GAO
Accountability * Integrity * Reliability
Highlights

Highlights of GAO-11-865T, a testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

July 26, 2011

CYBERSECURITY

Continued Attention Needed to Protect Our Nation's Critical Infrastructure

Why GAO Did This Study

Increasing computer interconnectivity, such as the growth of the Internet, has revolutionized the way our government, our nation, and much of the world communicate and conduct business. However, this widespread interconnectivity poses significant risks to the government's and the nation's computer systems, and to the critical infrastructures they support. These critical infrastructures include systems and assets—both physical and virtual—that are essential to the nation's security, economic prosperity, and public health, such as financial institutions, telecommunications networks, and energy production and transmission facilities. Because most of these infrastructures are owned by the private sector, establishing effective public-private partnerships is essential to securing them from pervasive cyber-based threats. Federal law and policy call for federal entities, such as the Department of Homeland Security (DHS), to work with private-sector partners to enhance the physical and cyber security of these critical infrastructures.

GAO is providing a statement describing (1) cyber threats facing cyber-reliant critical infrastructures; (2) recent actions the federal government has taken, in partnership with the private sector, to identify and protect cyber-reliant critical infrastructures; and (3) ongoing challenges to protecting these infrastructures. In preparing this statement, GAO relied on its previously published work in the area.

View GAO-11-865T or key components.
For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The threats to systems supporting critical infrastructures are evolving and growing. In a February 2011 testimony, the Director of National Intelligence noted that there has been a dramatic increase in cyber activity targeting U.S. computers and systems in the last year, including a more than tripling of the volume of malicious software since 2009. Varying types of threats from numerous sources can adversely affect computers, software, networks, organizations, entire industries, or the Internet itself. These include both unintentional and intentional threats, and may come in the form of targeted or untargeted attacks from criminal groups, hackers, disgruntled employees, hostile nations, or terrorists. The interconnectivity between information systems, the Internet, and other infrastructures can amplify the impact of these threats, potentially affecting the operations of critical infrastructure, the security of sensitive information, and the flow of commerce. Recent reported incidents include hackers accessing the personal information of hundreds of thousands of customers of a major U.S. bank and a sophisticated computer attack targeting control systems used to operate industrial processes in the energy, nuclear, and other critical sectors.

Over the past 2 years, the federal government, in partnership with the private sector, has taken a number of steps to address threats to cyber critical infrastructure. In early 2009, the White House conducted a review of the nation's cyberspace policy that addressed the missions and activities associated with the nation's information and communications infrastructure. The results of the review led, among other things, to the appointment of a national Cybersecurity Coordinator with responsibility for coordinating the nation's cybersecurity policies and activities. Also in 2009, DHS updated its National Infrastructure Protection Plan, which provides a framework for addressing threats to critical infrastructures and relies on a public-private partnership model for carrying out these efforts. DHS has also established a communications center to coordinate national response efforts to cyber attacks and work directly with other levels of government and the private sector and has conducted several cyber attack simulation exercises.

Despite recent actions taken, a number of significant challenges remain to enhancing the security of cyber-reliant critical infrastructures, such as

- implementing actions recommended by the president's cybersecurity policy review;
- updating the national strategy for securing the information and communications infrastructure;
- reassessing DHS's planning approach to critical infrastructure protection;
- strengthening public-private partnerships, particularly for information sharing;
- enhancing the national capability for cyber warning and analysis;
- addressing global aspects of cybersecurity and governance; and
- securing the modernized electricity grid, referred to as the "smart grid."

In prior reports, GAO has made many recommendations to address these challenges. GAO also continues to identify protecting the nation's cyber critical infrastructure as a governmentwide high-risk area.