March 7, 2013

CYBERSECURITY

A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges

Highlights of GAO-13-462T, a testimony before the Committee on Commerce, Science, and Transportation, and the Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

Federal government agencies and the nation's critical infrastructures have become increasingly dependent on computerized information systems and electronic data to carry out their operations. While creating significant benefits, this can also introduce vulnerabilities to cyber-threats. Pervasive cyber attacks against the United States could have a serious impact on national security, the economy, and public health and safety. The number of reported cyber incidents has continued to rise, resulting in data theft, economic loss, and privacy breaches. Federal law and policy assign various entities responsibilities for securing federal information systems and protecting critical infrastructures. GAO has designated federal information security as a high-risk area since 1997 and in 2003 expanded this to include cyber critical infrastructure protection.

GAO was asked to testify on its recent report on challenges facing the government in effectively implementing cybersecurity and the extent to which the national cybersecurity strategy includes desirable characteristics of a national strategy. In preparing this statement, GAO relied on the report, as well as related previous work.

What GAO Recommends

In its report, GAO recommended that an integrated national strategy be developed that includes milestones and performance measures; costs and resources; and a clear definition of roles and responsibilities. It also stated that Congress should consider clarifying federal cybersecurity oversight roles through legislation.

What GAO Found

The federal government continues to face challenges in a number of key areas in effectively implementing cybersecurity; these challenge areas include the following, among others:

- **Designing and implementing risk-based cybersecurity programs at federal agencies.** Shortcomings persist in assessing risks, developing and implementing security programs, and monitoring results at federal agencies. This is due in part to the fact that agencies have not fully implemented information security programs, resulting in reduced assurance that controls are in place and operating as intended to protect their information resources.
- **Establishing and identifying standards for critical infrastructures.** Agencies with responsibilities for critical infrastructure have not yet identified cybersecurity guidance widely used in their respective sectors. Moreover, critical infrastructure sectors vary in the extent to which they are required by law or regulation to comply with specific cybersecurity requirements.
- **Detecting, responding to, and mitigating cyber incidents.** Sharing information among federal agencies and key private-sector entities remains a challenge, due to, for example, the lack of a centralized information-sharing system. In addition, the Department of Homeland Security (DHS) has yet to fully develop a capability for predictive analysis of cyber threats.

The federal cybersecurity strategy has evolved over the past decade, with the issuance of several strategy documents and other initiatives that address aspects of these challenge areas. However, there is no overarching national cybersecurity strategy that synthesizes these documents or comprehensively describes the current strategy. In addition, the government's existing strategy documents do not always incorporate key desirable characteristics GAO has identified that can enhance the usefulness of national strategies. Specifically, while existing strategy documents have included elements of these characteristics—such as setting goals and subordinate objectives—they have generally lacked other key elements. These include milestones and performance measures to gauge results; costs of implementing the strategy and sources and types of resources needed; and a clear definition of the roles and responsibilities of federal entities. For example, although federal law assigns the Office of Management and Budget (OMB) responsibility for oversight of federal government information security, OMB recently transferred several of these responsibilities to DHS. This decision may have had practical benefits, such as leveraging additional resources and expertise, but it remains unclear how OMB and DHS are to share oversight of individual departments and agencies. Additional legislation could clarify these responsibilities. Further, without an integrated strategy that includes key characteristics, the federal government will be hindered in making further progress in addressing cybersecurity challenges.

View GAO-13-462T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.