June 16, 2010

CYBERSECURITY

Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-834T, a testimony before the 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 the federal government. In recent testimony, the Director of National Intelligence highlighted that many nation states, terrorist networks, and organized criminal groups have the capability to target elements of the United States information infrastructure for intelligence collection, intellectual property theft, or disruption. In July 2009, press accounts reported attacks on Web sites operated by major government agencies. The ever-increasing dependence of federal agencies on information systems to carry out essential, everyday operations can make them vulnerable to an array of cyber-based risks. Thus it is increasingly important that the federal government carry out a concerted effort to safeguard its systems and the information they contain.

GAO is providing a statement describing (1) cyber threats to federal information systems and cyber-based critical infrastructures, (2) control deficiencies that make federal systems vulnerable to those threats, and (3) opportunities that exist for improving federal cybersecurity. In preparing this statement, GAO relied on its previously published work in this area.

View GAO-10-834T 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 federal systems and critical infrastructure 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, which can vastly enhance the reach and impact of their actions. For example, cyber attackers do not need to be physically close to their targets, their attacks can easily cross state and national borders, and cyber attackers can easily preserve their anonymity. Further, 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 by over 400 percent from fiscal year 2006 to fiscal year 2009.

Compounding the growing number and kinds of threats, GAO—along with agencies' internal assessments—has identified significant deficiencies in the security controls on federal information systems, which have resulted in pervasive vulnerabilities. These include weaknesses in the security of both financial and non-financial systems and information, including vulnerabilities in critical federal systems. These deficiencies continue to place federal assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, and critical operations at risk of disruption.

Multiple opportunities exist to improve federal cybersecurity. To address identified deficiencies in agencies' security controls and shortfalls in their information security programs, GAO and agency inspectors general have made hundreds of recommendations over the past several years, many of which agencies are implementing. In addition, the White House, the Office of Management and Budget, and certain federal agencies have undertaken several governmentwide initiatives intended to enhance information security at federal agencies. While progress has been made on these initiatives, they all face challenges that require sustained attention, and GAO has made several recommendations for improving the implementation and effectiveness of these initiatives. Further, the Department of Homeland Security also needs to fulfill its key cybersecurity responsibilities, such as developing capabilities for ensuring the protection of cyber-based critical infrastructures and implementing lessons learned from a major cyber simulation exercise. Finally, a GAO-convened panel of experts has made several recommendations for improving the nation's cybersecurity strategy. Realizing these opportunities for improvement can help ensure that the federal government's systems, information, and critical cyber-based infrastructures are effectively protected.