GAO Highlights

Highlights of GAO-15-758T, a testimony before the Subcommittees on Research and Technology and Oversight, Committee on Science, Space, and Technology, House of Representatives

July 8, 2015

INFORMATION SECURITY

Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies

Why GAO Did This Study

Effective cybersecurity for federal information systems is essential to preventing the loss of resources, the compromise of sensitive information, and the disruption of government operations. Since 1997, GAO has designated federal information security as a government-wide high-risk area, and in 2003 expanded this area to include computerized systems supporting the nation's critical infrastructure. Earlier this year, in GAO's high-risk update, the area was further expanded to include protecting the privacy of personal information that is collected, maintained, and shared by both federal and nonfederal entities.

This statement summarizes (1) cyber threats to federal systems, (2) challenges facing federal agencies in securing their systems and information, and (3) government-wide initiatives aimed at improving cybersecurity. In preparing this statement, GAO relied on its previously published and ongoing work in this area.

What GAO Recommends

In previous work, GAO and agency inspectors general have made hundreds of recommendations to assist agencies in addressing cybersecurity challenges. GAO has also made recommendations to improve government-wide initiatives.

View GAO-15-758T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Federal systems face an evolving array of cyber-based threats. These threats can be unintentional—for example, from equipment failure or 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 recent incidents involving breaches of sensitive data and the sharp increase in information security incidents reported by federal agencies over the last several years, which have risen from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014.

GAO has identified a number of challenges federal agencies face in addressing threats to their cybersecurity. For example, agencies have been challenged with designing and implementing risk-based cybersecurity programs, as illustrated by 19 of 24 major agencies declaring cybersecurity as a significant deficiency or material weakness for financial reporting purposes. Other challenges include:

- enhancing oversight of contractors providing IT services,
- improving security incident response activities,
- responding to breaches of personal information, and
- implementing cybersecurity programs at small agencies.

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

Several government-wide initiatives are under way to bolster cybersecurity.

- **Personal Identity Verification:** The President and the Office of Management and Budget (OMB) directed agencies to issue credentials with enhanced security features to control access to federal facilities and systems. OMB recently reported that only 41 percent of user accounts at 23 civilian agencies had required these credentials to access agency systems.
- **Continuous Diagnostics and Mitigation:** This program is to provide agencies with tools for continuously monitoring cybersecurity risks. The Department of State adopted a continuous monitoring program, and GAO reported on the benefits and challenges in implementing the program.
- **National Cybersecurity Protection System:** This system is to provide capabilities for monitoring network traffic and detecting and preventing intrusions. GAO has ongoing work reviewing the system's implementation. Preliminary observations indicate that implementation of the intrusion detection and prevention capabilities may be limited and requirements for future capabilities appear to have not been fully defined.

While these initiatives are intended to improve security, no single technology or tool is sufficient to protect against all cyber threats. Rather, agencies need to employ a multi-layered approach to security that includes well-trained personnel, effective and consistently applied processes, and appropriate technologies.