PRESIDENTIAL AND CONGRESSIONAL TRANSITION

Management Agenda: *Strengthen Cybersecurity Over Sensitive Data and Protect Critical Infrastructure*

The Presidential Transition Act points to the U.S. Government Accountability Office (GAO) as a resource for incoming administrations as well as new Congresses.

GAO's **Management Agenda** is a streamlined tool for new leaders to quickly learn about critical management challenges and risks facing the federal government and the actions needed to address those challenges.

Strengthen Cybersecurity Over Sensitive Data and Protect Critical Infrastructure is one of the eight management challenges highlighted in the Management Agenda.

Federal agencies and our nation's critical infrastructures depend on computerized (cyber) information systems and electronic data to carry out operations and to process, maintain, and report essential information. The security of these systems and data is vital to public confidence and the nation's safety, prosperity, and well-being.

Challenge: Unsecured Information and Infrastructure

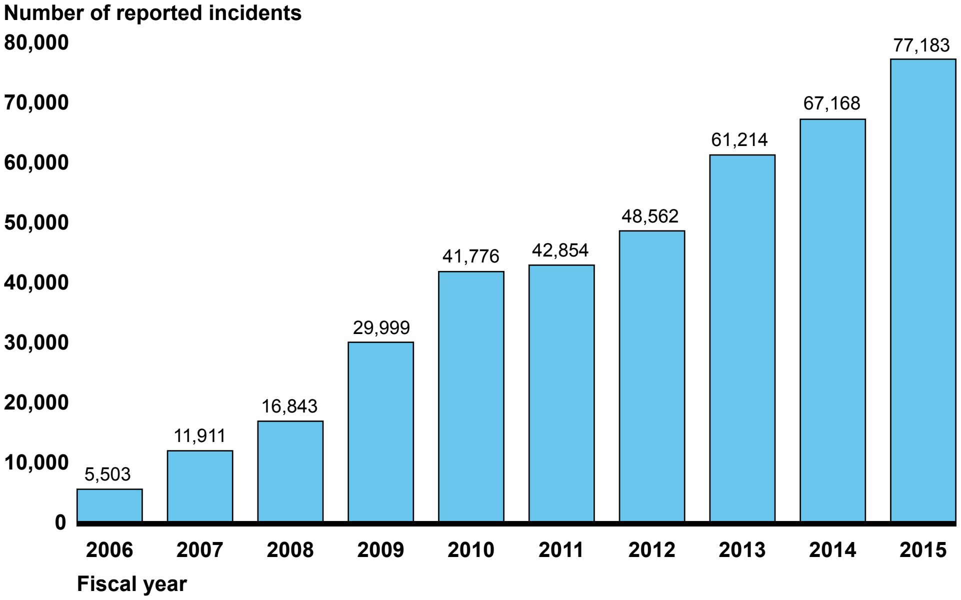
Computerized information and communications systems support federal agencies and the nation's critical infrastructures—such as energy, transportation systems, communications, and financial services. These vital systems are under assault from an array of evolving and sophisticated threats from hackers (foreign and domestic) and insiders alike. Protecting these IT systems and the data within them is a continuing concern.

These systems are often riddled with cybersecurity control weaknesses that increase the risk of compromise. Federal agency reports of information security incidents skyrocketed over the past decade. These incidents:

- jeopardize the privacy of personally identifiable information of millions of individuals;
- expose sensitive information to unauthorized use, disclosure, alteration, and loss; and
- disrupt agency operations.

Cybersecurity and privacy safeguards remain paramount as federal agencies and privately-owned critical infrastructures become ever more dependent on interconnected computer systems to communicate, deliver services, and conduct operations.

Incidents Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies, Fiscal Years 2006 through 2015



Sources: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal years 2006-2015. | GAO-16-501

Key Actions Needed

1. Implement risk-based information security programs at federal agencies.
2. Bolster cybersecurity controls over federal information systems.
3. Develop and implement privacy policies and procedures on a consistent basis.
4. Strengthen the effectiveness of public-private partnerships in securing cyber systems supporting critical infrastructures.

Related GAO Work

- Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information - High Risk Issue

Contact

Gregory C. Wilshusen
Director, Information
Security Issues
wilshuseng@gao.gov
202-512-6244