FY 2013 FISMA Report

Office of Management and Budget

March 2013

FY 2013 FISMA Report

- **Section II: Key Ongoing Information Security Initiatives**

  Describes the efforts being undertaken to protect government data and IT infrastructure assets, support the safe and secure adoption of emerging technology, and building a 21st century workforce.

- **Section III: Key Security Metrics**

  Presents the metrics used to assess the implementation of security capabilities, measure their effectiveness, and ascertain their impact on risk levels.

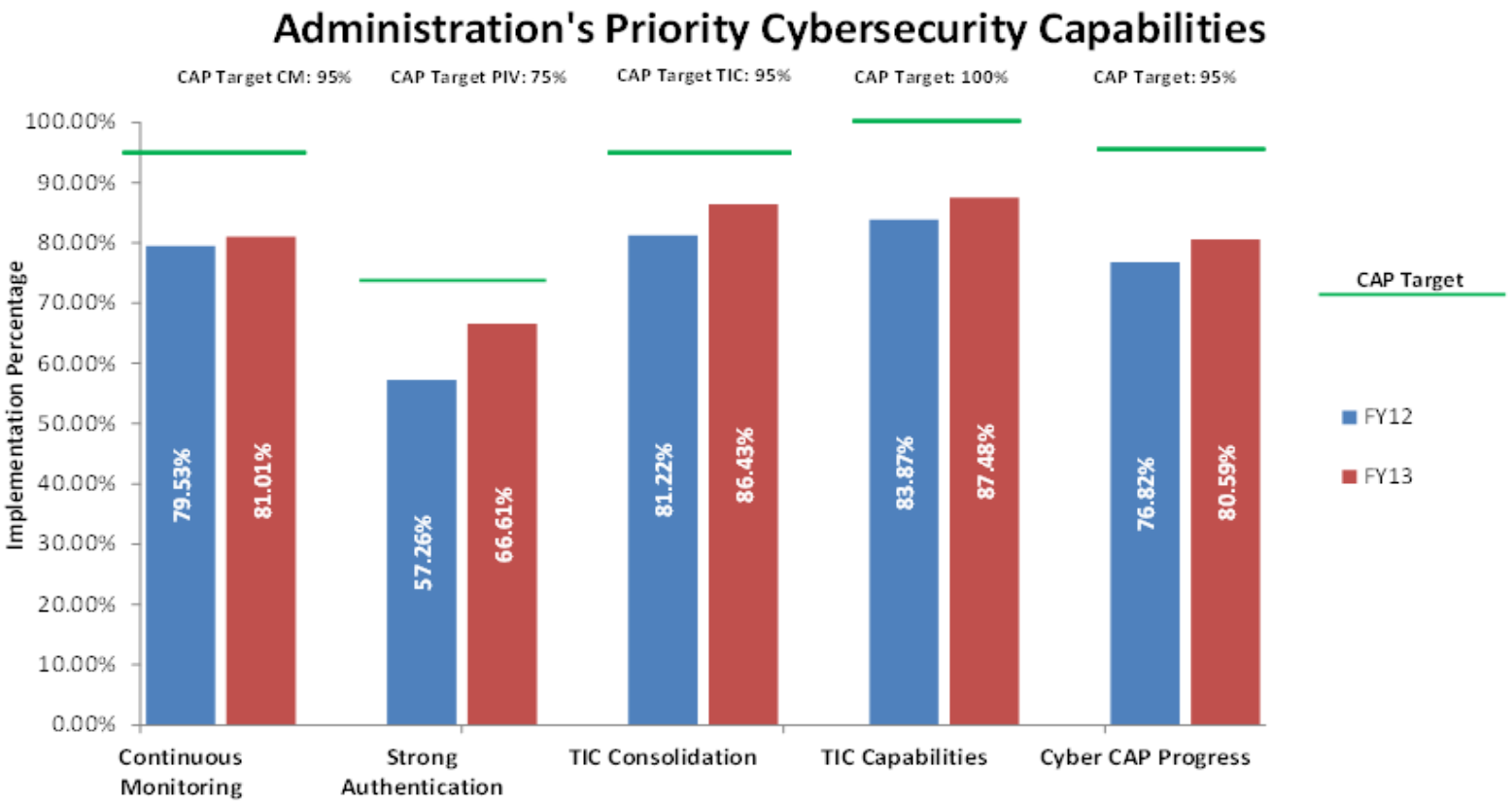
- **Section IV: Security Incidents and Response in the Federal Government**

  Presents information from the United States Computer Emergency Readiness Team (US-CERT) on computer security incidents and Federal efforts to remediate them.

Ongoing Information Security Initiatives

- Maintain focus on key strategies through the implementation of the Cyber CAP Goal
- Support the safe and secure adoption of emerging technologies such as mobile devices and cloud-based computing
- Build a sophisticated information security workforce by attracting and retaining capable personnel

Cross Agency Priority Cybersecurity Goal



Note:

- Continuous Monitoring is comprised of the following capability areas: Automated Asset Management, Automated Configuration Management, and Automated Vulnerability Management.
- Strong Authentication is comprised of the PIV Logical Access (HSPD-12) capability area.
- TIC Consolidation is comprised of the capability area TIC Traffic Consolidation.
- TIC Capabilities is comprised of the capability area TIC 2.0 Capabilities (Includes Einstein 2).
- Cyber CAP Progress represents an average of: Continuous Monitoring, Strong Authentication, TIC Consolidation and TIC Capabilities.

FISMA Capabilities FY 2012 vs. FY 2013

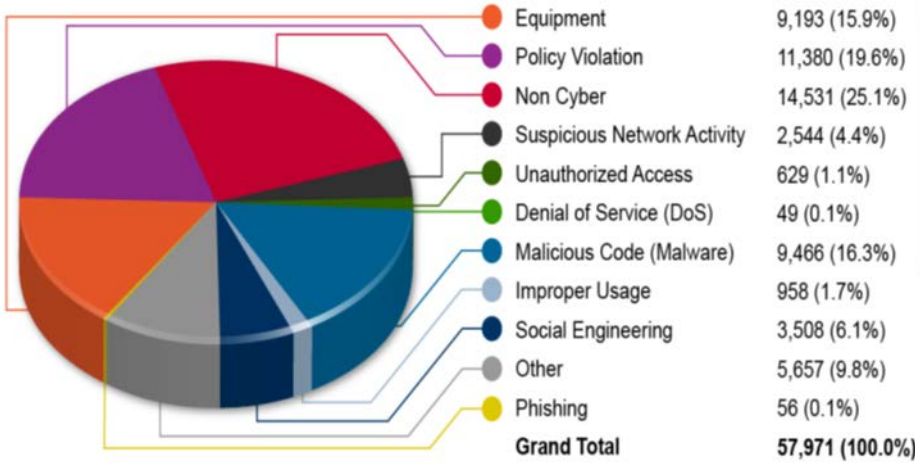
Capability Area	FY 2012	FY 2013
Automated Asset Management	86%	83%
Automated Configuration Management	70%	79%
Automated Vulnerability Management	83%	81%
TIC Traffic Consolidation	81%	86%
TIC 2.0 Capabilities (Includes Einstein 2)	84%	87%
PIV Logical Access	57%	67%
Portable Device Encryption	90%	84%
DNSSEC Implementation	74%	93%
E-Mail Validation Technology	64%	74%
Remote Access Authentication	53%	79%
Remote Access Encryption	82%	98%
Controlled Incident Detection	63%	73%
User Training	88%	94%
Users with Security Responsibility Training	92%	92%
Detect and Block Unauthorized Software	60%	73%
Email Encryption	35%	51%
Government-Wide Average	73%	81%

Metrics for Cross Agency Priority Goals

Note: Capability areas determined to be high priority by OMB and NSC staff.

Summary of Agency Reported Incidents

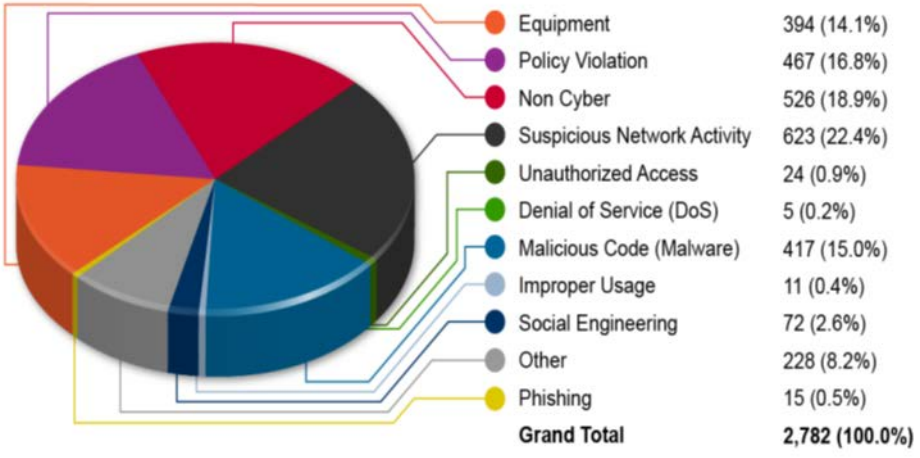
Summary of CFO Act Agency Incidents



Highlights

- Equipment, Policy Violations, Non Cyber, Malicious Code, and Social Engineering Incidents account for 83% of all Incidents
- More serious Incidents, such as Unauthorized Access and DoS attacks are <2%

Summary of Non-CFO Act Agency Incidents



Highlights

- Equipment, Policy Violations, Non Cyber Suspicious Activity and Malicious Code Incidents account for 87% of all Incidents
- More serious Incidents, such as Unauthorized Access and DoS attacks are <1%

Information Security Spending Reported by CFO Act Agencies

Agency Information Security Spending by Major Category ($ in millions), FY 2013 Actual

Agency	Prevent Malicious Cyber Activity	Detect, Analyze, and Mitigate Intrusions	Shape the Cybersecurity Environment	Total
Dept. of Agriculture	$39	$23	$1	$63
Dept. of Commerce	$47	$74	$42	$163
Dept. of Education	$11	$11	$0	$22
Dept. of Energy	$112	$69	$37	$218
Dept. of Justice	$105	$335	$6	$446
Dept. of Labor	$5	$9	$9	$23
Dept. of State	$51	$30	$5	$86
Dept. of Transportation	$44	$48	$5	$96
Dept. of Veterans Affairs	$11	$102	$7	$121
Dept. of the Interior	$13	$24	$1	$38
Dept. of the Treasury	$146	$109	$13	$268
Dept. of Defense	$2,471	$1,055	$3,580	$7,106
Dept. of Health & Human Services	$44	$111	$26	$181
Dept. of Homeland Security	$369	$590	$150	$1,109
Dept. of Housing & Urban Development	$4	$7	$0	$12
Environmental Protection Agency	$1	$19	$0	$20
General Services Administration	$28	$10	$8	$46
International Assistance Programs	$8	$7	$7	$22
National Science Foundation	$3	$6	$141	$150
NASA	$27	$40	$19	$86
Nuclear Regulatory Commission	$4	$10	$3	$17
Office of Personnel Management	$2	$5	$0	$7
Small Business Administration	$1	$4	$0	$5
Social Security Administration	$27	$11	$2	$40
Total Information Security Spending	**$3,575**	**$2,707**	**$4,063**	**$10,344**

Key Next Steps in 2014

- OMB and DHS will continue implementation of M-14-03, "Enhancing the Security of Federal Information and Information Systems," to ensure agencies manage information security risk on a continuous basis.
- OMB/NSC, with support from DHS, will develop outcome-based metrics for the FY 2015-FY 2017 CAP Goal metrics:
  - Information Security Continuous Monitoring
  - Phishing and Malware Defense
  - Identity, Credential, and Access Management (ICAM)
- DHS will continue with the rollout of EINSTEIN 3 Accelerated (E3A) and securing memorandums of agreement (MOAs) with all departments and agencies.
- DHS is working to develop the cyber workforce by providing an evolving, robust collection of trainings online that map to the workforce development framework.
- OMB, NSC, and DHS will continue CyberStat sessions.

Appendix Slides

Cross Agency Priority (CAP) Goals

- **Continuous Monitoring**
  - Goal: Determine if deployed security controls remain effective over time in light of the inevitable hardware and software changes that occur.
  - Objective: Transform a static security control assessment and risk determination process into a dynamic system that provides essential, near-real-time, security-status-related information.
  - Result: Be able to take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding network operations.
- **Trusted Internet Connections (TIC)**
  - Goal: Improve the Federal Government's network security posture.
  - Objective: Consolidate external internet connections
  - Result: Enhanced monitoring and situational awareness of all external network connections. Enhanced detection and intrusion prevention capabilities against cyber attacks.
- **Authentication – HSPD 12**
  - Goal: Establish consistent, logical access control policy for federal computer networks.
  - Objective: Implement HSPD-12, which requires agencies to follow specific standards and processes for using Federal Personal Identity Verification (PIV) smartcard credentials. PIVs will be used pursuant to standardized background investigations to verify employees' and contractors' identities, and enable network authentication
  - Result: Robust, multi-factor authentication, digital signature, and encryption capabilities on all federal networks.