December 2011

CRITICAL INFRASTRUCTURE PROTECTION

Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-92, a report to congressional requesters

Why GAO Did This Study

Critical infrastructures are systems and assets critical to the nation's security, economy, and public health and safety, most of which are owned by the private sector. These assets rely on networked computers and systems, thus making them susceptible to cyber-based risks. Managing such risk involves the use of cybersecurity guidance that promotes or requires actions to enhance the confidentiality, integrity, and availability of computer systems.

For seven critical infrastructure sectors, GAO was asked to identify (1) cybersecurity guidance for entities within the sectors, (2) the extent to which implementation of this guidance is enforced and promoted, and (3) areas of commonalities and differences between sector cybersecurity guidance and guidance applicable to federal agencies. To do this, GAO collected and analyzed information from responsible private sector coordinating councils; federal agencies, including sector-specific agencies that are responsible for coordinating critical infrastructure protection efforts; and standards-making bodies. In addition, GAO compared a set of guidance in each of three subsectors with guidance applicable to federal agencies.

What GAO Recommends

GAO is recommending that the Department of Homeland Security (DHS), in collaboration with public and private sector partners, determine whether it is appropriate to have cybersecurity guidance listed in sector plans. DHS concurred with GAO's recommendation.

View GAO-12-92. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

A wide variety of cybersecurity guidance is available from national and international organizations for entities within the seven critical infrastructure sectors GAO reviewed—banking and finance; communications; energy; health care and public health; information technology; nuclear reactors, material, and waste; and water. Much of this guidance is tailored to business needs of entities or provides methods to address unique risks or operations. In addition, entities operating in regulated environments are subject to mandatory standards to meet their regulatory requirements; entities operating outside of a regulatory environment may voluntarily adopt standards and guidance. While private sector coordinating council representatives confirmed lists of cybersecurity guidance that they stated were used within their respective sectors, the representatives emphasized that the lists were not comprehensive and that additional standards and guidance are likely used.

Implementation of cybersecurity guidance can occur through a variety of mechanisms, including enforcement of regulations and voluntarily in response to business incentives; however, sector-specific agencies could take additional steps to promote the most applicable and effective guidance throughout the sectors. A number of subsectors within the sectors included in GAO's review, such as electricity in the energy sector, are required to meet mandatory cybersecurity standards established by regulation under federal law or face enforcement mechanisms, such as civil monetary penalties. By contrast, entities not subject to regulation may voluntarily implement cybersecurity guidance to, among other things, reduce risk, protect intellectual property, and meet customer expectations. Federal policy establishes the dissemination and promotion of cybersecurity-related standards and guidance as a goal to enhancing the security of our nation's cyber-reliant critical infrastructure. DHS and the other lead agencies for the sectors selected for review have disseminated and promoted cybersecurity guidance among and within sectors. However, DHS and the other sector-specific agencies have not identified the key cybersecurity guidance applicable to or widely used in each of their respective critical infrastructure sectors. In addition, most of the sector-specific critical infrastructure protection plans for the sectors reviewed do not identify key guidance and standards for cybersecurity because doing so was not specifically suggested by DHS guidance. Given the plethora of guidance available, individual entities within the sectors may be challenged in identifying the guidance that is most applicable and effective in improving their security posture. Improved knowledge of the guidance that is available could help both federal and private sector decision makers better coordinate their efforts to protect critical cyber-reliant assets.

Sector cybersecurity guidance that GAO compared in three subsectors within the banking and finance, energy, and nuclear sectors is substantially similar to guidance applicable to federal agencies. Specifically, one set of guidance for each subsector, along with supplementary documents, addressed most risk management steps and most recommended security controls that are specified for federal information systems in guidance from the Commerce Department's National Institute of Standards and Technology.