July 2005

CRITICAL INFRASTRUCTURE PROTECTION

Challenges in Addressing Cybersecurity

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-05-827T, a Testimony before the Subcommittee on Federal Financial Management, Government Information, and International Security, Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

Increasing computer interconnectivity has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. While the benefits have been enormous, this widespread interconnectivity also poses significant risks to our nation's computer systems and, more importantly, to the critical operations and infrastructures they support. The Homeland Security Act of 2002 and federal policy established the Department of Homeland Security (DHS) as the focal point for coordinating activities to protect the computer systems that support our nation's critical infrastructures. GAO was asked to summarize previous work, focusing on (1) DHS's responsibilities for cybersecurity-related critical infrastructure protection (CIP), (2) the status of the department's efforts to fulfill these responsibilities, (3) the challenges it faces in fulfilling its cybersecurity responsibilities, and (4) recommendations GAO has made to improve cybersecurity of our nation's critical infrastructure.

www.gao.gov/cgi-bin/getrpt?GAO-05-827T.

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

What GAO Found

As the focal point for CIP, the Department of Homeland Security (DHS) has many cybersecurity-related roles and responsibilities that GAO identified in law and policy (see table below for 13 key responsibilities). DHS established the National Cyber Security Division to take the lead in addressing the cybersecurity of critical infrastructures.

While DHS has initiated multiple efforts to fulfill its responsibilities, it has not fully addressed any of the 13 responsibilities, and much work remains ahead. For example, the department established the United States Computer Emergency Readiness Team as a public/private partnership to make cybersecurity a coordinated national effort, and it established forums to build greater trust and information sharing among federal officials with information security responsibilities and law enforcement entities. However, DHS has not yet developed national cyber threat and vulnerability assessments or government/industry contingency recovery plans for cybersecurity, including a plan for recovering key Internet functions.

DHS faces a number of challenges that have impeded its ability to fulfill its cybersecurity-related CIP responsibilities. These key challenges include achieving organizational stability, increasing awareness about cybersecurity roles and capabilities, establishing effective partnerships with stakeholders, and achieving two-way information sharing with these stakeholders. In its strategic plan for cybersecurity, DHS identifies steps that can begin to address the challenges. However, until it confronts and resolves these underlying challenges and implements its plans, DHS will have difficulty achieving significant results in strengthening the cybersecurity of our critical infrastructures. In recent years, GAO has made a series of recommendations to enhance the cybersecurity of critical infrastructures that if effectively implemented could greatly improve our nation's cybersecurity posture.

Table: DHS's Key Cybersecurity Responsibilities

• Develop a national plan for critical infrastructure protection, including cybersecurity. • Develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector. • Improve and enhance public/private information sharing involving cyber attacks, threats, and vulnerabilities. • Develop and enhance national cyber analysis and warning capabilities. • Provide and coordinate incident response and recovery planning efforts.	• Identify and assess cyber threats and vulnerabilities. • Support efforts to reduce cyber threats and vulnerabilities. • Promote and support research and development efforts to strengthen cyberspace security. • Promote awareness and outreach. • Foster training and certification. • Enhance federal, state, and local government cybersecurity. • Strengthen international cyberspace security. • Integrate cybersecurity with national security.

Source: GAO analysis of law and policy.