GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-06-383, a report to congressional requesters

Why GAO Did This Study

A wide array of cyber and physical assets is critical to America's national security, economic well-being, and public health and safety. Information related to threats, vulnerabilities, incidents, and security techniques is instrumental to guarding these critical infrastructures against attacks and mitigating the impact of attacks that may occur. The ability to share security-related information can unify the efforts of federal, state, and local government as well as the private sector, as appropriate, in preventing and minimizing terrorist attacks. The Critical Infrastructure Information Act of 2002 was enacted to encourage nonfederal entities to voluntarily share critical infrastructure information and established protections for it. The Department of Homeland Security (DHS) has a lead role in implementing the act. GAO was asked to determine (1) the status of DHS's efforts to implement the act and (2) the challenges it faces in carrying out the act.

What GAO Recommends

GAO is recommending that the Secretary of Homeland Security, among other things, better define DHS's and other federal agencies' critical infrastructure information needs, and explain how DHS and the other agencies will use the information received from the private sector. In oral comments on a draft of this report, DHS concurred with our findings and recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-06-383.

To view the full product, including the scope and methodology, click on the link above.
For more information, contact Dave Powner at 202-512-9286, Pownerd@gao.gov or Eileen Larence at 202-512-6510, Larencee@gao.gov.

April 2006

INFORMATION SHARING

DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information

What GAO Found

DHS has issued interim operating procedures and created a Program Office to administer the critical infrastructure protection program called for by the Critical Infrastructure Information Act. The interim procedures designate the responsibilities and authority of the Program Manager, and establish requirements related to accepting, protecting, sharing, and using critical infrastructure information as required by the act. The Program Office has begun to accept and safeguard critical infrastructure information submitted voluntarily by infrastructure owners and is sharing it with other DHS entities and, on a limited basis, with other government entities. For example, as of January 2006, the Program Office had received about 290 submissions of critical infrastructure information from various sectors. The Program Office also has initiated outreach efforts to publicize the program to the public and private sectors. In addition, it has trained approximately 750 potential users in DHS and other federal, state, and local government entities how to handle protected critical infrastructure information. This training is a prerequisite to being allowed to view the information. The Program Office has also trained at least 16 federal and state officials how to establish programs in their own entities so they can receive protected critical infrastructure information from DHS and then be authorized to store and share it.

DHS faces challenges that impede the private sector's willingness to share sensitive information. Key challenges include

- defining specific government needs for critical infrastructure information,
- determining how the information will be used,
- assuring the private sector that the information will be protected and who will be authorized to have access to the information, and
- demonstrating to critical infrastructure owners the benefits of sharing the information.

If DHS were able to surmount these challenges, it and other government users may begin to overcome the lack of trust that critical infrastructure owners have in the government's ability to use and protect their sensitive information.