September 19, 2016

FEDERAL INFORMATION SECURITY

Actions Needed to Address Challenges

GAO Highlights

Highlights of GAO-16-885T, a testimony before the President's Commission on Enhancing National Cybersecurity

Why GAO Did This Study

The dependence of federal agencies on computerized information systems and electronic data makes them potentially vulnerable to a wide and evolving array of cyber-based threats. Securing these systems and data is vital to the nation's safety, prosperity, and well-being.

Because of the significance of these risks and long-standing challenges in effectively implementing information security protections, GAO has designated federal information security as a government-wide high-risk area since 1997. In 2003 this area was expanded to include computerized systems supporting the nation's critical infrastructure, and again in February 2015 to include protecting the privacy of personally identifiable information collected, maintained, and shared by both federal and nonfederal entities.

GAO was asked to provide a statement on laws and policies shaping the federal IT security landscape and actions needed for addressing long-standing challenges to improving the nation's cybersecurity posture. In preparing this statement, GAO relied on previously published work.

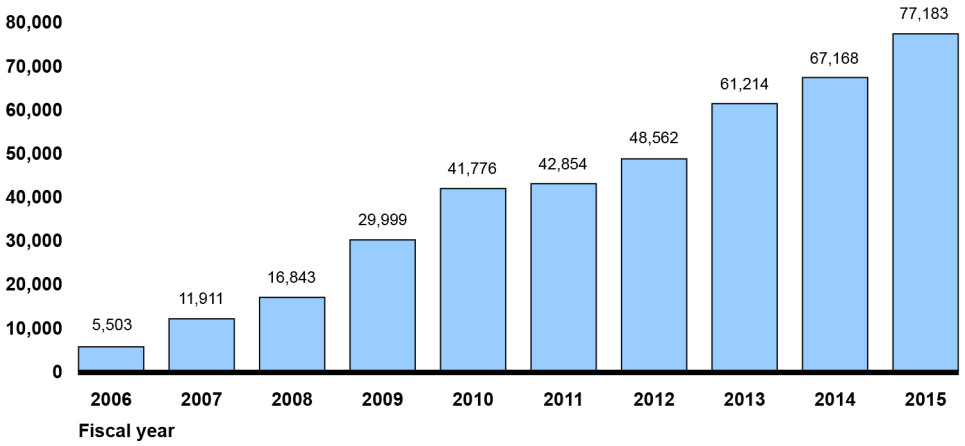
Over the past several years, GAO has made about 2,500 recommendations to federal agencies to enhance their information security programs and controls. As of September 16, 2016, about 1,000 have not been implemented.

View GAO-16-885T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Cyber incidents affecting federal agencies have continued to grow, increasing about 1,300 percent from fiscal year 2006 to fiscal year 2015.

Cyber Incidents Reported by Federal Agencies, Fiscal Year 2006--2015



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal years 2006-2015. | GAO-16-885T

Several laws and policies establish a framework for the federal government's information security and assign implementation and oversight responsibilities to key federal entities, including the Office of Management and Budget, executive branch agencies, and the Department of Homeland Security (DHS).

However, implementation of this framework has been inconsistent, and additional actions are needed:

- **Effectively implement risk-based information security programs.** Agencies have been challenged to fully and effectively establish and implement information security programs. They need to enhance capabilities to identify cyber threats, implement sustainable processes for securely configuring their computer assets, patch vulnerable systems and replace unsupported software, ensure comprehensive testing and evaluation of their security on a regular basis, and strengthen oversight of IT contractors.
- **Improve capabilities for detecting, responding to, and mitigating cyber incidents.** Even with strong security, organizations can continue to be victimized by attacks exploiting previously unknown vulnerabilities. To address this, DHS needs to expand the capabilities and adoption of its intrusion detection and prevention system, and agencies need to improve their practices for responding to cyber incidents and data breaches.
- **Expand cyber workforce and training efforts.** Ensuring that the government has a sufficient cybersecurity workforce with the right skills and training remains an ongoing challenge. Government-wide efforts are needed to better recruit and retain a qualified cybersecurity workforce and to improve workforce planning activities at agencies.