GAO Information Security Update

Presented to

Federal Computer Security Program Managers' Forum

August 20, 2014

Agenda

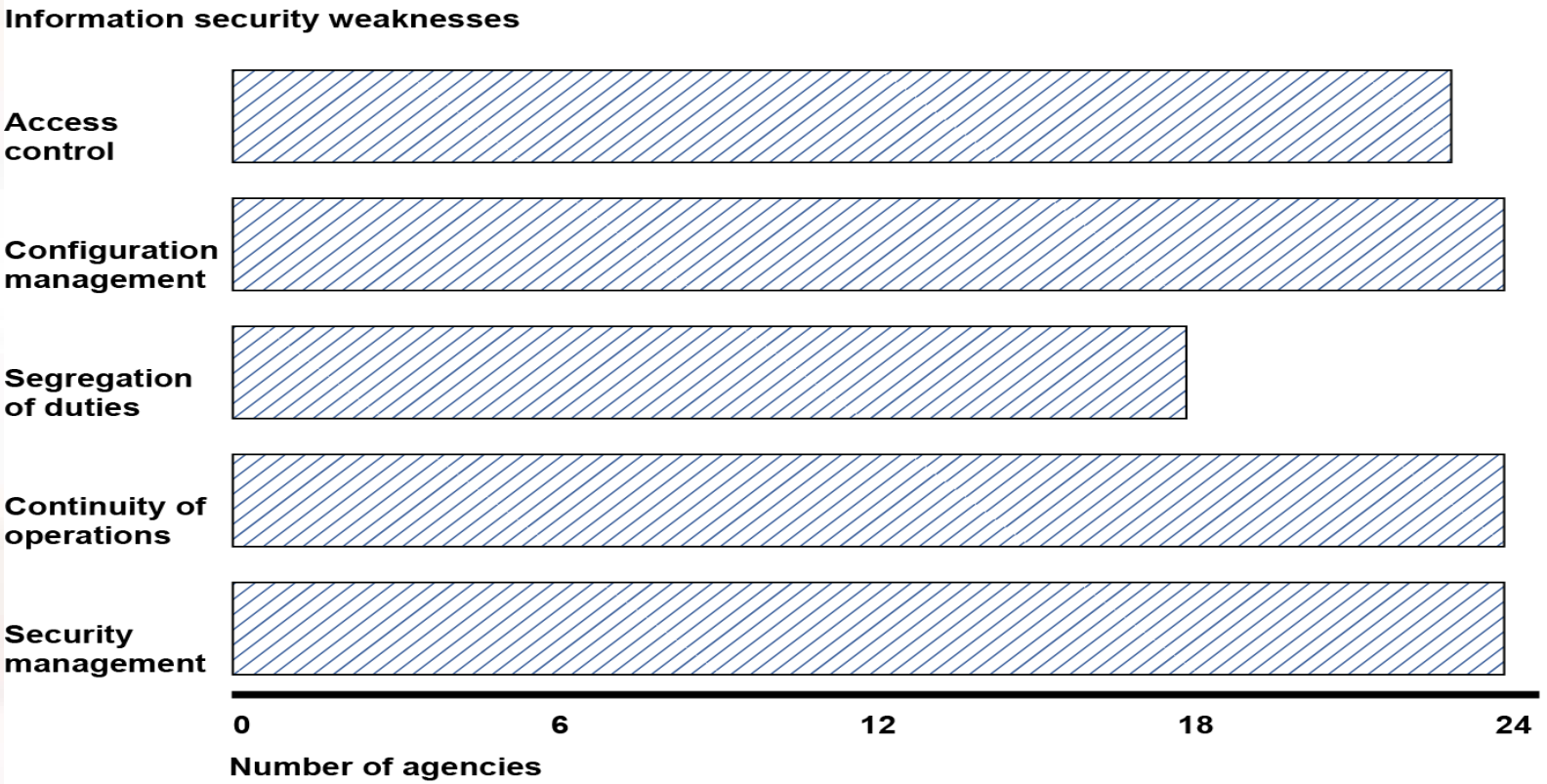
- Snapshots of Federal Information Security
- Ongoing and Planned Work
- Sense of the Information Security Community
- Recent GAO Reports
- Questions

Agencies largely report increases in security capabilities

Capability Area	FY 2012	FY 2013
Automated Asset Management Information Security Continuous Monitoring (ISCM)	86%	83%
Automated Configuration Management (ISCM)	70%	79%
Automated Vulnerability Management (ISCM)	83%	81%
Trusted Internet Connections Traffic Consolidation	81%	86%
Personal Identity Verification Logical Access (HSPD-12)	57%	67%
Portable Device Encryption	90%	84%
Remote Access Encryption	82%	98%
Email Encryption	35%	51%
User Security Training	88%	94%
Users with Security Responsibility Training	92%	92%

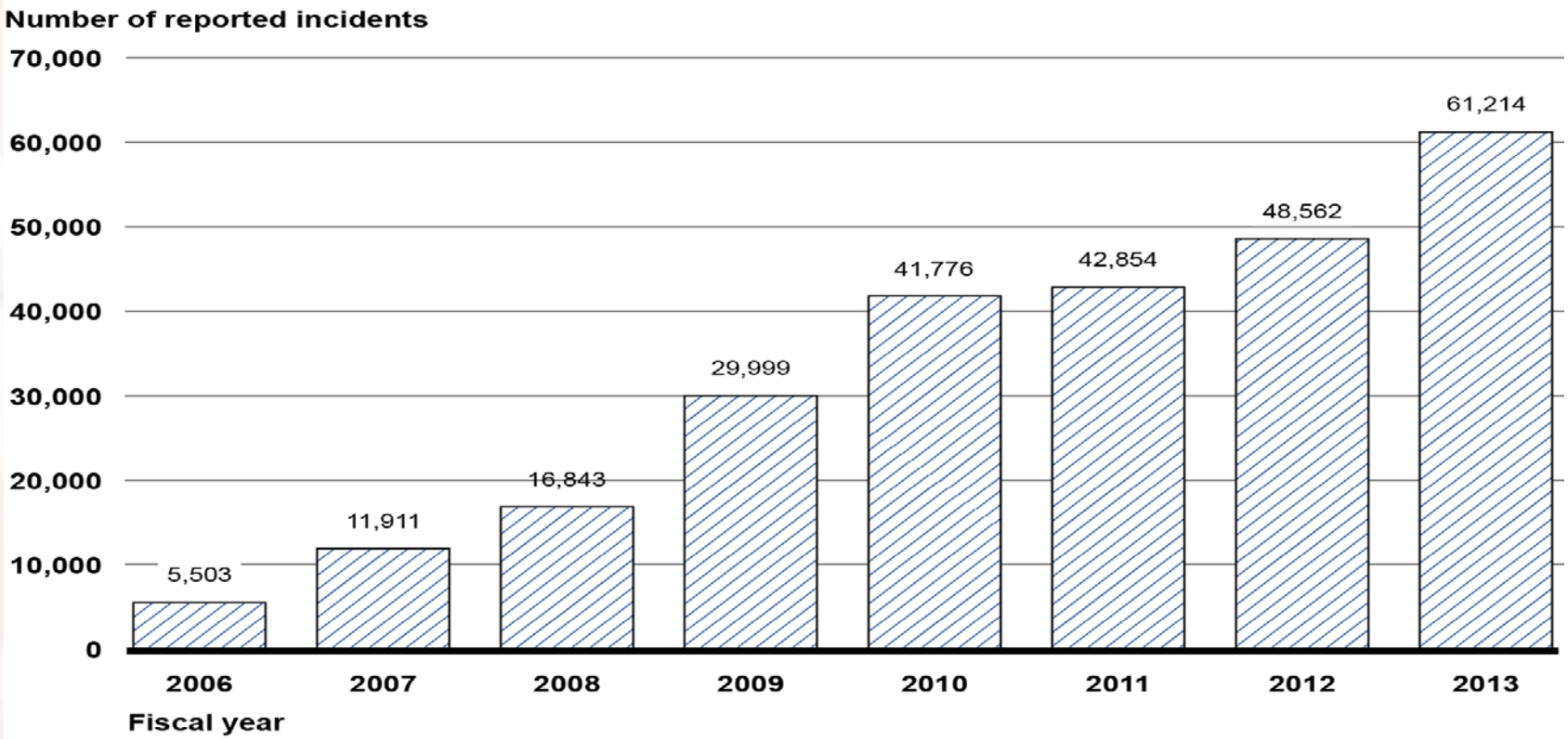
Source: Data reported to DHS via CyberScope from October 1, 2012 to September 30, 2013 and OMB's May 1, 2014 annual report to Congress.

Agencies experienced weaknesses in information security controls



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

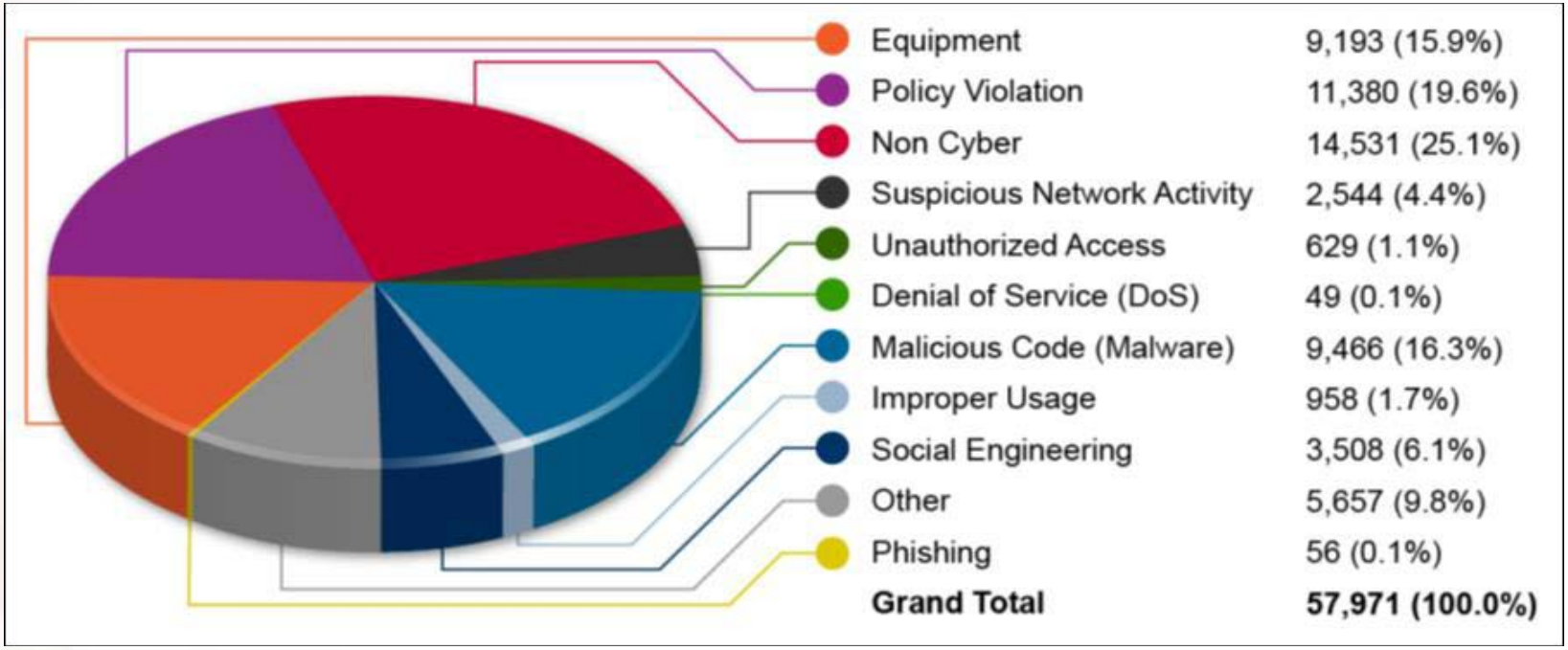
Reported security incidents continue to rise



Source: GAO analysis of US-CERT data for fiscal years 2006-2013.

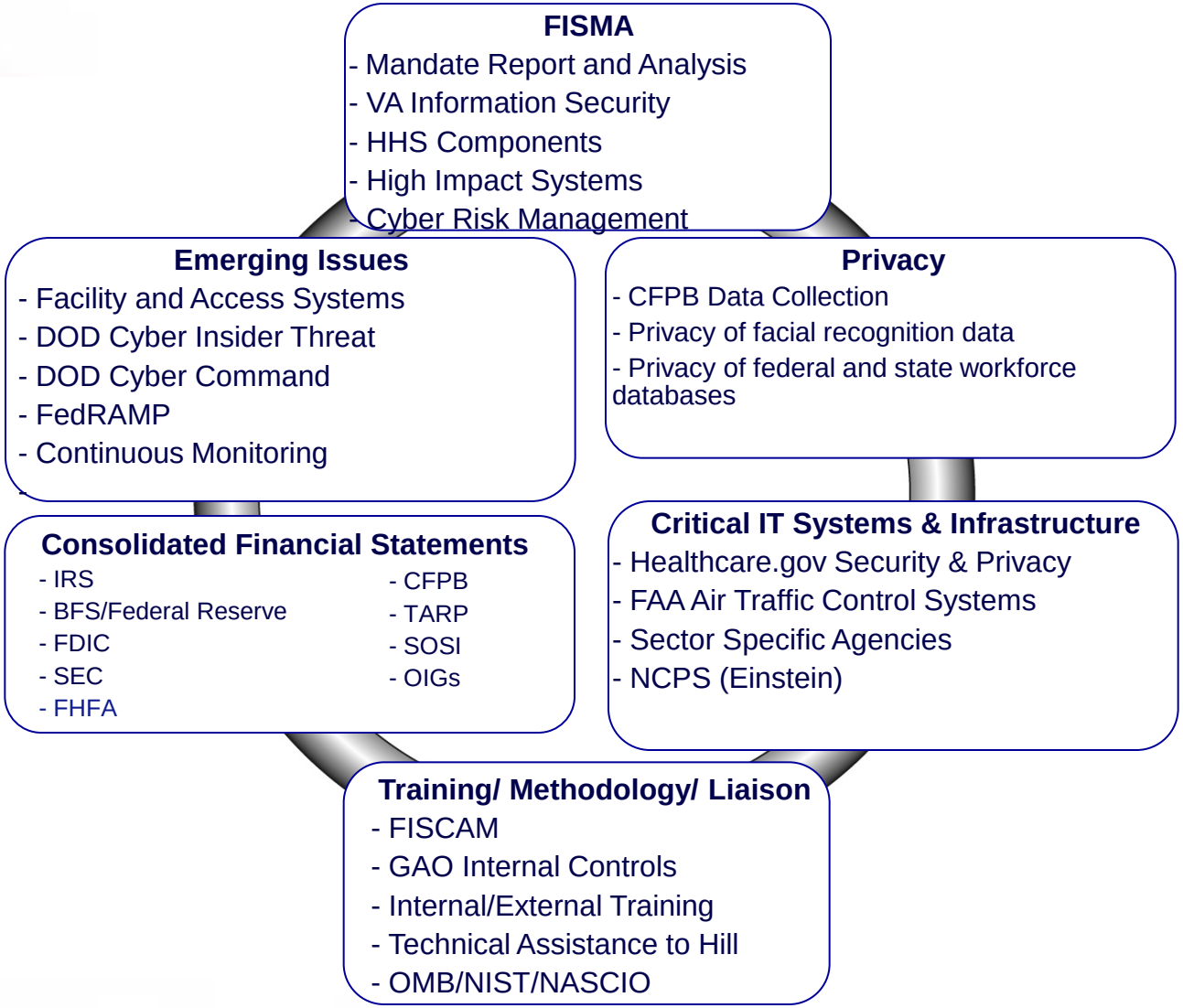
Agencies reported a variety of incidents

Summary of CFO Act Agency Incidents Reported to US-CERT in FY 2013



Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013 and OMB's May 1, 2014 annual report to Congress.

Ongoing and Planned Work



Ongoing and Planned Work – FISMA-related

- Mandated Report
- VA Information Security
- HHS Components
- High Impact Systems
- Cyber Risk Management

Ongoing and Planned Work – Emerging Issues

- Facility and Access Systems
- DOD Cyber Insider Threat
- DOD Cyber Command
- FedRAMP
- Continuous Monitoring

Ongoing and Planned Work – Consolidated Financial Statements

- IRS
- BFS / Federal Reserve
- FDIC
- SEC
- FHFA
- CFPB
- TARP
- SOSI
- OIGs

Ongoing and Planned Work – Critical IT Systems & Infrastructure

- Healthcare.gov Security & Privacy
- FAA Air Traffic Control Systems
- Sector Specific Agencies
- National Cybersecurity Protection System (Einstein)

Ongoing and Planned Work – Privacy-related

- CFPB Data Collection Security & Privacy
- Privacy of Facial Recognition Data
- Privacy of Federal and State Workforce Databases

Sense of the Information Security Community

1. Has your agency's continuous monitoring processes generated tangible benefits to the assessment and authorization of systems? To the resolution of identified vulnerabilities?

Sense of the Information Security Community

2. If your agency has migrated some of its systems to a cloud environment, does your agency have a clear understanding of how the data is protected in transit or at rest, and where such data resides (e.g. in the U.S. or overseas)?

Sense of the Information Security Community

3. Has your agency's continuous monitoring efforts been aided, hindered, or unaffected by cloud computing?

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-14-674, *Information Security:* FDIC Made Progress in Securing Key Financial Systems, but Weaknesses Remain (July 2014)
- GAO-14-344, *Information Security:* Additional Oversight Needed to Improve Programs at Small Agencies (June 2014)
- GAO-14-354, *Information Security:* Agencies Need to Improve Cyber Incident Response Practices (April 2014)
- GAO-14-419, *Information Security:* SEC Needs to Improve Controls over Financial Systems and Data (April 2014)

Recent GAO Reports

- GAO-14-405, *Information Security:* IRS Needs to Address Control Weaknesses That Place Financial and Taxpayer Data at Risk (April 2014)
- GAO-14-487T, *Information Security:* Federal Agencies Need to Enhance Responses to Data Breaches (April 2014)
- GAO-14-469T, *Information Security:* VA Needs to Address Long-Standing Challenges (March 2014)
- GAO-14-125, *Critical Infrastructure Protection:* More Comprehensive Planning Would Enhance the Cybersecurity of Public Safety Entities' Emerging Technology (January 2014)

Recent GAO Reports

- GAO-14-44, *Computer Matching Act:* OMB and Selected Agencies Need to Ensure Consistent Implementation (January 2014)
- GAO-14-34, *Information Security:* Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent (December 2013)
- GAO-13-776, *Federal Information Security:* Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness (September 2013)

Questions

Contacts

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

Larry Crosland
Assistant Director, Information Security Issues
CroslandL@gao.gov