March 20, 2007

CRITICAL INFRASTRUCTURE:

Challenges Remain in Protecting Key Sectors

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-626T, a testimony before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives

Why GAO Did This Study

As Hurricane Katrina so forcefully demonstrated, the nation's critical infrastructures—both physical and cyber—have been vulnerable to a wide variety of threats. Because about 85 percent of the nation's critical infrastructure is owned by the private sector, it is vital that the public and private sectors work together to protect these assets. The Department of Homeland Security (DHS) is responsible for coordinating a national protection strategy including formation of government and private sector councils as a collaborating tool. The councils, among other things, are to identify their most critical assets, assess the risks they face, and identify protective measures, in sector-specific plans that comply with DHS's National Infrastructure Protection Plan (NIPP). This testimony is based primarily on GAO's October 2006 sector council report and a body of work on cyber critical infrastructure protection. Specifically, it addresses (1) the extent to which these councils have been established, (2) key facilitating factors and challenges affecting the formation of the council, (3) key facilitating factors and challenges encountered in developing sector plans, and (4) the status of DHS's efforts to fulfill key cybersecurity responsibilities.

GAO has made previous recommendations, particularly in the area of cybersecurity that have not been fully implemented. Continued monitoring will determine whether further recommendations are warranted.

www.gao.gov/cgi-bin/getrpt?GAO-07-626T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Eileen Larence at (202) 512-8777 or larencee@gao.gov.

What GAO Found

To better coordinate infrastructure protection efforts as called for in the NIPP, all 17 critical infrastructure sectors have established their respective government councils, and nearly all sectors have initiated their voluntary private sector councils. But council progress has varied due to their characteristics and level of maturity. For example, the public health and healthcare sector is quite diverse and collaboration has been difficult as a result; on the other hand, the nuclear sector is quite homogenous and has a long history of collaboration. As a result, council activities have ranged from getting organized to refining infrastructure protection strategies. Ten sectors, such as banking and finance, had formed councils prior to development of the NIPP and had collaborated on plans for economic reasons, while others had formed councils more recently. As a result, the more mature councils could focus on strategic issues, such as recovering after disasters, while the newer councils were focusing on getting organized.

Council members reported mixed views on what factors facilitated or challenged their actions. For example, long-standing working relationships with regulatory agencies and within sectors were frequently cited as the most helpful factor. Challenges most frequently cited included the lack of an effective relationship with DHS as well as private sector hesitancy to share information on vulnerabilities with the government or within the sector for fear the information would be released and open to competitors. GAO's past work has shown that a lack of trust in DHS and fear that sensitive information would be released are recurring barriers to the private sector's sharing information with the federal government, and GAO has made recommendations to help address these barriers. DHS has generally concurred with these recommendations and is in the process of implementing them.

All the sectors met the December 2006 deadline to submit their sector-specific plans to DHS, although the level of collaboration between the sector and government councils on the plans, which the NIPP recognizes as critical to establishing relationships between the government and private sectors, varied by sector. Issuing the NIPP and completing sector plans are only first steps to ensure critical infrastructure is protected. Moving forward to implement sector plans and make progress will require continued commitment and oversight.

While DHS has initiatives under way to fulfill its many cybersecurity responsibilities, major tasks remain to be done. These include assessing and reducing cyber threats and vulnerabilities and coordinating incident response and recovery planning efforts. Effective leadership by the Assistant Secretary for Cyber Security and Telecommunications is essential to DHS fulfilling its key responsibilities, addressing the challenges, and implementing recommendations.