GAO
Accountability * Integrity * Reliability

Federal Information Security Management Act (FISMA)

Presented to

Information **S**ecurity and **P**rivacy **A**dvisory **B**oard

February 14, 2013

Agenda

- FISMA Legislation
- Changes in Information Security Practices
- GAO's FISMA Role
- Information Security Program Reviews
- Results of Reviews
- Common Recommendations
- Recent GAO Reports
- Questions

FISMA - The Legislation

Public Law 107-347, Title III

- Enacted into law on December 17, 2002, as title III of the E-Government Act of 2002
- Applies to all federal agencies
- Permanently authorized and strengthened information security program, evaluation, and reporting requirements.
- Assigns specific responsibilities to agency heads and chief information officers (CIO), IGs, NIST, OMB, and GAO.

Changes to security practices

Launching a new security reporting tool—Cyberscope

- In fiscal year 2010, OMB mandated that agencies use Cyberscope for submitting their information security data to OMB.

Changes to security practices

Developing new security metrics

- In fiscal year 2010, OMB convened a joint task force12 that developed new security performance metrics that are intended to encourage agencies to focus on risk and improve information security.

  The revised metrics included reporting on

Changes to security practices

Revised security metrics

- Boundary protection—to report information on the status of agencies' implementation of the Trusted Internet Connections initiative.
- Remote access and telework—to report information on the methods allowed to remotely connect to agency network resources.

Changes to security practices

Revised security metrics (continued)

- Identity and access management—to report on the extent to which agencies have issued and implemented personal identity verification cards in accordance with Homeland Security Presidential Directive 12.

- Data protection—to report agencies' use of encryption on portable computers, such as laptops

Changes to security practices

- **Current cross-agency priorities for enhancing cybersecurity**
  - TIC/Einstein
    - External connections
  - Continuous monitoring
    - Automated monitoring capabilities
    - Cyberscope
  - HSPD-12, PIV Cards
    - Logical access

GAO's FISMA Role

- We issue reports every two years as periodically required by FISMA; we also respond to FISMA-related requests, which typically include at least one testimony per year.
- Issued four reports since 2005
- Our most recent report issued in October 2011 (GAO-12-137).
- In addition, when conducting information security audits at individual federal agencies, we evaluate the agency's implementation of FISMA.

Information Security Program Reviews

Audit Objective

- To determine whether the agency has effectively implemented appropriate information security controls to protect the confidentiality, integrity, and availability of the information and systems that support its mission.

Information Security Program Reviews

- Methodology Used to Address Objective
  - The Federal Information Systems Control Audit Manual (FISCAM) - GAO-09-232G
  - NIST Special Publications (i.e. 800-53, 37, 137; FIPS 199, 200)
  - Agency Policies and Procedures

Information Security Program Reviews

(1) Security Management –examine and determine the effectiveness of the agency's security program.

(2) Access Controls – examine both logical and physical controls, including how well the agency safeguards IT and other sensitive information (both automated and paper).

(3) Configuration Management- examine and determine whether agency controls provide reasonable assurance that changes to information system resources are authorized and systems are configured and operated securely.

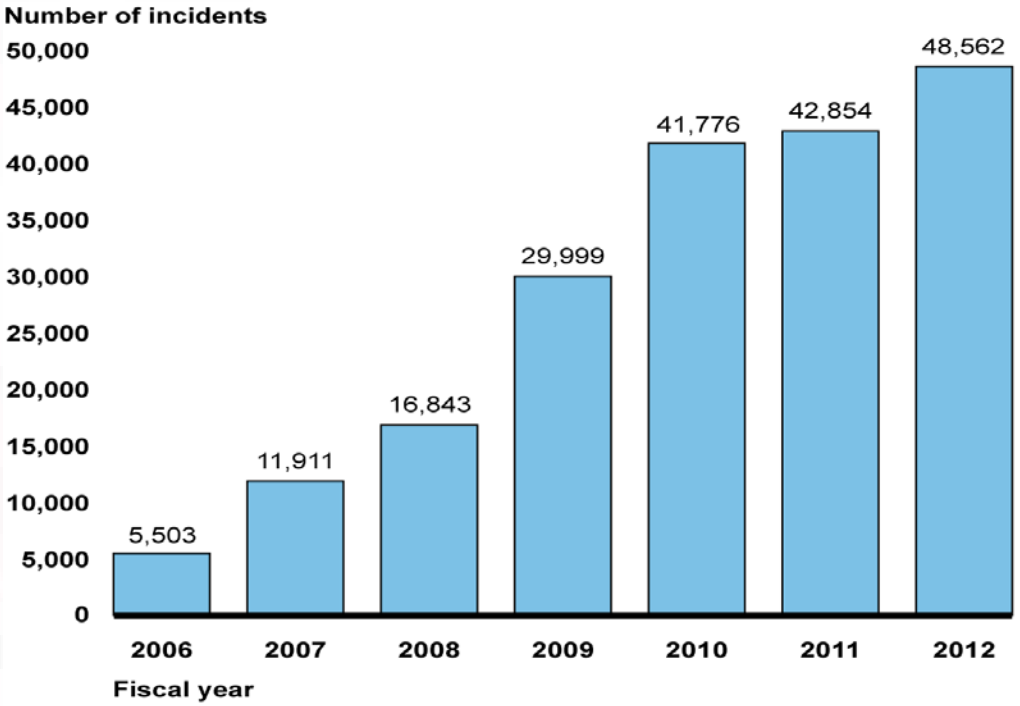
Information Security Program Reviews

(4) Segregation of Duties-examine and determine whether agency controls provide reasonable assurance that changes to information system resources are authorized and systems are configured and operated securely.

(5) Contingency Planning- examine and determine whether agency controls provide reasonable assurance that contingency planning protects information resources and minimizes the risk of unplanned interruptions and provides for recovery of critical operations should interruptions occur.

Results of Reviews

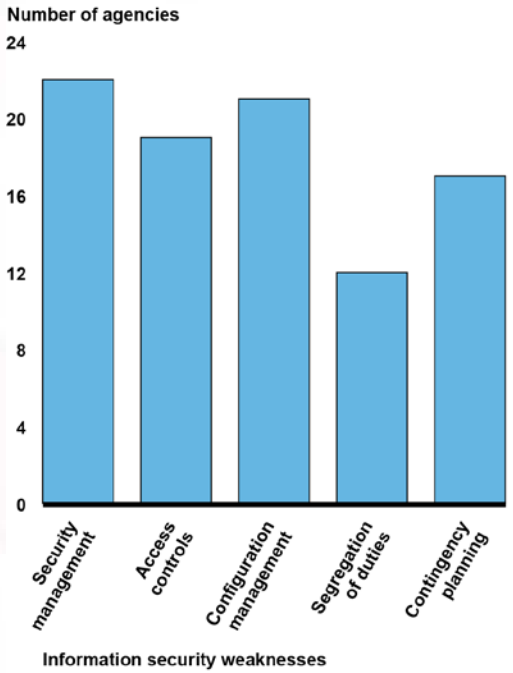
- **Reported security incidents continue to rise**



Source: GAO analysis of US-CERT data for fiscal years 2006-2012.

Results of Reviews

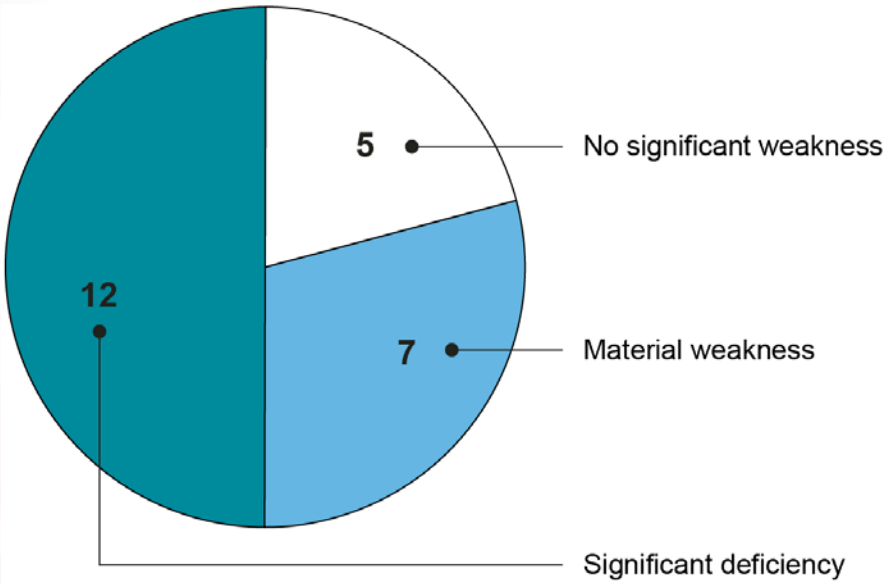
- **Agencies had weaknesses in most FISCAM general control areas in FY 2012**



Source: GAO analysis of agency, inspectors general, and GAO reports as of December 13, 2012.

Snapshots of Federal Information Security (cont.)

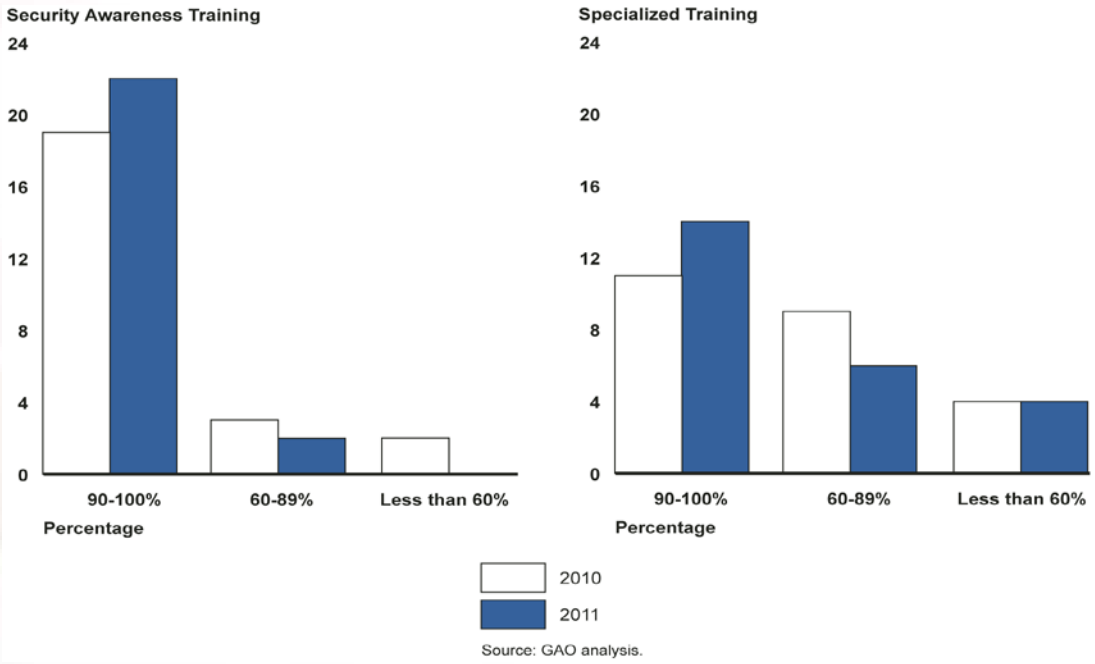
- **Agencies continue to report information security weaknesses over financial systems**



Source: GAO analysis of agency performance and accountability reports, annual financial reports, or other financial statement reports for fiscal year 2012.

Results of Reviews

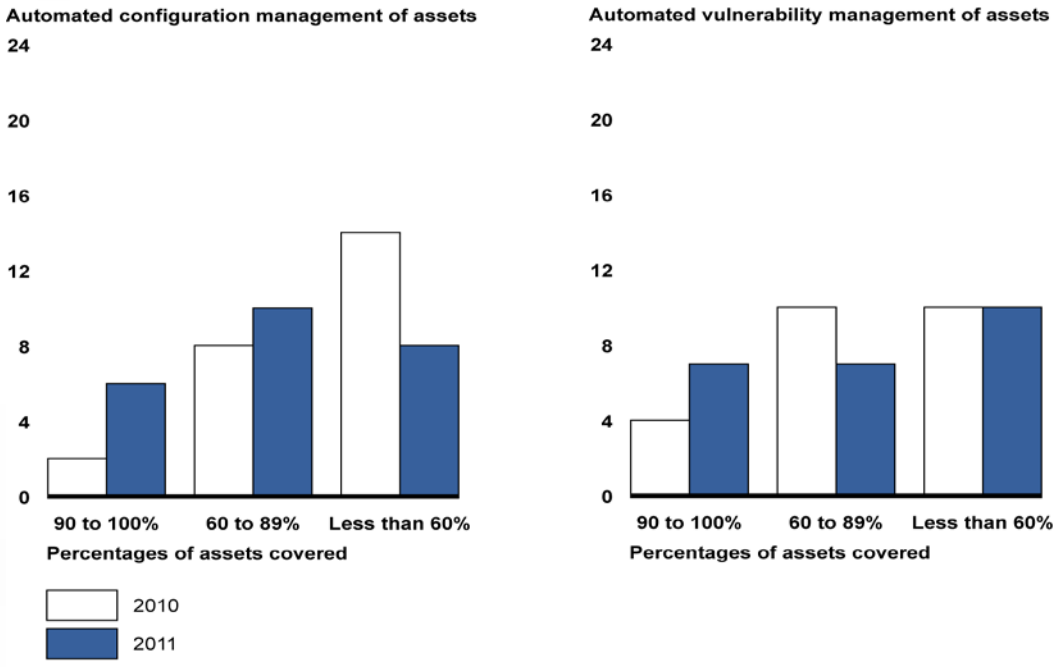
- **Agencies have provided training to increasing percentages of personnel**



Source: GAO analysis.

Results of Reviews

- Agencies have increased automated capabilities for managing assets



Source: GAO analysis of agency fiscal year 2010 and 2011 data.

Common Recommendations

- **Common recommendations for improving security controls:**
  - Change vendor-supplied IDs and passwords
  - Strengthen authentication controls
  - Use two-factor authentication for remote access
  - Limit access to bona fide needs
  - Remove inactive accounts & accounts of separated users
  - Install patches timely
  - Keep software current
  - Use encrypted protocols
  - Implement access control lists

Common Recommendations

- **Common recommendations for improving security programs:**
  - Provide role-based training for those with significant security responsibilities
  - Monitor assets, configurations, vulnerabilities frequently
  - Test effectiveness of IT security controls
  - Remedy known vulnerabilities timely
  - Verify effectiveness of remediation efforts
  - Implement adequate incident detection and response capabilities
  - Test viability of contingency plans

Indicators of Success

Agencies Need to:

(1) develop and implement remedial action plans for resolving known security deficiencies of government systems,

(2) fully develop and effectively implement agencywide information security programs, as required by the Federal Information Security Management Act of 2002, and

(3) demonstrate measurable, sustained progress in improving security over federal systems.

Recent GAO Reports

- GAO-13-155, *Information Security: Federal Communications Commission Needs to Strengthen Controls over Enhanced Secured Network Project*, (January 2013).
- GAO-12-757, *Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged, (*September 2012).
- GAO-12-816, *Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices, (*August 2012).
- *GAO-12-696, Information Security: Environmental Protection Agency Needs to Resolve Weaknesses, (*July 2012).

Recent GAO Reports

- GAO-12-666T, *Cybersecurity: Threats Impacting the Nation* (April 2012)
- GAO-12-424R, *Management Report: Improvements Needed in SEC's Internal Control and Accounting Procedure* (April 2012)
- GAO-12-393, *Information Security: IRS Needs to Further Enhance Internal Control over Financial Reporting and Taxpayer Data* (March 2012)
- GAO-12-361, *IT Supply Chain: National Security-Related Agencies Need to Better Address Risks* (March 2012)
- GAO-12-507T, *Cybersecurity: Challenges in Securing the Modernized Electricity Grid* (February 2012)

Recent GAO Reports

- GAO-12-92, *Critical Infrastructure Protection: Cybersecurity Guidance is Available, but More Can Be Done to Promote Its Use* (December 2011)
- GAO-12-8, *Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination* (November 2011)
- GAO-12-130T, *Information Security: Additional Guidance Needed to Address Cloud Computing Concerns* (October 2011)
- GAO-12-137, *Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements* (October 2011)

Recent GAO Reports

- GAO-11-751, *Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards* (September 2011)
- GAO-11-708, *Information Security: FDIC Has Made Progress, but Further Actions Are Needed to Protect Financial Data* (August 2011)
- GAO-11-695R, *Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates* (July 2011)
- GAO-11-865T, *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure* (July 2011)

Recent GAO Reports

- GAO-11-149, *Information Security: State Has Taken Steps to Implement a Continuous Monitoring Application, but Key Challenges Remain* (July 2011)
- GAO-11-75, *Defense Department Cyber Efforts: DOD Faces Challenges in Its Cyber Activities* (July 2011)
- GAO-11-605, *Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate* (June 2011)
- GAO-11-463T, *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems* (March 2011)
- GAO-11-308, *Information Security: IRS Needs to Enhance Internal Control Over Financial Reporting and Taxpayer Data* (March 2011)

Questions

Contacts

Anjalique Lawrence
Assistant Director, Information Security Issues
LawrenceAJ@gao.gov
(202) 512-6308