GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-08-1157T, a report to Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives

September 16, 2008

CRITICAL INFRASTRUCTURE PROTECTION

DHS Needs to Better Address Its Cybersecurity Responsibilities

Why GAO Did This Study

Recent cyber attacks demonstrate the potentially devastating impact these pose to our nation's computer systems and to the federal operations and critical infrastructures that they support. They also highlight that we need to be vigilant against individuals and groups with malicious intent, such as criminals, terrorists, and nation-states perpetuating these attacks. Federal law and policy established the Department of Homeland Security (DHS) as the focal point for coordinating cybersecurity, including making it responsible for protecting systems that support critical infrastructures, a practice commonly referred to as cyber critical infrastructure protection. Since 2005, GAO has reported on the responsibilities and progress DHS has made in its cybersecurity efforts. GAO was asked to summarize its key reports and their associated recommendations aimed at securing our nation's cyber critical infrastructure. To do so, GAO relied on previous reports, as well as two reports being released today, and analyzed information about the status of recommendations.

What GAO Recommends

GAO has previously made about 30 recommendations to help DHS fulfill its cybersecurity responsibilities and resolve underlying challenges. DHS in large part concurred with GAO's recommendations and in many cases has actions planned and underway to implement them.

To view the full product, including the scope and methodology, click on GAO-08-1157T. For more information, contact David A. Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

GAO has reported over the last several years that DHS has yet to fully satisfy its cybersecurity responsibilities. To address these shortfalls, GAO has made about 30 recommendations in the following key areas.

Key Cybersecurity Areas Reviewed by GAO
1. Bolstering cyber analysis and warning capabilities.
2. Reducing organizational inefficiencies.
3. Completing actions identified during cyber exercises.
4. Developing sector-specific plans that fully address all of the cyber-related criteria.
5. Improving cybersecurity of infrastructure control systems (which are computer-based systems that monitor and control sensitive processes and physical functions).
6. Strengthening DHS's ability to help recover from Internet disruptions.

Source: GAO analysis.

Specifically, examples of what GAO reported and recommended are as follows:

- Cyber analysis and warning—In July 2008, GAO reported that DHS's United States Computer Emergency Readiness Team (US-CERT) did not fully address 15 key cyber analysis and warning attributes. For example, US-CERT provided warnings by developing and distributing a wide array of notifications; however, these notifications were not consistently actionable or timely. Consequently, GAO recommended that DHS address these attribute shortfalls.
- Cyber exercises—In September 2008, GAO reported that since conducting a cyber attack exercise in 2006, DHS demonstrated progress in addressing eight lessons it learned from this effort. However, its actions to address the lessons had not been fully implemented. GAO recommended that the department schedule and complete all identified corrective activities.
- Control systems—In a September 2007 report and October 2007 testimony, GAO identified that DHS was sponsoring multiple efforts to improve control system cybersecurity using vulnerability evaluation and response tools. However, the department had not established a strategy to coordinate this and other efforts across federal agencies and the private sector, and it did not effectively share control system vulnerabilities with others. Accordingly, GAO recommended that DHS develop a strategy to guide efforts for securing such systems and establish a process for sharing vulnerability information.

While DHS has developed and implemented capabilities to address aspects of these areas, it still has not fully satisfied any of them. Until these and other areas are effectively addressed, our nation's cyber critical infrastructure is at risk of increasing threats posed by terrorists, nation-states, and others.