



Highlights of [GAO-04-780](#), a report to congressional requesters

CRITICAL INFRASTRUCTURE PROTECTION

Improving Information Sharing with Infrastructure Sectors

Why GAO Did This Study

Critical infrastructure protection (CIP) activities called for in federal policy and law are intended to enhance the security of the public and private infrastructures that are essential to our nation's security, economic security, and public health and safety. Effective information-sharing partnerships between industry sectors and government can contribute to CIP efforts.

Federal policy has encouraged the voluntary creation of information sharing and analysis centers (ISAC) to facilitate infrastructure sector participation in CIP information sharing efforts. GAO was asked to identify actions that the Department of Homeland Security (DHS) could take to improve the effectiveness of CIP information-sharing efforts.

What GAO Recommends

GAO recommends that the Secretary of Homeland Security direct officials within DHS to (1) proceed with the development of an information-sharing plan that describes the roles and responsibilities of DHS, the ISACs, and other entities and (2) establish appropriate department policies and procedures for interactions with other CIP entities and for coordination and information sharing among DHS components. DHS commented on a draft of this report and generally agreed with our findings and recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-04-780.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at 202-512-3317 or Daceyr@gao.gov.

What GAO Found

Federal awareness of the importance of securing the nation's critical infrastructures—and the federal government's strategy to encourage cooperative efforts among state and local governments and the private sector to protect these infrastructures—have been evolving since the mid-1990s. Federal policy continues to emphasize the importance of the ISACs and their information-sharing functions. In addition, federal policy established specific responsibilities for DHS and other federal agencies involved with the CIP sectors. The ISACs have identified challenges requiring further federal action, including building trusted relationships; developing processes to facilitate information sharing; overcoming barriers to information sharing; clarifying the roles and responsibilities of the various government and private-sector entities that are involved in protecting critical infrastructures; and funding ISAC operations and activities.

Although DHS has taken a number of actions to implement the public/private partnership called for by federal CIP policy, it has not yet developed a plan that describes how it will carry out its information-sharing responsibilities and relationships. Such a plan could encourage improved information sharing among the ISACs, other CIP entities, and the department by clarifying the roles and responsibilities of all the entities involved and clearly articulating actions to address the challenges that remain. DHS officials indicated that they intend to develop an information-sharing plan, but no specific time frame for completing the plan has been established.

The department also lacks policies and procedures to ensure effective coordination and sharing of ISAC-provided information among the appropriate components within the department. Developing policies and procedures would help ensure that information is effectively and efficiently shared among its components and with other government and private-sector CIP entities.