June 24, 2015

CYBERSECURITY

Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies

GAO Highlights

Highlights of GAO-15-725T, a testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives

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. Federal information and systems face an evolving array of cyber-based threats, and recent data breaches at federal agencies highlight the impact that can result from ineffective security controls.

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. 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) challenges facing federal agencies in securing their systems and information and (2) government-wide initiatives, including those led by DHS, 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-15-725T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

GAO has identified a number of challenges federal agencies face in addressing threats to their cybersecurity, including the following:

- Designing and implementing a risk-based cybersecurity program.
- Enhancing oversight of contractors providing IT services.
- Improving security incident response activities.
- Responding to breaches of personal information.
- 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, including sensitive personal information, will be at an increased risk of compromise from cyber-based attacks and other threats.

In an effort to bolster cybersecurity across the federal government, several government-wide initiatives, spearheaded by the Department of Homeland Security (DHS) and the Office of Management and Budget (OMB), are under way. These include the following:

- **Personal Identity Verification:** In 2004, the President directed the establishment of a government-wide standard for secure and reliable forms of ID for federal employees and contractor personnel who access government facilities and systems. Subsequently, OMB directed agencies to issue personal identity verification credentials 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 for accessing agency systems.
- **Continuous Diagnostics and Mitigation:** DHS, in collaboration with the General Services Administration, has established a government-wide contract for agencies to purchase tools that are intended to identify cybersecurity risks on an ongoing basis. These tools can support agencies' efforts to monitor their networks for security vulnerabilities and generate prioritized alerts to enable agency staff to mitigate the most critical weaknesses. The Department of State adopted a continuous monitoring program, and in 2011 GAO reported on the benefits of the program and challenges the department faced in implementing its approach.
- **National Cybersecurity Protection System (NCPS):** This system, also referred to as EINSTEIN, is to include capabilities for monitoring network traffic and detecting and preventing intrusions, among other things. GAO has ongoing work reviewing the implementation of NCPS, and preliminary observations indicate that implementation of the intrusion detection and prevention capabilities may be limited and DHS appears to have not fully defined requirements for future capabilities.

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, "defense in depth" approach to security that includes well-trained personnel, effective and consistently applied processes, and appropriate technologies.