GAO Information Security Update

Presented to

Federal Computer Security Program Managers' Forum

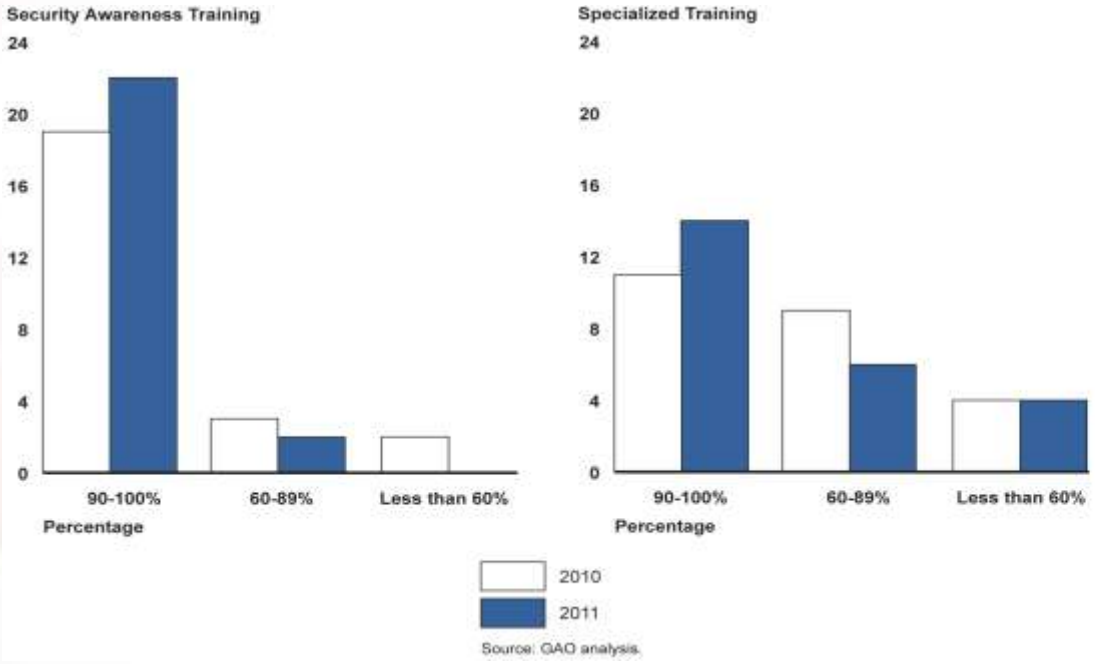
June 12, 2012

Agenda

- Snapshots of Federal Information Security
- Ongoing and Planned Work
- Current Bills to Amend FISMA
- Recent GAO Reports
- Questions

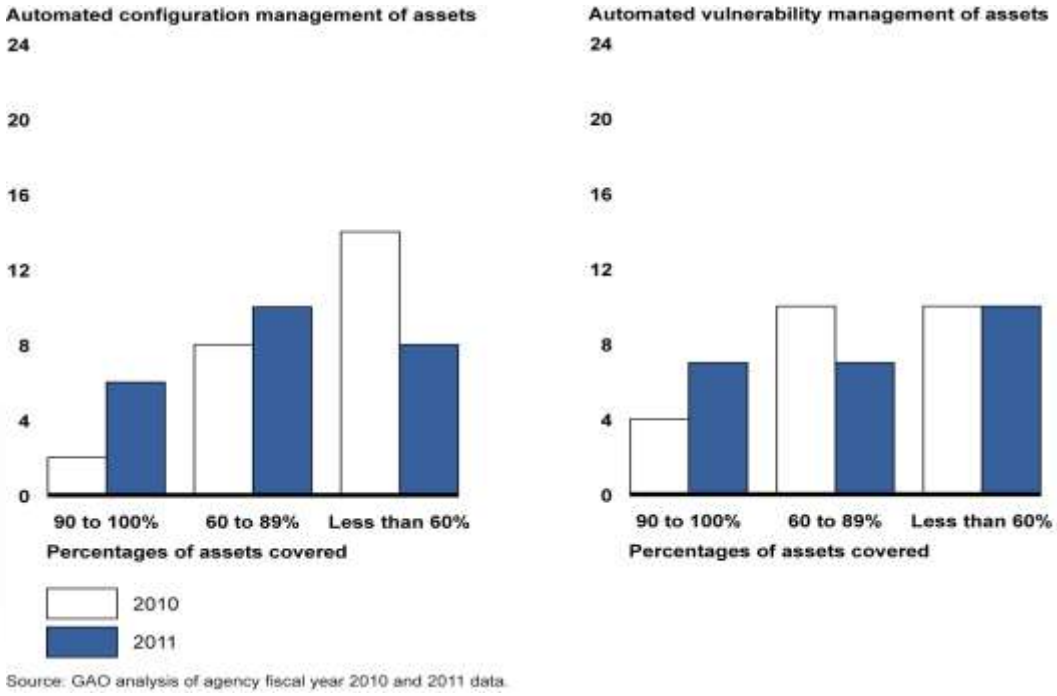
Snapshots of Federal Information Security

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



Snapshots of Federal Information Security (cont.)

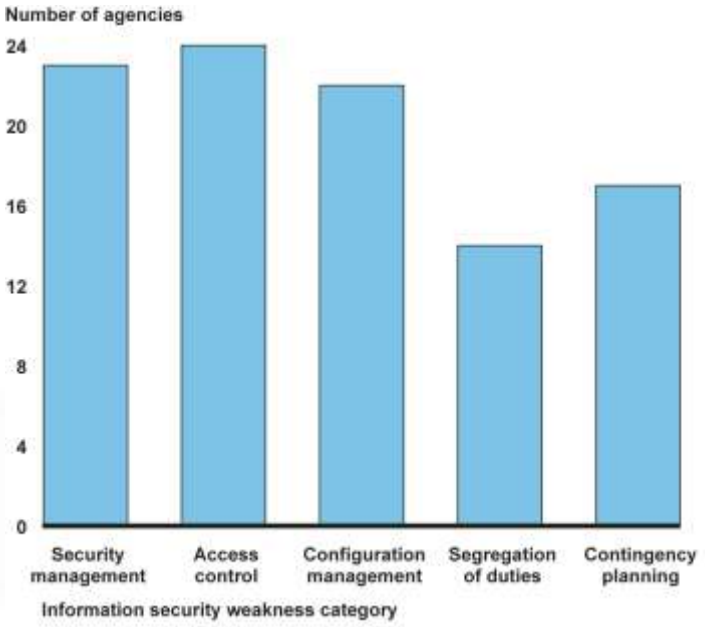
- Agencies have increased automated capabilities for managing assets



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

Snapshots of Federal Information Security (cont.)

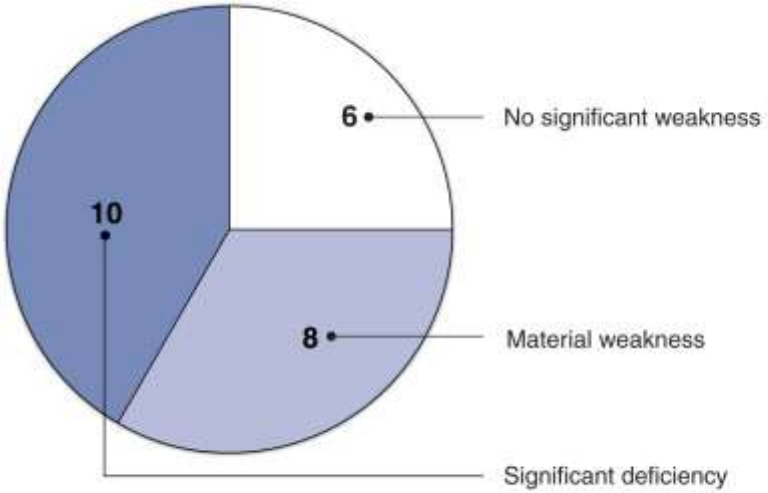
- **Most agencies had weaknesses in most FISCAM general control areas in FY 2011**



Source: GAO analysis of agency, inspectors general, and GAO reports.

Snapshots of Federal Information Security (cont.)

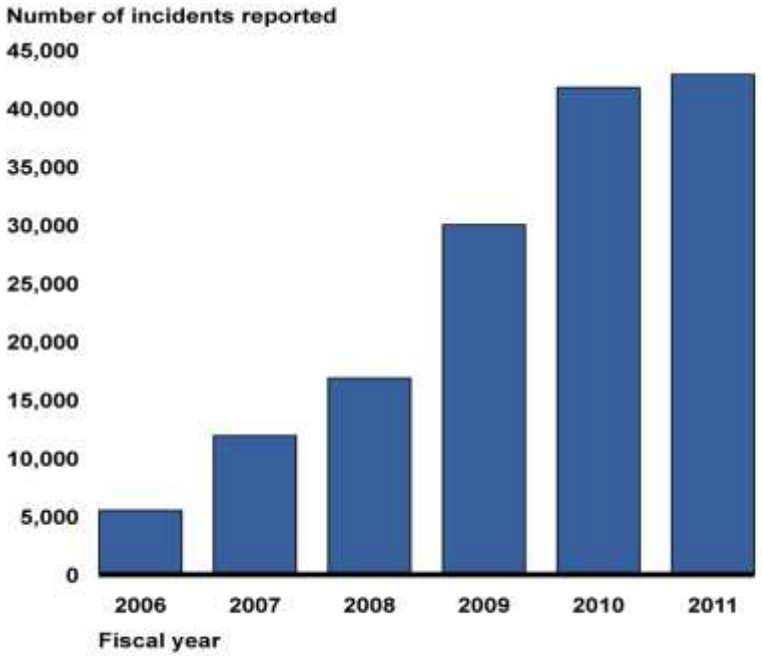
- **Agencies continue to report information security weaknesses over financial systems**



Source: GAO analysis of agency performance and accountability reports, annual financial reports, or other financial statement reports for fiscal year 2011.

Snapshots of Federal Information Security (cont.)

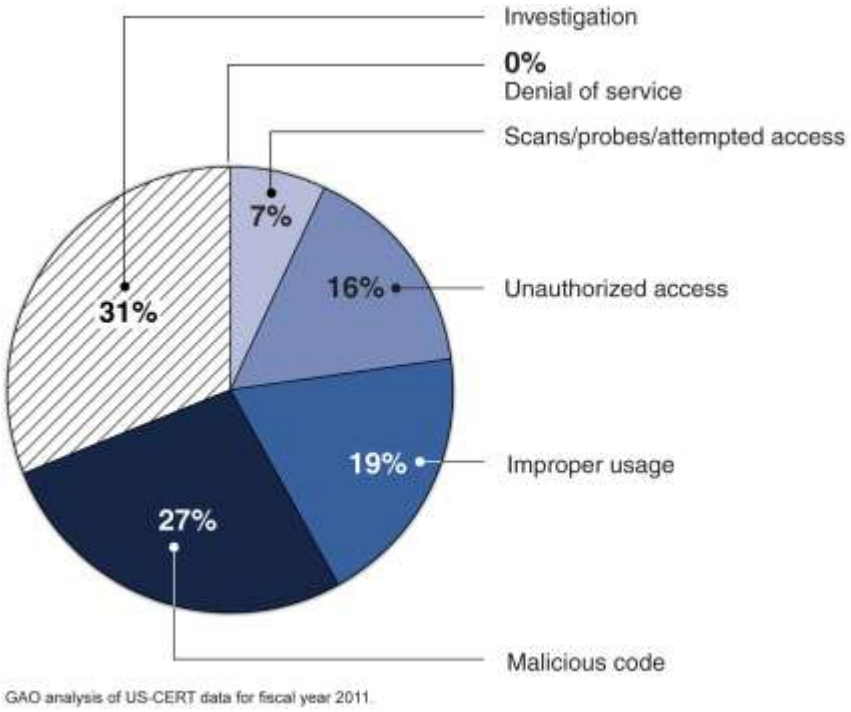
- **Reported security incidents continue to rise**



Source: GAO analysis of US-CERT data for fiscal years 2006-2011.

Snapshots of Federal Information Security (cont.)

- **Agencies reported a variety of incidents**



GAO analysis of US-CERT data for fiscal year 2011.

Snapshots of Federal Information Security (cont.)

- **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

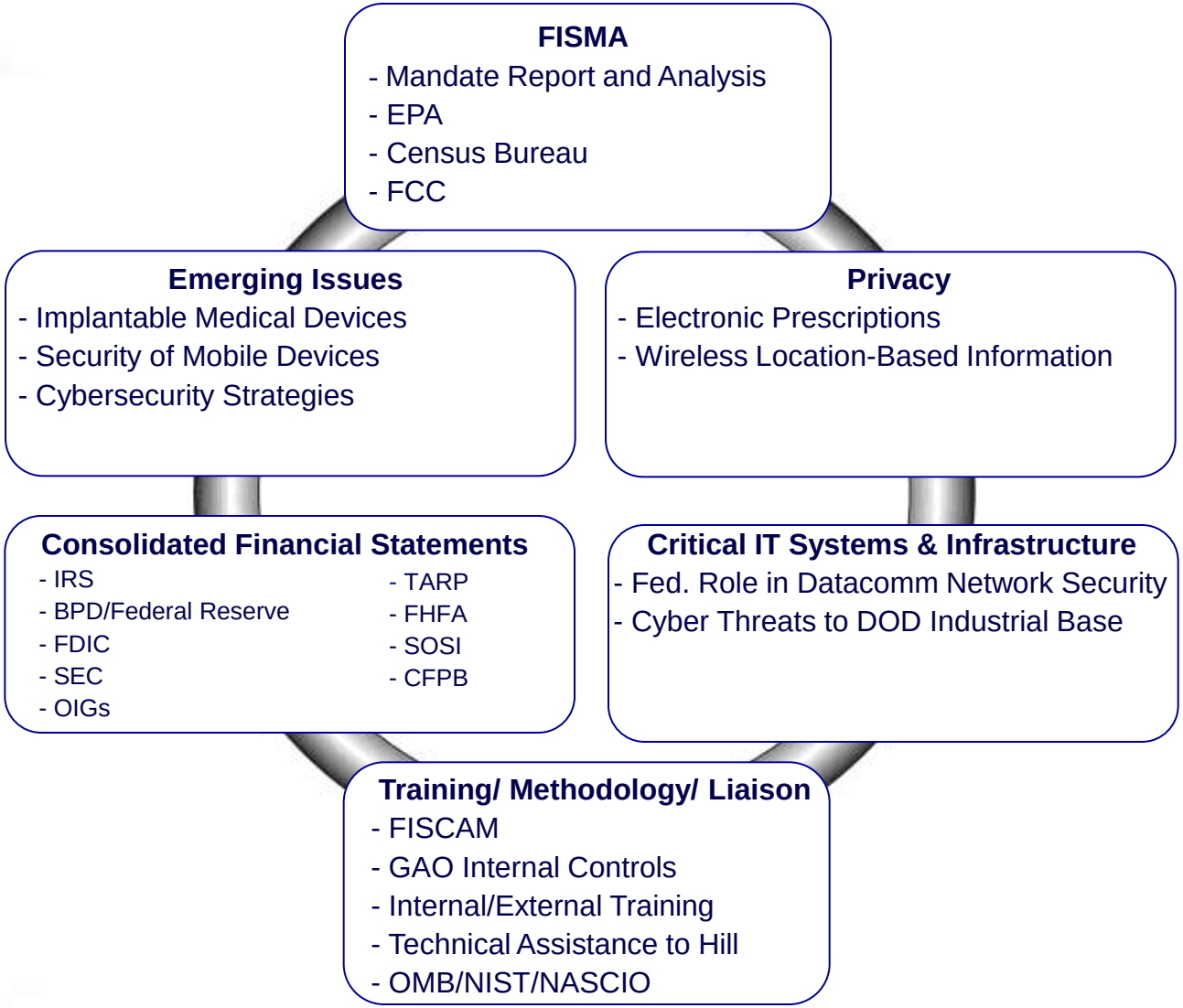
Snapshots of Federal Information Security (cont.)

- **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

Snapshots of Federal Information Security (cont.)

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

Ongoing and Planned Work



Current Bills to Amend FISMA

- **Four bills introduced to amend FISMA**
  - Lieberman/Collins(S 2105), McCain/Hutchinson(S 2151), Issa/Cummings(House passed HR 4257),and Langevin/Bartlett (HR1136)
- **Major Issues**
  - Disparity in oversight of agency information security programs (OMB, DHS, Commerce, or National Office for Cyberspace)
  - Emphasis on continuous monitoring, operational capabilities, and incident detection and response
  - Varying approaches on IG evaluations

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

Gregory Wilshusen
Director, Information Security Issues
WilshusenG@gao.gov

Anjalique Lawrence
Assistant Director, Information Security Issues
LawrenceAJ@gao.gov