GAO Information Security Update

Presented to

Federal Computer Security Program Managers' Forum

June 4, 2013

Agenda

- Snapshots of Federal Information Security
- Ongoing and Planned Work
- Sense of the Information Security Community
- Recent GAO Reports
- Questions

Agencies report security improvements

- Provided training to increasing percentages of privileged users

- Increased automated capabilities for managing assets

- Increased automated capabilities for managing vulnerabilities

- Increased TIC traffic consolidation and capabilities

- Increased implementation of continuous monitoring programs

Most agencies have information security weaknesses in most control areas
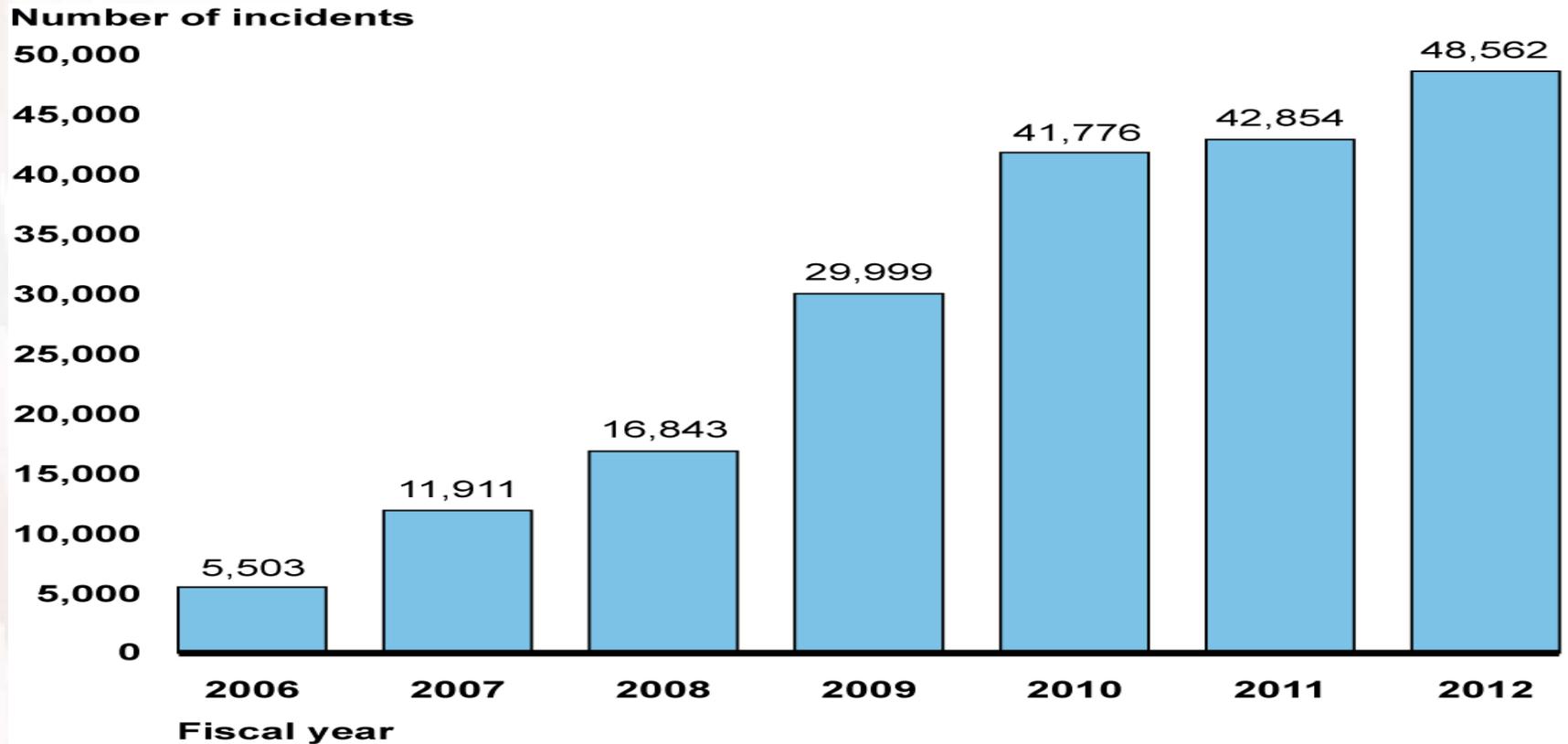
Number of agencies
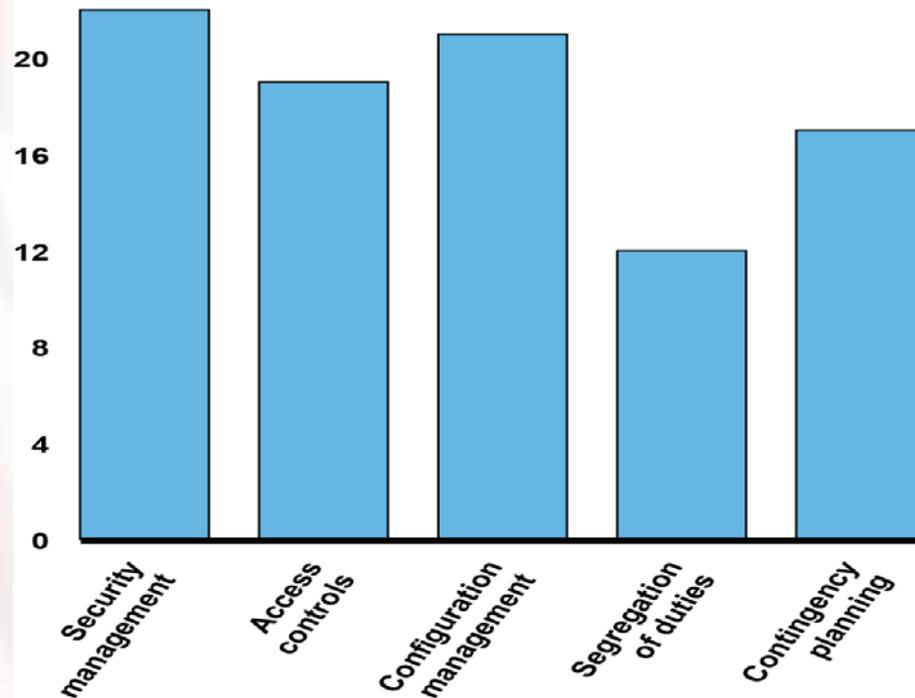
Information security weaknesses

Source: GAO analysis of agency, inspectors general, and GAO reports as of December 13, 2012.
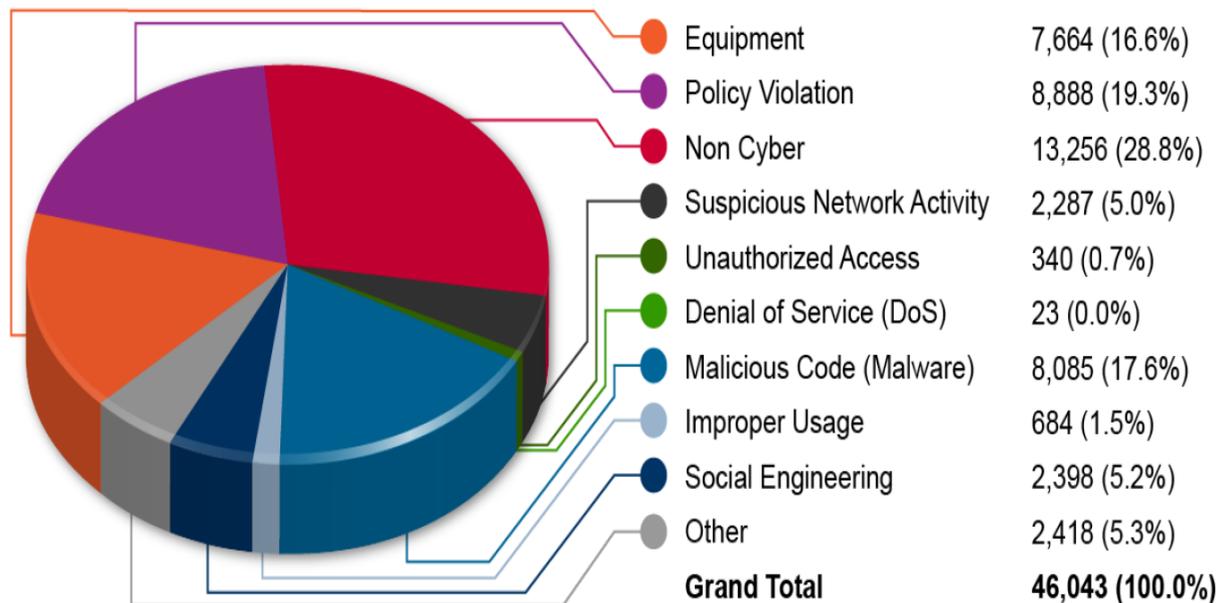
Reported security incidents continue to rise

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

Agencies reported a variety of incidents

Figure 3. Summary of CFO Act Agency Incidents Reported to US-CERT in FY 2012

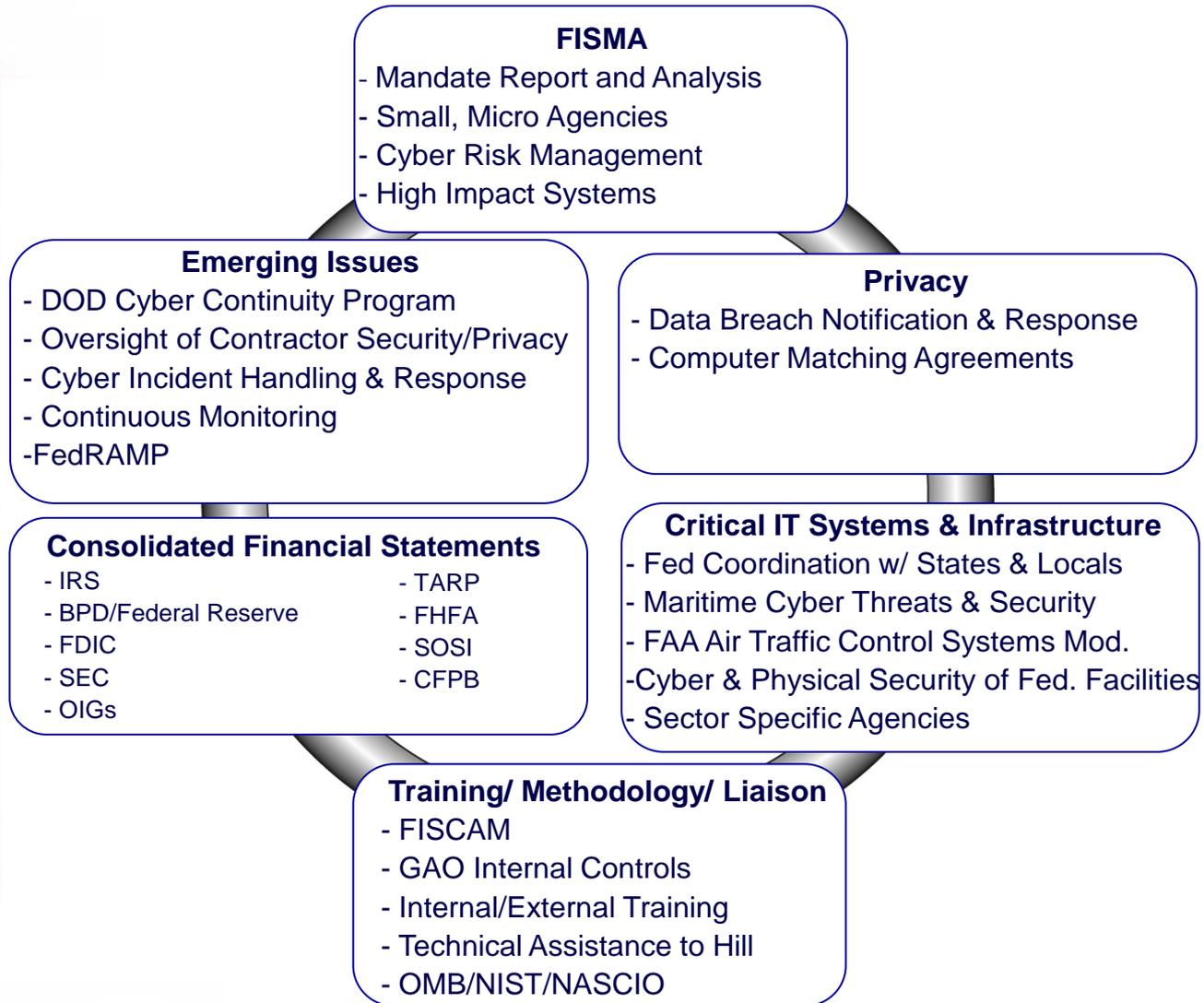|	
Equipment	7,664 (16.6%)
Policy Violation	8,888 (19.3%)
Non Cyber	13,256 (28.8%)
Suspicious Network Activity	2,287 (5.0%)
Unauthorized Access	340 (0.7%)
Denial of Service (DoS)	23 (0.0%)
Malicious Code (Malware)	8,085 (17.6%)
Improper Usage	684 (1.5%)
Social Engineering	2,398 (5.2%)
Other	2,418 (5.3%)
Grand Total	**46,043 (100.0%)**

Key Challenges to Enhancing Cybersecurity

- Designing and implementing risk-based information security programs at federal agencies
- Establishing and identifying standards for critical infrastructures
- Detecting, responding to, and mitigating cyber incidents
- Promoting education, awareness, and workforce planning
- Supporting cyber research and development
- Securing use of new technologies
- Managing risks to global IT supply chain
- Addressing international cyberspace challenges

Ongoing and Planned Work

FISMA
- Mandate Report and Analysis
- Small, Micro Agencies
- Cyber Risk Management
- High Impact Systems

Emerging Issues
- DOD Cyber Continuity Program
- Oversight of Contractor Security/Privacy
- Cyber Incident Handling & Response
- Continuous Monitoring
- FedRAMP

Privacy
- Data Breach Notification & Response
- Computer Matching Agreements

Consolidated Financial Statements
- IRS
- BPD/Federal Reserve
- FDIC
- SEC
- OIGs
- TARP
- FHFA
- SOSI
- CFPB

Critical IT Systems & Infrastructure
- Fed Coordination w/ States & Locals
- Maritime Cyber Threats & Security
- FAA Air Traffic Control Systems Mod.
- Cyber & Physical Security of Fed. Facilities
- Sector Specific Agencies

Training/ Methodology/ Liaison
- FISCAM
- GAO Internal Controls
- Internal/External Training
- Technical Assistance to Hill
- OMB/NIST/NASCIO

Sense of the Information Security Community

1. Do you believe effective implementation of the administration's cybersecurity priorities (continuous monitoring, strong authentication, and TIC) will greatly improve cybersecurity within the federal government?

Sense of the Information Security Community

2. Do you believe your agency has effectively developed *and* implemented a continuous monitoring or continuous diagnostic and mitigation strategy?

Sense of the Information Security Community

3. Do you believe your agency has sufficient oversight, awareness, and ability to ensure effective information security and privacy controls over systems operated and information processed by contractors or other third parties on the agency's behalf?

Sense of the Information Security Community

4. Do you believe cybersecurity is receiving the appropriate attention by your agency head?

Sense of the Information Security Community

5. Do you believe audits and evaluations of agency information security programs and practices help to improve security? Are detrimental to security? Or both?

Sense of the Information Security Community

6. Do you believe FISMA the law and/or NIST implementing guidelines need to be changed?

Recent GAO Reports

- GAO-13-275, *Communications Networks: Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts* (April 2013)

- GAO-13-462T, *Cybersecurity: A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges* (March 2013)

- GAO-13-350, *Information Security: IRS Has Improved Controls but Needs to Resolve Weaknesses* (March 2013)

- GAO-13-187, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented* (Feb. 2013)

Recent GAO Reports (cont.)

- GAO-13-155, *Information Security: Federal Communications Commission Needs to Strengthen Controls over Enhanced Secured Network Project* (January 2013)

- GAO-13-63, *Information Security: Actions Needed by Census Bureau to Address Weaknesses* (January 2013)

- GAO-12-903, *Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy* (September 2012)

- GAO-12-757, *Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged* (Sept. 2012)

Recent GAO Reports (cont.)

- GAO-12-816, *Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices* (August 2012)

- GAO-12-961T, *Privacy: Federal Law Should Be Updated to Address Changing Technology Landscape* (July 2012)

- GAO-12-926T, *Cybersecurity: Challenges in Securing the Electricity Grid* (July 2012)

- GAO-12-696, *Information Security: Environmental Protection Agency Needs to Resolve Weaknesses* (July 2012)

- GAO-12-876T, *Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage* (June 2012)

Questions

Contacts

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

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