July 2010

CRITICAL INFRASTRUCTURE PROTECTION

Key Private and Public Cyber Expectations Need to Be Consistently Addressed

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-628, a report to congressional requesters

Why GAO Did This Study

Pervasive and sustained computer-based attacks pose a potentially devastating impact to systems and operations and the critical infrastructures they support. Addressing these threats depends on effective partnerships between the government and private sector owners and operators of critical infrastructure. Federal policy, including the Department of Homeland Security's (DHS) National Infrastructure Protection Plan, calls for a partnership model that includes public and private councils to coordinate policy and information sharing and analysis centers to gather and disseminate information on threats to physical and cyber-related infrastructure. GAO was asked to determine (1) private sector stakeholders' expectations for cyber-related, public-private partnerships and to what extent these expectations are being met and (2) public sector stakeholders' expectations for cyber-related, public-private partnerships and to what extent these expectations are being met. To do this, GAO conducted surveys and interviews of public and private sector officials and analyzed relevant policies and other documents.

What GAO Recommends

GAO recommends that the national Cybersecurity Coordinator and DHS work with their federal and private sector partners to enhance information-sharing efforts. The national Cybersecurity Coordinator provided no comments on a draft of this report. DHS concurred with GAO's recommendations.

View GAO-10-628 or key components.
For more information, contact David A. Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

Private sector stakeholders reported that they expect their federal partners to provide usable, timely, and actionable cyber threat information and alerts; access to sensitive or classified information; a secure mechanism for sharing information; security clearances; and a single centralized government cybersecurity organization to coordinate government efforts. However, according to private sector stakeholders, federal partners are not consistently meeting these expectations. For example, less than one-third of private sector respondents reported that they were receiving actionable cyber threat information and alerts to a great or moderate extent. (See table below.) Federal partners are taking steps that may address the key expectations of the private sector, including developing new information-sharing arrangements. However, while the ongoing efforts may address the public sector's ability to meet the private sector's expectations, much work remains to fully implement improved information sharing.

Private Sector Expected Services and the Extent to Which They Are Met

Services	Greatly or moderately expected	Greatly or moderately received
Timely and actionable cyber threat information	98%	27%
Timely and actionable cyber alerts	96%	27%
Access to actionable classified or sensitive information (such as intelligence and law enforcement information)	87%	16%
A secure information-sharing mechanism	78%	21%

Source: GAO analysis based on survey data of 56 private sector respondents.

Public sector stakeholders reported that they expect the private sector to provide a commitment to execute plans and recommendations, timely and actionable cyber threat information and alerts, and appropriate staff and resources. Four of the five public sector councils that GAO held structured interviews with reported that their respective private sector partners are committed to executing plans and recommendations and providing timely and actionable information. However, public sector council officials stated that improvements could be made to the partnership, including improving private sector sharing of sensitive information. Some private sector stakeholders do not want to share their proprietary information with the federal government for fear of public disclosure and potential loss of market share, among other reasons.

Without improvements in meeting private and public sector expectations, the partnerships will remain less than optimal, and there is a risk that owners of critical infrastructure will not have the information necessary to thwart cyber attacks that could have catastrophic effects on our nation's cyber-reliant critical infrastructure.