerabilities, protecting against intrusions, and anticipating future threats. GAO was asked to determine (1) what actions have been taken to develop interagency mechanisms to plan and coordinate CNCI activities and (2) what challenges CNCI faces in achieving its objectives related to securing federal information systems. To do this, GAO reviewed CNCI plans, policies, and other documentation and interviewed officials at the Office of Management and Budget (OMB), Department of Homeland Security, and the Office of the Director of National Intelligence (ODNI), among other agencies. GAO also reviewed studies examining aspects of federal cybersecurity and interviewed recognized cybersecurity experts.

### What GAO Recommends

GAO is recommending that OMB take steps to address each of the identified challenges. OMB agreed with five of six recommendations, disagreeing with the recommendation regarding defining roles and responsibilities. However, such definitions are key to achieving CNCI's objective of securing federal systems.

View GAO-10-338 or key components.
For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or Davi D'Agostino at (202) 512-5431 or dagostinod@gao.gov.

### What GAO Found

The White House and federal agencies have taken steps to plan and coordinate CNCI activities by establishing several interagency working groups. These include the National Cyber Study Group, which carried out initial brainstorming and information-gathering for the establishment of the initiative; the Communications Security and Cyber Policy Coordinating Committee, which presented final plans to the President and coordinated initial implementation activities; and the Joint Interagency Cyber Task Force, which serves as the focal point for monitoring and coordinating projects and enabling the participation of both intelligence-community and non-intelligence-community agencies. These groups have used a combination of status meetings and other reporting mechanisms to track implementation of projects.

CNCI faces several challenges in meeting its objectives:

- **Defining roles and responsibilities.** Federal agencies have overlapping and uncoordinated responsibilities for cybersecurity, and it is unclear where overall responsibility for coordination lies.
- **Establishing measures of effectiveness.** The initiative has not yet developed measures of the effectiveness in meeting its goals. While federal agencies have begun to develop effectiveness measures for information security, these have not been applied to the initiative.
- **Establishing an appropriate level of transparency.** Few of the elements of CNCI have been made public, and the rationale for classifying related information remains unclear, hindering coordination with private sector entities and accountability to the public.
- **Reaching agreement on the scope of educational efforts**. Stakeholders have yet to reach agreement on whether to address broad education and public awareness as part of the initiative, or remain focused on the federal cyber workforce.

Until these challenges are adequately addressed, there is a risk that CNCI will not fully achieve its goal to reduce vulnerabilities, protect against intrusions, and anticipate future threats against federal executive branch information systems.

The federal government also faces strategic challenges beyond the scope of CNCI in securing federal information systems:

- **Coordinating actions with international entities**. The federal government does not have a formal strategy for coordinating outreach to international partners for the purposes of standards setting, law enforcement, and information sharing.
- **Strategically addressing identity management and authentication.** Authenticating the identities of persons or systems seeking to access federal systems remains a significant governmentwide challenge. However, the federal government is still lacking a fully developed plan for implementation of identity management and authentication efforts.