September 13, 2006

CRITICAL INFRASTRUCTURE PROTECTION

DHS Leadership Needed To Enhance Cybersecurity

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-06-1087T, a testimony before the House Committee on Homeland Security, Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity

Why GAO Did This Study

Increasing computer interconnectivity has revolutionized the way that 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 establish 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 recent reports on (1) DHS's responsibilities for cybersecurity-related critical infrastructure protection and for recovering the Internet in case of a major disruption (2) challenges facing DHS in addressing its cybersecurity responsibilities, including leadership challenges, and (3) recommendations to improve the cybersecurity of national critical infrastructures, including the Internet.

www.gao.gov/cgi-bin/getrpt?GAO-06-1087T.

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

In 2005 and 2006, GAO reported that DHS had initiated efforts to address its responsibilities for enhancing the cybersecurity of critical infrastructures, but that more remained to be done. Specifically, in 2005, GAO reported that DHS had initiated efforts to fulfill 13 key cybersecurity responsibilities, but it had not fully addressed any of them. For example, DHS established forums to foster information sharing among federal officials with information security responsibilities and among various law enforcement entities, but had not developed national threat and vulnerability assessments for cybersecurity. Since that time, DHS has made progress on its 13 key responsibilities—including the release of its *National Infrastructure Protection Plan*—but none have been completely addressed. Moreover, in 2006, GAO reported that DHS had begun a variety of initiatives to fulfill its responsibility to develop an integrated public/private plan for Internet recovery, but these efforts were not complete or comprehensive. For example, DHS established working groups to facilitate coordination among government and industry infrastructure officials and fostered exercises in which government and private industry could practice responding to cyber events, but many of its efforts lacked timeframes for completion and the relationships among its various initiatives were not evident.

DHS faces a number of challenges that have impeded its ability to fulfill its cybersecurity responsibilities, including establishing effective partnerships with stakeholders, demonstrating the value it can provide to private sector infrastructure owners, and reaching consensus on DHS's role in Internet recovery and on when the department should get involved in responding to an Internet disruption. DHS faces a particular challenge in attaining the organizational stability and leadership it needs to gain the trust of other stakeholders in the cybersecurity world—including other government agencies as well as the private sector. In May 2005, we reported that multiple senior DHS cybersecurity officials had recently left the department. In July 2005, DHS undertook a reorganization which established the position of the Assistant Secretary of Cyber Security and Telecommunications—in part to raise the visibility of cybersecurity issues in the department. However, over a year later, this position remains vacant.

To strengthen DHS's ability to implement its cybersecurity responsibilities and to resolve underlying challenges, GAO has made about 25 recommendations over the last several years. These recommendations focus on the need to (1) conduct threat and vulnerability assessments, (2) develop a strategic analysis and warning capability for identifying potential cyber attacks, (3) protect infrastructure control systems, (4) enhance public/private information sharing, and (5) facilitate recovery planning, including recovery of the Internet in case of a major disruption. These recommendations provide a high-level road map for DHS to use to help improve our nation's cybersecurity posture. Until they are addressed, DHS will have difficulty achieving results as the federal cybersecurity focal point.