November 17, 2009

CYBERSECURITY

Continued Efforts Are Needed to Protect Information Systems from Evolving Threats

GAO Accountability•Integrity•Reliability

Highlights

Highlights of GAO-10-230T, a statement to the Subcommittee on Terrorism and Homeland Security, Committee on the Judiciary, U.S. Senate

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 months, federal officials have cited the continued efforts of foreign nations and criminals to target government and private sector networks; terrorist groups have expressed a desire to use cyber attacks to target the United States; and press accounts have reported attacks on the Web sites of government agencies. The ever-increasing dependence of federal agencies on computerized systems to carry out essential, everyday operations can make them vulnerable to an array of cyber-based risks. Thus it is increasingly important for the federal government to have effective information security controls in place to safeguard its systems and the information they contain.

GAO was asked to provide a statement describing (1) cyber threats to federal information systems and cyber-based critical infrastructures, (2) control deficiencies at federal agencies that make these systems and infrastructures vulnerable to cyber 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-10-230T or key components. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or David A. Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

Cyber-based threats to federal systems and critical infrastructure are evolving and growing. These threats can be unintentional or intentional, targeted or non-targeted, and can come from a variety of sources, including criminals, terrorists, and adversarial 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 more easily preserve their anonymity. Further, the growing interconnectivity between information systems, the Internet, and other infrastructure presents increasing opportunities for such attacks. In addition, reports of security incidents from federal agencies are on the rise, increasing by over 200 percent from fiscal year 2006 to fiscal year 2008.

Compounding the growing number and kinds of threats, GAO—along with agencies and their inspectors general—has identified significant weaknesses in the security controls on federal information systems, resulting in pervasive vulnerabilities. These include deficiencies in the security of financial systems and information and vulnerabilities in other critical federal information systems. GAO has identified weaknesses in all major categories of information security controls at federal agencies. For example, in fiscal year 2008, weaknesses were reported in such controls at 23 of 24 major agencies. Specifically, agencies did not consistently authenticate users to prevent unauthorized access to systems; apply encryption to protect sensitive data; and log, audit, and monitor security-relevant events, among other actions. An underlying cause of these weaknesses is agencies' failure to fully or effectively implement information security programs, which entails assessing and managing risk, developing and implementing security policies and procedures, promoting security awareness and training, monitoring the adequacy of security controls, and implementing appropriate remedial actions.

Multiple opportunities exist to enhance cybersecurity. In light of weaknesses in agencies' information security controls, GAO and inspectors general have made hundreds of recommendations to improve security, many of which agencies are implementing. In addition, the White House and the Office of Management and Budget, collaborating with other agencies, have launched several initiatives aimed at improving aspects of federal cybersecurity. The Department of Homeland Security, which plays a key role in coordinating cybersecurity activities, also needs to fulfill its responsibilities, such as developing capabilities for protecting cyber-reliant critical infrastructures and implementing lessons learned from a major cyber simulation exercise. Finally, a panel of experts convened by GAO 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-reliant infrastructure are effectively protected.