GAO

Accountability·Integrity·Reliability

Highlights

Highlights of GAO-09-835T, a testimony before the Subcommittee on Technology and Innovation, Committee on Science and Technology, House of Representatives

Why GAO Did This Study

Federal laws and policy have assigned important roles and responsibilities to the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) for securing computer networks and systems. DHS is charged with coordinating the protection of computer-reliant critical infrastructure--much of which is owned by the private sector—and securing its own computer systems, while NIST is responsible for developing standards and guidelines for implementing security controls over information and information systems.

GAO was asked to describe cybersecurity efforts at DHS and NIST—including partnership activities with the private sector—and the use of cybersecurity performance metrics in the federal government. To do so, GAO relied on its reports on federal information security and federal efforts to fulfill national cybersecurity responsibilities.

What GAO Recommends

GAO has previously made about 30 recommendations to help DHS fulfill its cybersecurity responsibilities and resolve underlying challenges. In addition, GAO has made about 60 recommendations to strengthen security over information systems supporting DHS's programs for border security and its terrorist watch list. DHS has actions planned and underway to implement them.

View GAO-09-835T or key components.
For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

June 25, 2009

CYBERSECURITY

Continued Federal Efforts Are Needed to Protect Critical Systems and Information

What GAO Found

Since 2005, GAO has reported that DHS has yet to comprehensively satisfy its key cybersecurity responsibilities, including those related to establishing effective partnerships with the private sector. Shortcomings exist in key areas that are essential for DHS to address in order to fully implement its cybersecurity responsibilities (see table). DHS has since developed and implemented certain capabilities, but still has not fully satisfied aspects of these responsibilities and needs to take further action to enhance the public/private partnerships needed to adequately protect cyber critical infrastructure. GAO has also previously reported on significant security weaknesses in systems supporting two of the department's programs, one that tracks foreign nationals entering and exiting the United States, and one for matching airline passenger information against terrorist watch-list records. DHS has corrected information security weaknesses for systems supporting the terrorist watch-list, but needs to take additional actions to mitigate vulnerabilities associated with systems tracking foreign nationals.

Key Cybersecurity Areas Reviewed by GAO

1. Bolstering cyber analysis and warning capabilities
2. Improving cybersecurity of infrastructure control systems
3. Strengthening DHS's ability to help recover from Internet disruptions
4. Reducing organizational inefficiencies
5. Completing actions identified during cyber exercises
6. Developing sector-specific plans that fully address all of the cyber-related criteria
7. Securing internal information systems

Source: GAO.

NIST plays a key role in providing important information security standards and guidance. Pursuant to its responsibilities under the Federal Information Security Management Act (FISMA), NIST has developed standards specifying minimum security requirements for federal information and information systems; and provided corresponding guidance that details the controls necessary for securing those systems. It has also been working with both public and private sector entities to enhance information security requirements. The resulting guidance and tools provided by NIST serve as important resources for federal agencies that can be applied to information security programs.

As GAO recently testified in May, opportunities exist to improve the metrics used to assess agency information security programs. According to the performance metrics established by the Office of Management and Budget (OMB), agencies reported increased compliance in implementing key information security control activities. However, GAO and agency inspectors general continue to report significant weaknesses in controls. This dichotomy exists in part because the OMB-defined metrics generally do not measure how well controls are implemented. As a result, reported metrics may provide an incomplete picture of an agency's information security program.