GAO Information Security Update

Presented to

Federal Computer Security Program Managers' Forum

August 26, 2015

Agenda

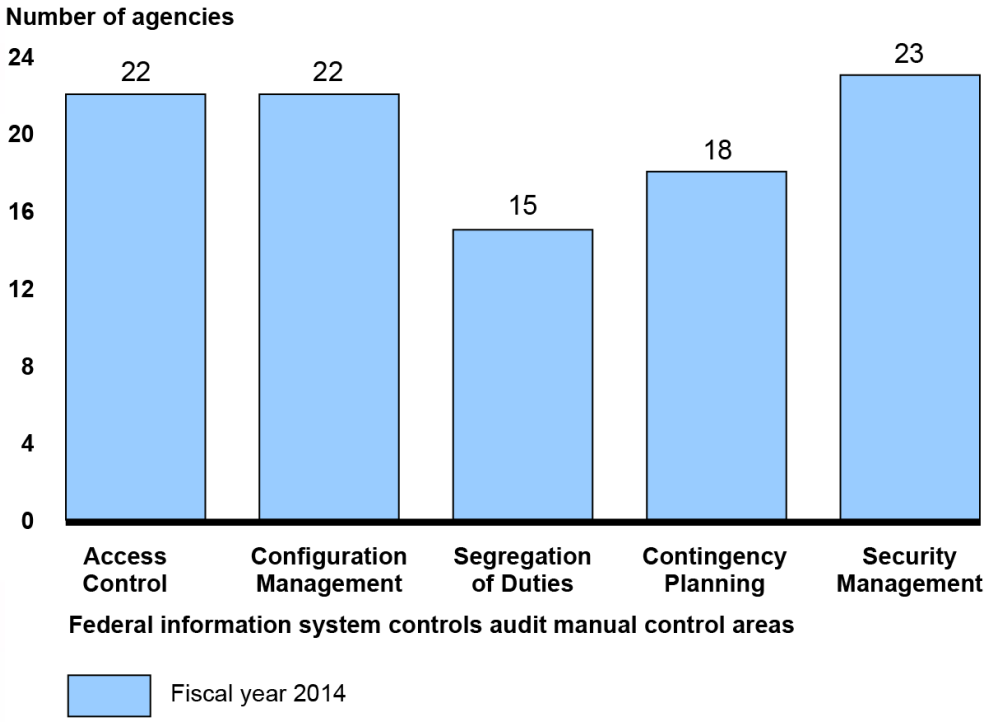
- Snapshots of Federal Information Security
- Ongoing and Planned Work
- Sense of the Information Security Community
- Recent GAO Reports
- Questions

Agencies largely report increases in security capabilities

Capability Area	FY 2013	FY 2014
Automated Asset Management Information Security Continuous Monitoring (ISCM)	83%	96%
Automated Configuration Management (ISCM)	79%	86%
Automated Vulnerability Management (ISCM)	81%	94%
Trusted Internet Connections Traffic Consolidation	86%	95%
Personal Identity Verification Logical Access (HSPD-12)	67%	72%
Remote Access Authentication	79%	77%
Portable Device Encryption	84%	55%
Email Encryption	51%	54%
User Security Training	94%	93%
Users with Security Responsibility Training	92%	80%

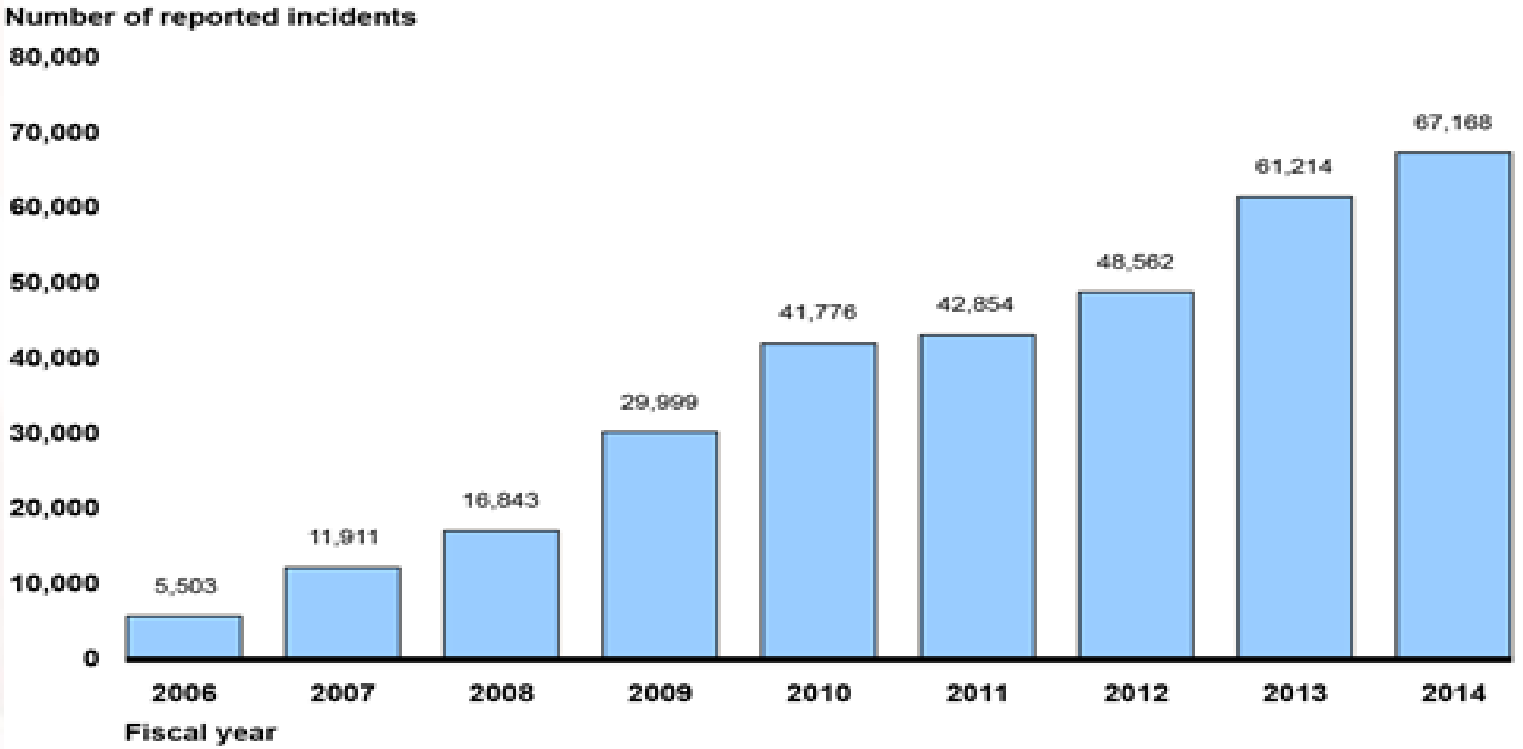
Source: Data reported to DHS via CyberScope from October 1, 2012 to September 30, 2013 and OMB's May 1, 2015 annual report to Congress.

Agencies experienced weaknesses in information security controls



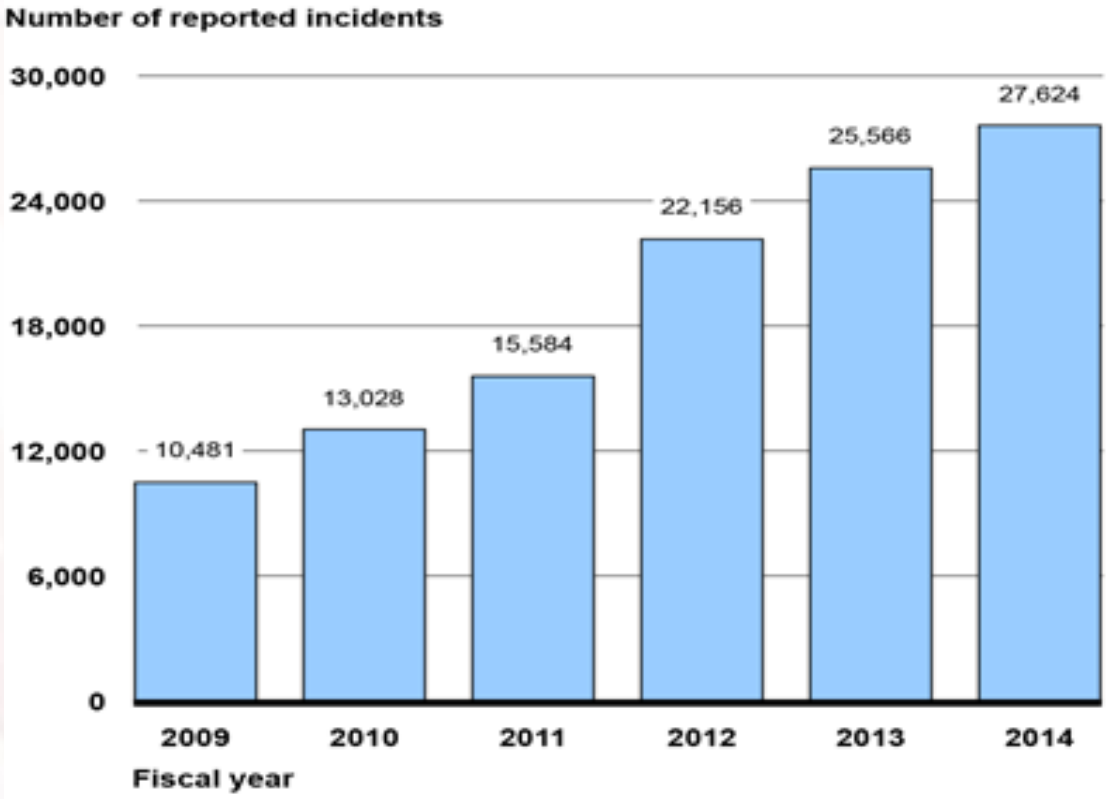
Source: GAO analysis of agency, inspectors general, and GAO reports.

Reported security incidents continue to rise



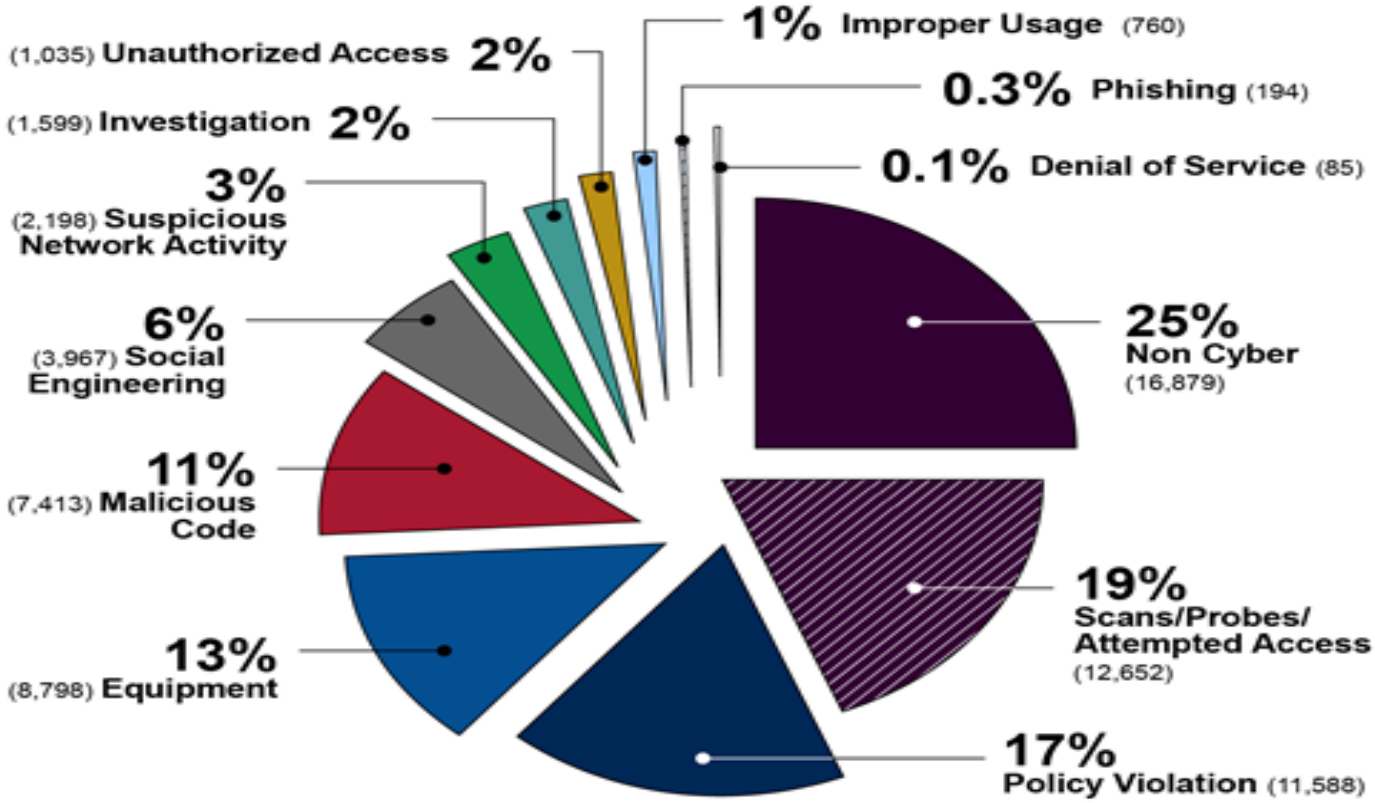
Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2006-2014. | GAO-15-714

Reported PII incidents are also increasing



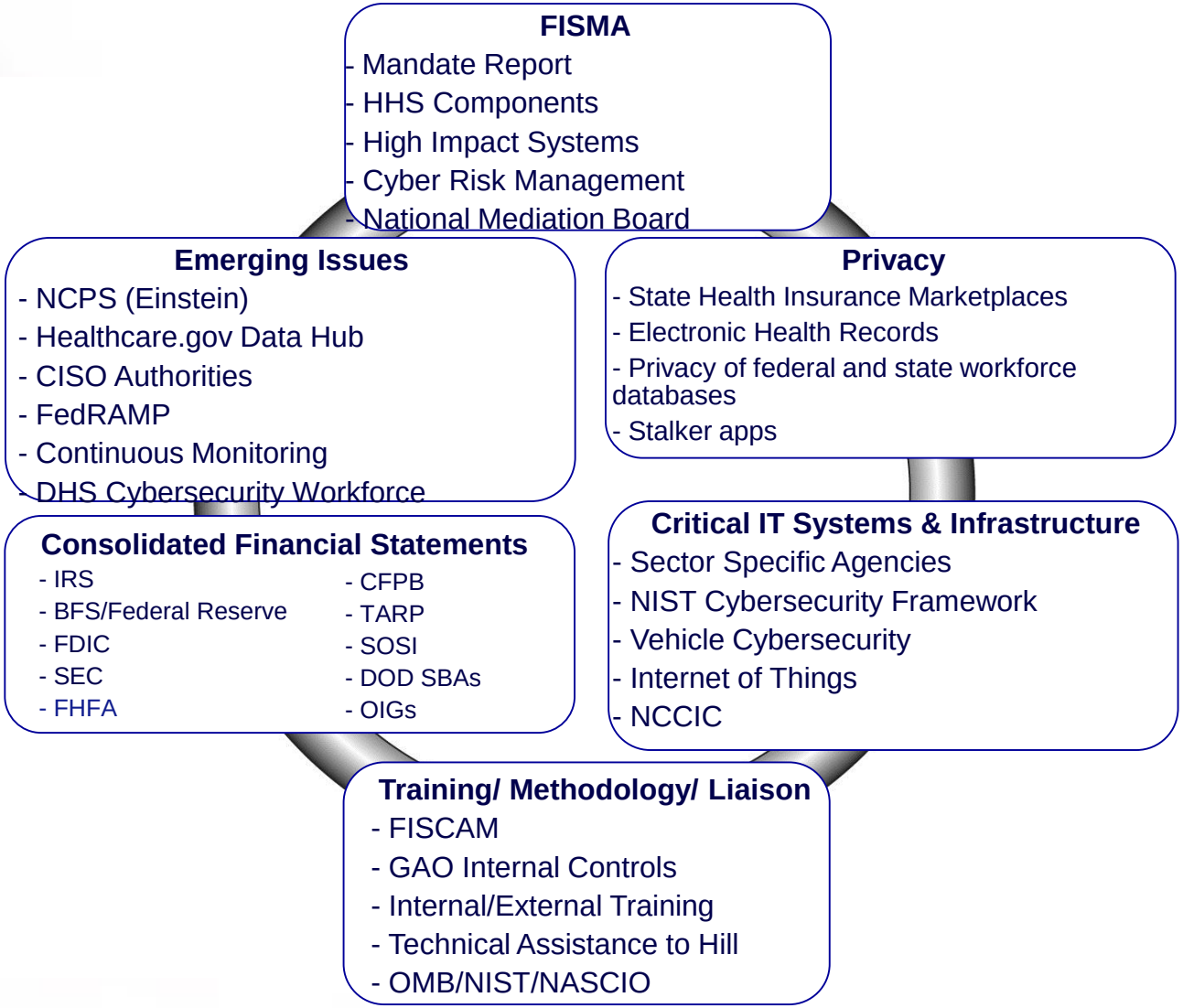
Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2009-2014. | Product #

Agencies reported a variety of incidents



Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal year 2014. | GAO-15-714

Ongoing and Planned Work



Ongoing and Planned Work – FISMA-related

- Mandated Report
- HHS Components (FDA, CDC, NIH)
- High Impact Systems (NASA, NRC, OPM, VA)
- Cyber Risk Management
- National Mediation Board

Ongoing and Planned Work – Emerging Issues

- National Cybersecurity Protection System (Einstein)
- Healthcare.gov Data Hub
- CISO Authorities
- FedRAMP
- Continuous Monitoring
- DHS Cybersecurity Workforce

Ongoing and Planned Work – Consolidated Financial Statements

- IRS
- BFS / Federal Reserve
- FDIC
- SEC
- FHFA
- CFPB
- TARP
- SOSI
- DOD Statements of Budget Activity (Army, Navy, AF)
- OIGs

Ongoing and Planned Work – Critical IT Systems & Infrastructure

- Sector Specific Agencies
- NIST Cybersecurity Framework
- Vehicle Cybersecurity
- Internet of Things
- National Cybersecurity and Communications Integration Center

Ongoing and Planned Work – Privacy-related

- State Health Insurance Marketplaces (CA, KY, VT)
- Electronic Health Records
- Privacy of Federal and State Workforce Databases
- Stalker Apps

Sense of the Information Security Community

1. Does your agency currently have the capability to successfully implement CDM? Will it be an improvement over current continuous monitoring activities at your agency?

Sense of the Information Security Community

2. Are you currently where you need to be regarding implementation of PIV cards or other multi-factor authentication?

Sense of the Information Security Community

3. Was this summer's cybersecurity sprint a useful exercise for improving information security at your agency?

Sense of the Information Security Community

4. What are the three biggest challenges you face in securing your agency's computer networks and systems?

Sense of the Information Security Community

5. How can GAO and OIGs improve their audits and evaluations of information security practices to better assist you in securing your computer networks and systems?

Recent GAO Reports

- GAO-15-758T, Information Security: Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies (July 2015)
- GAO-15-725T, Cybersecurity: Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies (June 2015)
- GAO-15-621, Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law (July 2015)
- GAO-15-573T, Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems (April 2015)

Recent GAO Reports

- GAO-15-544, Insider Threats: DOD Should Strengthen Management and Guidance to Protect Classified Information and Systems (June 2015)
- GAO-15-509, Cybersecurity: Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information (July 2015)
- GAO-15-426, Information Security: FDIC Implemented Many Controls over Financial Systems but Opportunities for Improvement Remain (April 2015)
- GAO-15-370, Air Traffic Control: FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen (April 2015)

Recent GAO Reports

- GAO-15-337, Information Security: IRS Needs to Continue Improving Controls over Financial and Taxpayer Data (March 2015)
- GAO-15-290, High-Risk Series: An Update (February 2015)
- GAO-15-221, Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems (January 2015)
- GAO-15-177, Information Security: VA Needs to Address Identified Vulnerabilities (November 2014)
- GAO-15-6, Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems (December 2014)

Questions

Contact

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