GAO

Highlights

Highlights of GAO-15-573T, a testimony before the Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

Federal agencies, as well as their contractors, depend on interconnected computer systems and electronic data to carry out essential mission-related functions. Thus, the security of these systems and networks is vital to protecting national and economic security, public health and safety, and the flow of commerce. If information security controls are ineffective, resources may be lost, information—including sensitive personal information—may be compromised, and the operations of government and critical infrastructure could be disrupted, with potentially catastrophic effects. Federal law sets forth various requirements, roles, and responsibilities for securing federal agencies' systems and information. In addition, GAO has designated federal information security as a high-risk area since 1997.

GAO was asked to provide a statement summarizing cyber threats facing federal agency and contractor systems, and challenges in securing these systems. In preparing this statement, GAO relied on its previously published work in this area.

What GAO Recommends

In its previous work, GAO has made numerous recommendations to agencies to assist in addressing the identified cybersecurity challenges.

View GAO-15-573T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

April 22, 2015

CYBERSECURITY

Actions Needed to Address Challenges Facing Federal Systems

What GAO Found

Federal and contractor systems face an evolving array of cyber-based threats. These threats can be unintentional—for example, from equipment failure, careless or poorly trained employees; or intentional—targeted or untargeted attacks from criminals, hackers, adversarial nations, or terrorists, among others. Threat actors use a variety of attack techniques that can adversely affect federal information, computers, software, networks, or operations, potentially resulting in the disclosure, alteration, or loss of sensitive information; destruction or disruption of critical systems; or damage to economic and national security. These concerns are further highlighted by the sharp increase in cyber incidents reported by federal agencies over the last several years, as well as the reported impact of such incidents on government and contractor systems.

Because of the risk posed by these threats, it is crucial that the federal government take appropriate steps to secure its information and information systems. However, GAO has identified a number of challenges facing the government's approach to cybersecurity, including the following:

- **Implementing risk-based cybersecurity programs at federal agencies:** For fiscal year 2014, 19 of 24 major federal agencies reported that deficiencies in information security controls constituted either a material weakness or significant deficiency in internal controls over their financial reporting. In addition, inspectors general at 23 of these agencies cited information security as a major management challenge for their agency.
- **Securing building and access control systems:** GAO previously reported that the Department of Homeland Security lacked a strategy for addressing cyber risks to agencies' building and access control systems—computers that monitor and control building operations—and that the General Services Administration had not fully assessed the risk of cyber attacks to such systems.
- **Overseeing contractors:** The agencies GAO reviewed were inconsistent in overseeing contractors' implementation of security controls for systems they operate on behalf of agencies.
- **Improving incident response:** The agencies GAO reviewed did not always effectively respond to cybersecurity incidents or develop comprehensive policies, plans, and procedures to guide incident-response activities.
- **Responding to breaches of personally identifiable information:** The agencies GAO reviewed have inconsistently implemented policies and procedures for responding to data breaches involving sensitive personal information.
- **Implementing security programs at small agencies:** Smaller federal agencies (generally those with 6,000 or fewer employees) have not always fully implemented comprehensive agency-wide information security programs.

Until agencies take actions to address these challenges—including the hundreds of recommendations made by GAO and inspectors general—their systems and information will be at increased risk of compromise from cyber-based attacks and other threats.