April 24, 2012

CYBERSECURITY

Threats Impacting the Nation

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-666T, a testimony before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Nearly every aspect of American society increasingly depends upon information technology systems and networks. This includes increasing computer interconnectivity, particularly through the widespread use of the Internet as a medium of communication and commerce. While providing significant benefits, this increased interconnectivity can also create vulnerabilities to cyber-based threats. Pervasive and sustained cyber attacks against the United States could have a potentially devastating impact on federal and nonfederal systems, disrupting the operations of governments and businesses and the lives of private individuals. Accordingly, GAO has designated federal information security as a governmentwide high-risk area since 1997, and in 2003 expanded it to include protecting systems and assets vital to the nation (referred to as critical infrastructures).

GAO is providing a statement that describes (1) cyber threats facing the nation's systems, (2) vulnerabilities present in federal information systems and systems supporting critical infrastructure, and (3) reported cyber incidents and their impacts. In preparing this statement, GAO relied on previously published work in these areas and reviewed more recent GAO, agency, and inspectors general work, as well as reports on security incidents.

What GAO Recommends

GAO has previously made recommendations to resolve identified significant control deficiencies.

View GAO-12-666T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The nation faces an evolving array of cyber-based threats arising from a variety of sources. These threats can be intentional or unintentional. Unintentional threats can be caused by software upgrades or defective equipment that inadvertently disrupt systems, and intentional threats can be both targeted and untargeted attacks from a variety of threat sources. Sources of threats include criminal groups, hackers, terrorists, organization insiders, and foreign nations engaged in crime, political activism, or espionage and information warfare. These threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary gain or political advantage, among others. Moreover, potential threat actors have a variety of attack techniques at their disposal, which can adversely affect computers, software, a network, an organization's operation, an industry, or the Internet itself. The nature of cyber attacks can vastly enhance their reach and impact due to the fact that attackers do not need to be physically close to their victims and can more easily remain anonymous, among other things. The magnitude of the threat is compounded by the ever-increasing sophistication of cyber attack techniques, such as attacks that may combine multiple techniques. Using these techniques, threat actors may target individuals, businesses, critical infrastructures, or government organizations.

The threat posed by cyber attacks is heightened by vulnerabilities in federal systems and systems supporting critical infrastructure. Specifically, significant weaknesses in information security controls continue to threaten the confidentiality, integrity, and availability of critical information and information systems supporting the operations, assets, and personnel of federal government agencies. For example, 18 of 24 major federal agencies have reported inadequate information security controls for financial reporting for fiscal year 2011, and inspectors general at 22 of these agencies identified information security as a major management challenge for their agency. Moreover, GAO, agency, and inspector general assessments of information security controls during fiscal year 2011 revealed that most major agencies had weaknesses in most major categories of information system controls. In addition, GAO has identified vulnerabilities in systems that monitor and control sensitive processes and physical functions supporting the nation's critical infrastructures. These and similar weaknesses can be exploited by threat actors, with potentially severe effects.

The number of cybersecurity incidents reported by federal agencies continues to rise, and recent incidents illustrate that these pose serious risk. Over the past 6 years, the number of incidents reported by federal agencies to the federal information security incident center has increased by nearly 680 percent. These incidents include unauthorized access to systems; improper use of computing resources; and the installation of malicious software, among others. Reported attacks and unintentional incidents involving federal, private, and infrastructure systems demonstrate that the impact of a serious attack could be significant, including loss of personal or sensitive information, disruption or destruction of critical infrastructure, and damage to national and economic security.