GAO Information Security Issues

Presented to:

Federal Audit Executive Council

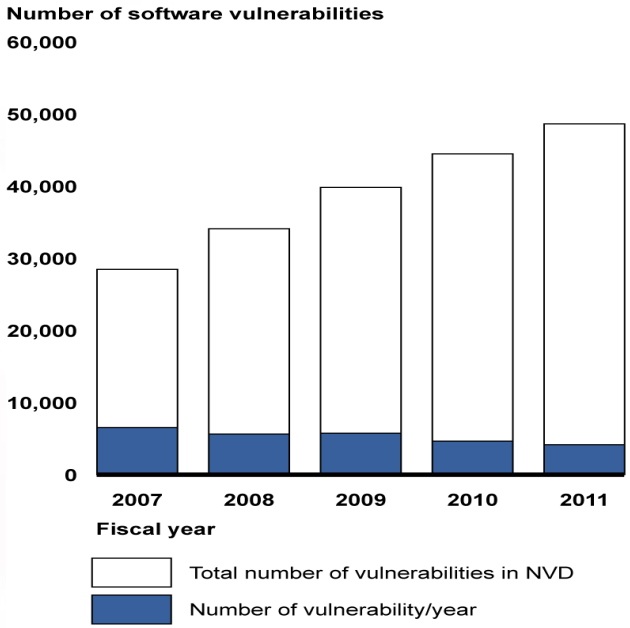
April 18, 2012

Agenda

- Snapshots of Federal Information Security
- Highlights of Selected GAO Reports
- GAO Focus Areas
- List of Recent GAO Reports on Cybersecurity
- Questions and Answers

Snapshots of Federal Information Security

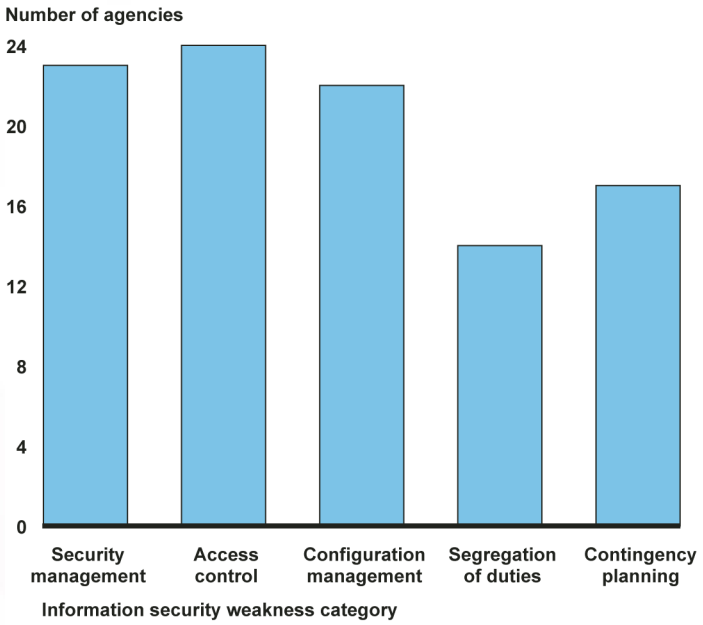
- **Increasing software vulnerabilities is one of several security challenges confronting agencies**



Source: GAO analysis of software vulnerabilities reported in the National Vulnerability Database (NVD) 2007-2011.

Snapshots of Federal Information Security

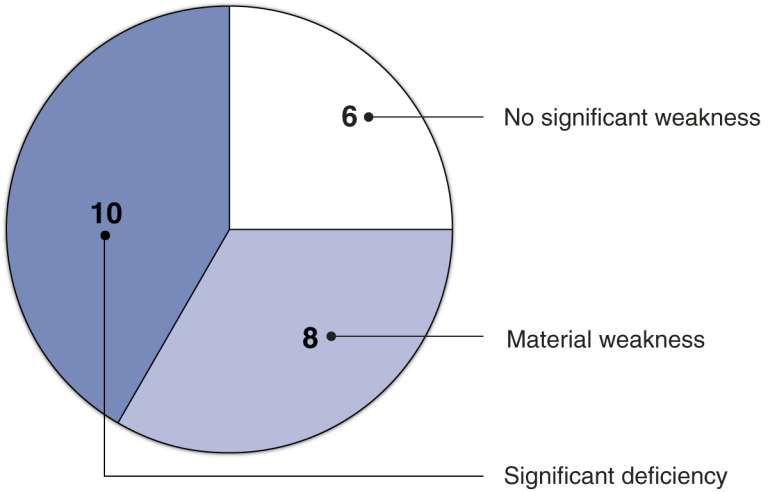
- **Most agencies have weaknesses in most FISCAM general control areas in FY 2011**



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

Snapshots of Federal Information Security

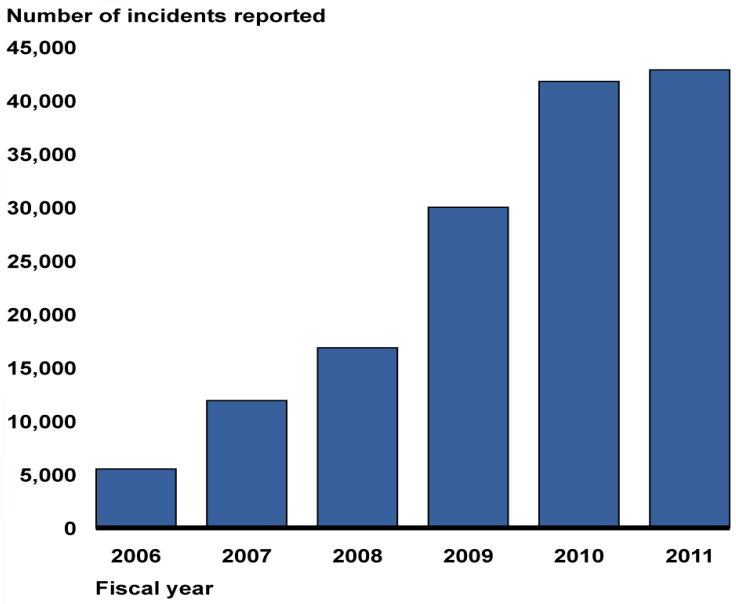
- **Agencies continue to report information security weaknesses over financial systems**



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

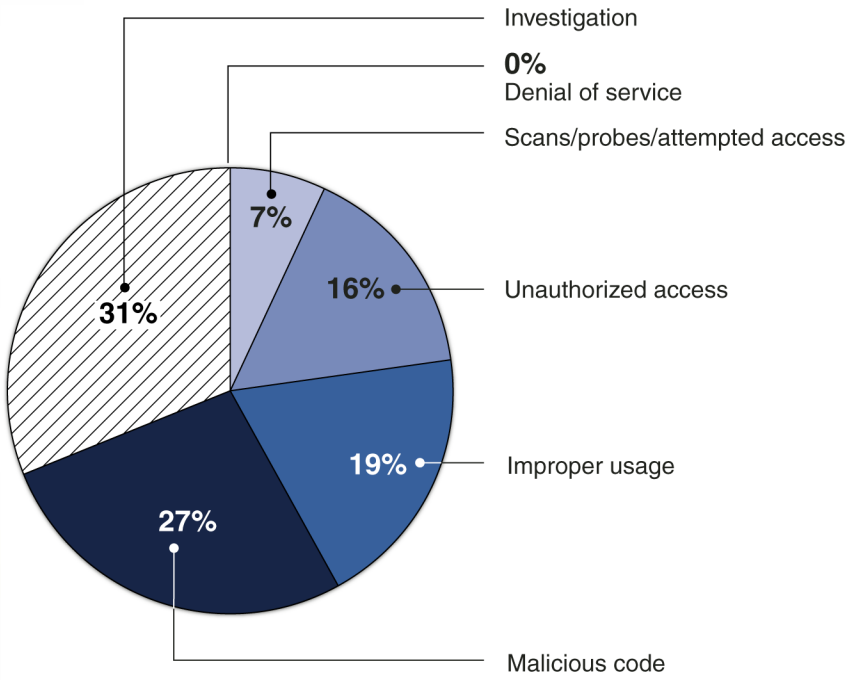
- **Reported security incidents continue to rise**



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

Snapshots of Federal Information Security

- **Types of reported security incidents varied**



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

Snapshots of Federal Information Security

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

Review of State Dept.'s iPost continuous monitoring system (GAO-11-149)

- Requested by Senators Carper, Lieberman, Brown
- 4 objectives: Identify scope, use, controls, benefits and challenges associated with iPost
- Key findings:
  - iPost covers many, but not all, devices and controls
  - Risk scoring helps to identify vulnerabilities, prioritize remediation & provide accountability
  - Challenges include limitations of automated tools, implementing configuration management, adopting a strategy, and managing stakeholder expectations

Review of PIV Implementation (GAO-11-751)

- Requested by Senators Lieberman, Collins, Carper
- 2 objectives: Assess progress, identify obstacles
- Scope: 8 agencies plus OMB, GSA; Oct 2010 – Sept 2011
- Key findings:
  - Substantial progress conducting BIs and issuing cards
  - Fair to limited progress using electronic features for physical and logical access; minimal for interoperability
  - Obstacles include: logistical problems issuing cards to individuals in remote locations; low priority to implement electronic capabilities; and lack of trust in credentials issued by other agencies

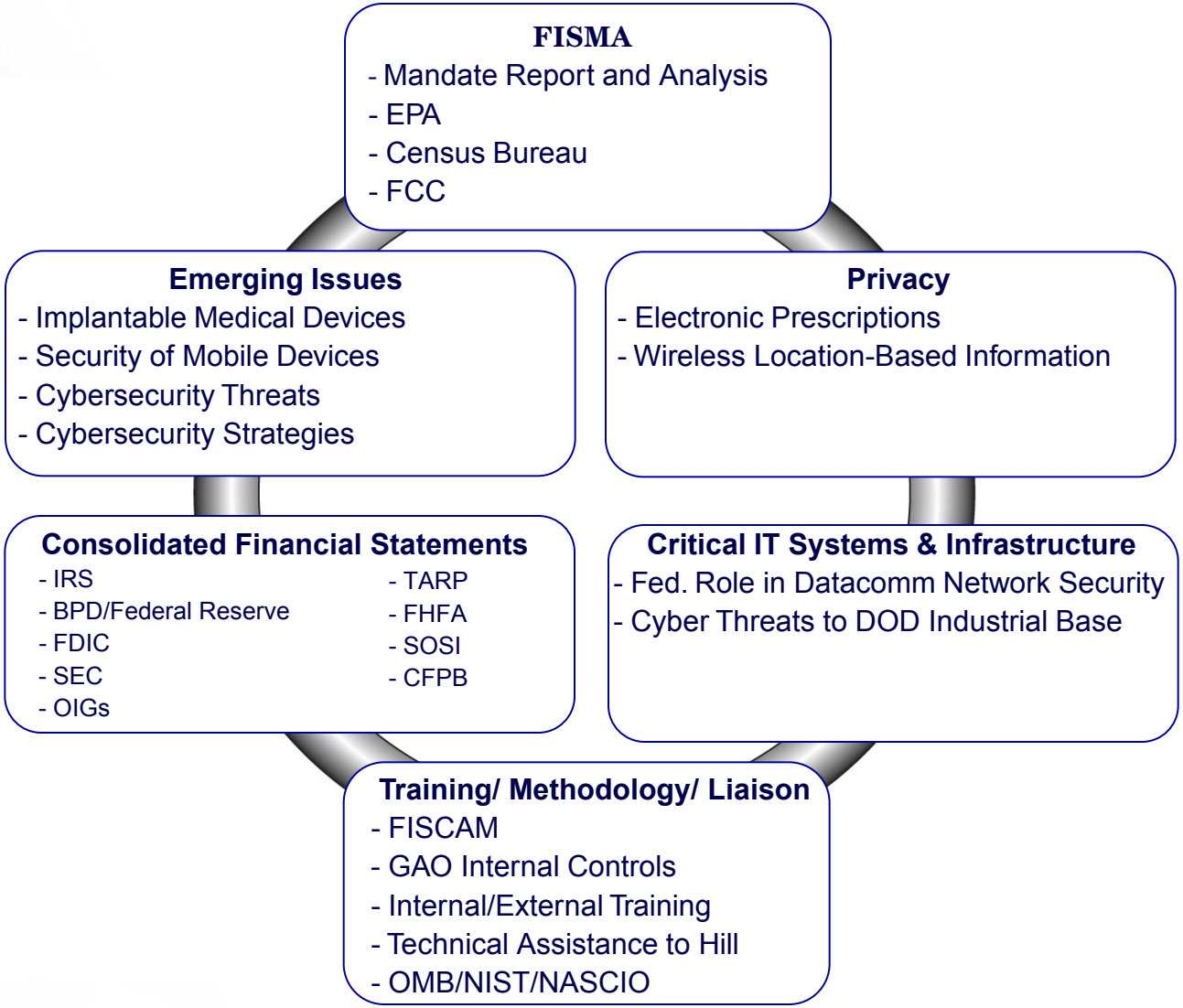
Review of Cybersecurity Human Capital (GAO-12-8)

- Requested by Senator Schumer
- 2 objectives: Assess agency workforce planning activities for cybersecurity and status of governmentwide initiatives
- Scope: 8 agencies plus OPM, NIST; Dec 2010 – Nov 2011
- Key Findings:
  - Agencies varied in their use of workforce planning practices – 5 of 8 developed cyber workforce plans; all faced challenges identifying size of workforce and several with filling cybersecurity positions; 6 of 8 identified hiring process as an obstacle; training opportunities varied
  - Governmentwide efforts to enhance cyber workforce, but efforts lack planning and coordination

Review of IT Supply Chain (GAO-12-361)

- Requested by Senators Kyl, Hutchison, Collins, Carper, Gillibrand, and Rep. Upton
- 3 objectives: Identify risks, extent agencies addressed risks, extent agencies identified foreign technology in networks
- Scope: 4 agencies – Energy, DHS, Justice, DOD
- Key Findings:
  - IT supply chain may introduce malicious code, counterfeits, shortages or disruptions, unintentional vulnerabilities
  - Energy, DHS, Justice have not fully addressed risk, DOD is further along; governmentwide efforts are underway
  - Agencies have not identified foreign technology

Cybersecurity Focus Areas



Recent GAO Reports

- GAO-12-424R, Management Rpt: Improvements Needed in SEC's Internal Control and Accounting Procedure (Apr. 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)
- GAO-12-92, Critical Infrastructure Protection: Cybersecurity Guidance is Available, but More Can Be Done to Promote Its Use (December 2011)

Recent GAO Reports (cont.)

- GAO-12-8, Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination (Nov. 2011)
- GAO-12-130T, Information Security: Additional Guidance Needed to Address Cloud Computing Concerns (Oct. 2011)
- GAO-12-137, Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements (Oct. 2011)
- GAO-11-751, Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards (Sept. 2011)

Recent GAO Reports (cont.)

- GAO-11-708, Information Security: FDIC Has Made Progress, but Further Actions Are Needed to Protect Financial Data (Aug. 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)
- GAO-11-149, Information Security: State Has Taken Steps to Implement a Continuous Monitoring Application, but Key Challenges Remain (July 2011)

Recent GAO Reports (cont.)

- 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)
- GAO-11-278, High-Risk Series: An Update (February 2011)

Recent GAO Reports (cont.)

- GAO-11-117, Electric Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed (January 2011)
- GAO-11-67, Information Security: National Nuclear Security Administration Needs to Improve Contingency Planning for Its Classified Supercomputing Operations (December 2010)
- GAO-11-43, Information Security: Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risks (November 2010)
- GAO-11-20, Information Security: National Archives and Records Administration Needs to Implement Key Program Elements and Controls (October 2010)

Recent GAO Reports (cont.)

- GAO-11-24, Cyberspace Policy: Executive Branch is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership is Needed (October 2010)
- GAO-10-916, Information Security: Progress Made on Harmonizing Policies and Guidance for National Security and Non-National Security Systems (September 2010)
- GAO-10-628, Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed (July 2010)
- GAO-10-606, Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance (July 2010)

GAO Contact

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

www.gao.gov