March 16, 2011

CYBERSECURITY

Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-11-463T, a testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Pervasive and sustained cyber attacks continue to pose a potentially devastating threat to the systems and operations of our nation's critical infrastructure and the federal government. In recent testimony, the Director of National Intelligence stated that there had been a dramatic increase in malicious cyber activity targeting U.S. computers and networks. In addition, recent reports of cyber attacks and incidents affecting federal systems and critical infrastructures illustrate the potential impact of such events on national and economic security. The nation's ever-increasing dependence on information systems to carry out essential everyday operations makes it vulnerable to an array of cyber-based risks. Thus it is increasingly important that federal and nonfederal entities carry out concerted efforts to safeguard their systems and the information they contain.

GAO is providing a statement describing (1) cyber threats to cyber-reliant critical infrastructures and federal information systems and (2) the continuing challenges facing federal agencies in protecting the nation's cyber-reliant critical infrastructure and federal systems. In preparing this statement, GAO relied on its previously published work in the area, which included many recommendations for improvements.

View GAO-11-463T or key components. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Cyber-based threats to critical infrastructure and federal systems are evolving and growing. These threats can come from a variety of sources, including criminals and foreign nations, as well as hackers and disgruntled employees. These potential attackers have a variety of techniques at their disposal that can vastly expand the reach and impact of their actions. In addition, the interconnectivity between information systems, the Internet, and other infrastructure presents increasing opportunities for such attacks. Consistent with this, reports of security incidents from federal agencies are on the rise, increasing over 650 percent over the past 5 years. In addition, reports of cyber attacks and information security incidents affecting federal systems and systems supporting critical infrastructure illustrate the serious impact such incidents can have on national and economic security, including the loss of classified information and intellectual property worth millions of dollars.

The administration and executive branch agencies continue to act to better protect cyber-reliant critical infrastructures, improve the security of federal systems, and strengthen the nation's cybersecurity posture. However, they have not yet fully implemented key actions that are intended to address threats and improve the current U.S. approach to cybersecurity, such as

- implementing near- and mid-term actions recommended by the cybersecurity policy review directed by the president;
- updating the national strategy for securing the information and communications infrastructure;
- developing a comprehensive national strategy for addressing global cybersecurity and governance; and
- creating a prioritized national and federal research and development agenda for improving cybersecurity.

Federal systems continue to be afflicted by persistent information security control weaknesses. For example, as part of its audit of the fiscal year 2010 financial statements for the U.S. government, GAO determined that serious and widespread information security control deficiencies were a governmentwide material weakness. Over the past several years, GAO and agency inspectors general have made hundreds of recommendations to agencies for actions necessary to resolve prior significant control deficiencies and information security program shortfalls. The White House, the Office of Management and Budget, and selected federal agencies have undertaken additional governmentwide initiatives intended to enhance information security at federal agencies. However, these initiatives face challenges, such as better defining agency roles and responsibilities and establishing measures of effectiveness, and require sustained attention, which agencies have begun to provide.

As such, GAO continues to identify protecting the federal government's information systems and the nation's cyber critical infrastructure as a governmentwide high-risk area.