Cross Agency Priority Goal

Cybersecurity

Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator; Alejandro Mayorkas, Deputy Secretary, Department of Homeland Security; Bob Work, Deputy Secretary, Department of Defense

FY2014 Quarter 4

Overview

Goal Statement

Improve awareness of security practices, vulnerabilities, and threats to the operating environment, by limiting access to only authorized users and implementing technologies and processes that reduce the risk from malicious activity.

Urgency

The President has identified the Cybersecurity threat as one of the most serious national security, public safety, and economic challenges we face as a nation. Ultimately, the Cybersecurity challenge in Federal government is not just a technology issue. It is also an organizational, people, and performance issue requiring creative solutions to address emerging and increasingly sophisticated threats, and new vulnerabilities introduced by rapidly changing technology.

Vision

Implement the Administration's priority Cybersecurity capabilities and develop performance based metrics to measure their success. The Administration's priority Cybersecurity capabilities are:

- **Information Security Continuous Monitoring Mitigation (ISCM)** – Provide ongoing observation, assessment, analysis, and diagnosis of an organization's Cybersecurity: posture, hygiene, and operational readiness.
- **Identity, Credential, and Access Management (ICAM)** – Implement a set of capabilities that ensure users must authenticate to information technology resources and have access to only those resources that are required for their job function.
- **Trusted Internet Connection (TIC)** – Protect the data and information entering and exiting Federal networks; Identify network connections that may pose a security risk to mission success.

Progress Update

CFO Act Agencies*

- Federal Cyber CAP goal performance increased 3.89% this Quarter at 89%.
- TIC compliance increased by another 1.90% and now stands at 93%.
- TIC 2.0 security capabilities increased by 0.22% and now stands at 92%.
- TIC traffic consolidation increased 3.57% and has now exceeded the CAP goal at 95%.
- Information Security Continuous Monitoring Mitigation improved 4.05% as growth was seen in every capability area to 92%
    - Asset Management 0.87% (Q4 FY2014: 96 %)
    - Configuration Management 6.19% (Q4 FY2014: 86%)
    - Vulnerability Management 5.07% (Q4 FY2014: 94%)
- Strong Authentication for logical access increased 7.41% (Q4 FY2014: 72%).

Strong Authentication Details

- The Civilian CFO Act Agencies increased their use of PIV cards for logical access by 10.83% to 41.01%.
- 9 agencies had double digit increases.
- 7 agencies now exceed the CAP goal target of 75%.
- 16 now report at 10% or greater.
- 5 agencies remain at 0% for PIV implementation.

* - All agencies denoted by 31 U.S.C. 901 (b) participate in the Cybersecurity CAP Goal reporting process.

Action Plan Summary

Sub-Goal	Major Actions to Achieve Impact	Key Indicator/Metrics
Information Security Continuous Monitoring:	• Understand the risks posed by hardware and software on Federal networks; • Maintain ongoing, near real-time awareness of information security risks and rapidly respond to support organizational risk management decisions.	• Assets: % of assets in 2.1* where an automated capability (device discovery process) provides visibility at the organization's enterprise level into asset inventory information for all hardware assets. • Configurations: % of the applicable hardware assets (per question 2.1*), of each kind of operating system software in 3.1*, has an automated capability to identify deviations from the approved configuration baselines identified in 3.1.1* and provide visibility at the organization's enterprise level. • Vulnerability: % of hardware assets identified in section 2.1* that are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization's enterprise level.
Strong Authentication (Identity, Credential, and Access Management):	• Ensure only authorized employees have access to Federal information systems; • Ensure only authorized employees have access to information needed for designated business functions.	• % of ALL people required to use Personal Identity Verification (PIV) Card to authenticate (5.2.5 & 5.4.5)*
Trusted Internet Connections (TIC):	• Protect data and information entering and exiting Federal networks; • Identify network connections that may pose a security risk to mission success.	• % of external network traffic passing through a Trusted Internet Connection (Excludes DOD). • % of required TIC capabilities implemented by TIC(s) used by the organization. (7.1 & 7.2)*
Anti-Phishing & Malware Defense:	• Implement technologies, processes and training to reduce the risk of malware introduced through email and malicious or compromised web sites.	• TBD in FY2015.

* - Referencing Question numbers in the FY14 CIO Annual FISMA Metrics document (http://www.dhs.gov/publication/fy14-fisma-documents)

Work Plan

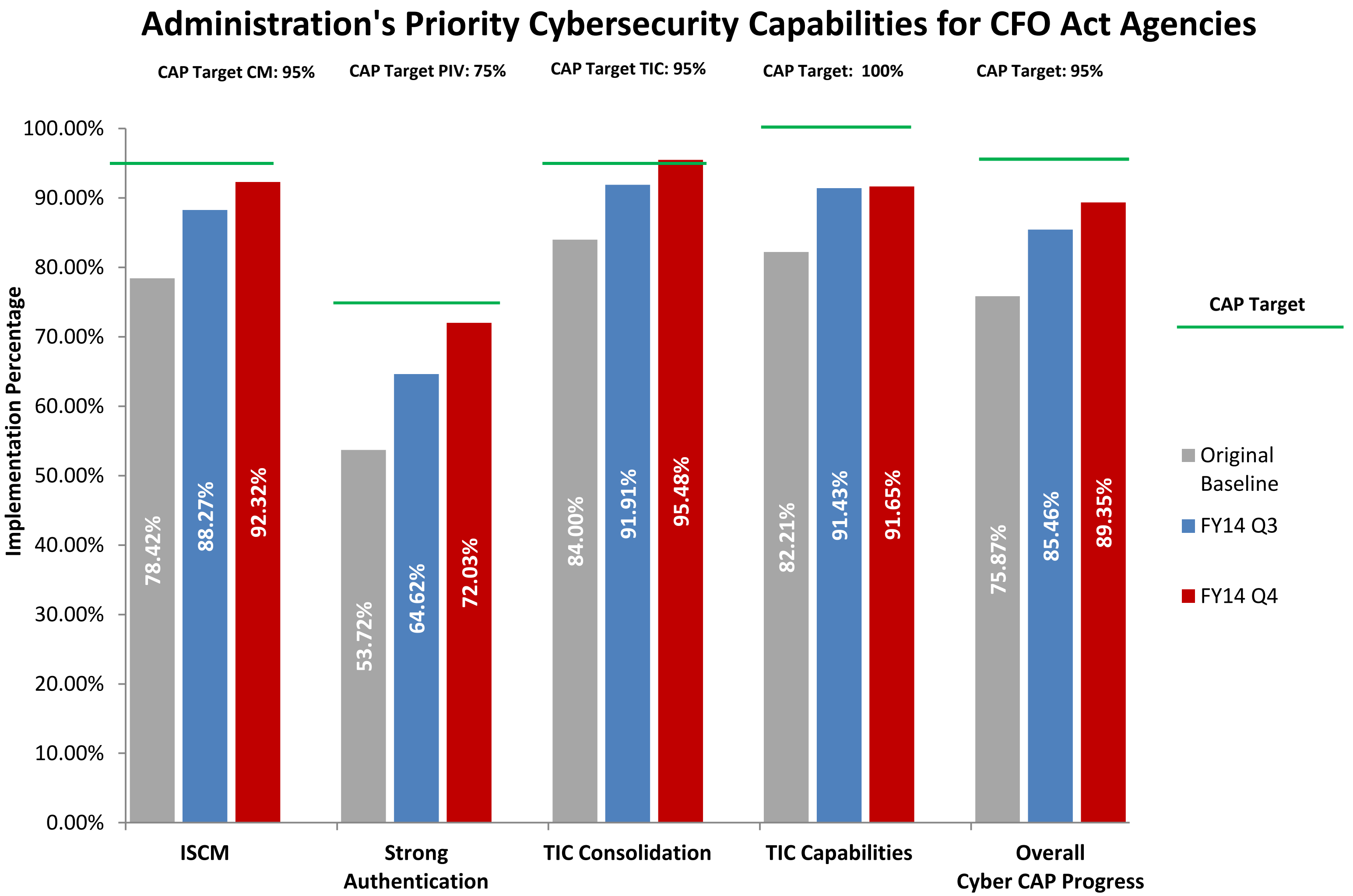
Milestone Summary			
Key Milestones	**Milestone Date**	**Milestone Status**	**Issues / Comments**
FY15 CIO FISMA Annual/CAP metrics published	10/03/14	Complete	http://www.dhs.gov/publication/fy15-fisma-documents
OMB FY14/15 FISMA Reporting Memo released	10/03/14	Complete	http://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-01.pdf
FY15 Q1 FISMA/CAP metrics published	11/14/14	Complete	http://www.dhs.gov/publication/fy15-fisma-documents
FY15 Q1 CAP metrics Reports due	1/15/15	On Track	
FY15 Q2 CAP metrics Reports due	04/15/15	Not Started	
FY15 CAP Goal agency targets due	04/15/15	Not Started	Based on FY15 Q1 metric results, agencies will provide future FY15 and FY16 targets
FY15 Q3 CAP metrics Reports due	07/15/15	Not Started	
FY15 Q4 CAP metrics Reports due	11/16/15	Not Started	Also know as the FY15 Annual metrics collection due date

Key Indicators

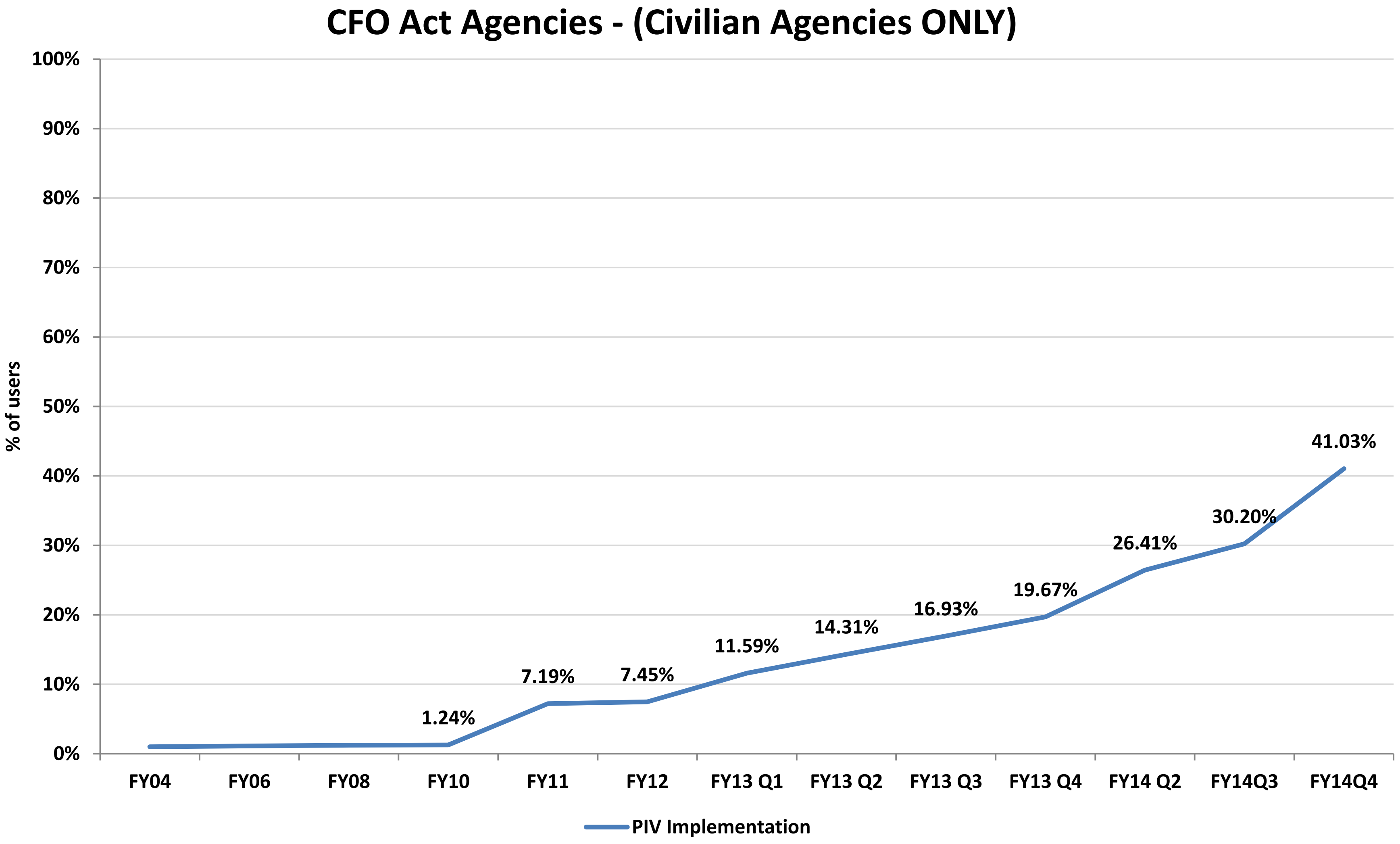
Key Implementation Milestones/Target					
Indicator	**Source**	**Baseline**	**Target**	**Q4 FY2014**	**Trend**
ISCM– Automated Asset Management: *% of assets in 2.1 that are covered by an automated capability (scans/device discovery processes) to provide enterprise-level visibility into asset inventory information for all hardware assets.* **ISCM – Configurations:** *% of the applicable hardware assets (per question 2.1) of each kind of operating system software in 3.1 covered by an automated capability to identify deviations from the approved configuration baselines identified in 3.1.1 and to provide visibility at the organization's enterprise level.* **ISCM – Vulnerabilities:** *% of hardware assets identified in section 2.1 that are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization's enterprise level.*	Agencies (FY2014 FISMA Reporting)	78.42%*	95%*	92.32%*	⬆
Strong Authentication – Identity Management: *% of ALL people required to use Personal Identity Verification (PIV) Card to authenticate.*	Agencies (FY2014 FISMA Reporting)	53.72%	75%	72.03%	⬆
TIC Consolidation: *% of external network traffic passing through a trusted Internet Connection (TIC). [Excludes DOD]*	Comprehensive National Security Initiative	84%	95%	95.48%	⬆
TIC Capabilities: *% of required TIC capabilities implemented by TIC(s) used by the organization.*	Comprehensive National Security Initiative	82.21%	100%	91.65%	⬆

* - % are based on the compilation of averages of the agency performance reported for the three ISCM categories (see slide #8)

Overall CAP Performance FY14Q3 vs FY14Q4



Strong Authentication Trend (Civilian ONLY)



CFO Act Agency Details for Q4 FY2014

Agency	ISCM Average	Automated Asset Management	Automated Configuration Management	Automated Vulnerability Management	PIV Local Access	Planned Agency PIV Target	TIC 2.0 Capabilities	TIC Traffic Consolidation	CAP Average
DHS	! 94.7	✓ 99	! 86	✓ 99	✓ 80	✓ 75	✗ 92	✓ 97	! 92.2
DOC	! 88.3	! 86	! 89	! 90	✓ 88	✗ 39	✗ 75	! 86	! 85.7
DOD	! 89.7	✓ 97	✗ 77	✓ 95	✓ 87	✓ 94	N/A	N/A	! 89.0
DOE	! 91.7	! 94	! 92	! 89	✗ 29	✓ 75	! 96	✗ 72	✗ 78.7
DOI	! 94.3	✓ 98	! 86	✓ 99	✗ 36	! 55	✗ 91	✓ 100	! 85.0
DOJ	✓ 99.0	✓ 99	✓ 99	✓ 99	✗ 44	! 50	✗ 88	✓ 100	! 88.2
DOL	✓ 98.7	✓ 100	✓ 99	✓ 97	✗ 0	✓ 75	✓ 100	✓ 100	! 82.7
DOT	! 87.7	✓ 96	! 90	✗ 77	✗ 31	✗ 20	✗ 85	✓ 99	✗ 79.7
ED	✓ 98.3	✓ 100	✓ 95	✓ 100	✓ 85	✓ 95	! 95	✓ 95	✓ 95.0
EPA	! 81.7	✗ 76	✓ 95	✗ 74	! 69	✓ 90	✗ 90	✓ 95	! 83.2
GSA	✓ 98.3	✓ 100	✓ 95	✓ 100	✓ 95	✓ 100	! 98	✓ 100	✓ 98.0
HHS	✗ 79.7	! 93	✗ 69	✗ 77	! 69	✓ 79	✗ 74	✓ 98	! 80.0
HUD	! 91.3	! 93	✓ 95	! 86	✗ 0	✓ 95	! 98	✓ 100	✗ 78.7
NASA	✓ 96.3	! 93	✓ 96	✓ 100	✓ 82	! 60	✗ 89	✓ 99	! 93.2
NRC	! 89.0	! 89	! 91	! 87	✗ 0	✗ 9	✓ 100	✓ 100	✗ 77.8
NSF	✓ 96.0	✓ 100	! 88	✓ 100	✗ 19	✗ 25	✓ 100	✓ 100	! 84.5
OPM	✓ 96.7	✓ 95	✓ 100	✓ 95	✗ 1	✓ 75	✗ 77	✓ 100	✗ 78.0
SBA	✓ 100.0	✓ 100	✓ 100	✓ 100	✗ 0	✗ 0	✓ 100	✓ 99	! 83.2
SSA	✓ 98.0	✓ 100	! 94	✓ 100	✓ 85	✓ 75	✗ 94	✓ 100	✓ 95.5
State	✓ 95.0	! 87	✓ 98	✓ 100	✗ 0	! 50	✗ 93	✓ 100	✗ 79.7
Treasury	✓ 98.3	✓ 99	✓ 99	✓ 97	✗ 43	✗ 39	! 99	✓ 99	! 89.3
USAID	! 90.0	! 85	✓ 100	! 85	✗ 3	✗ 5	✗ 92	✓ 100	✗ 77.5
USDA	✓ 99.7	✓ 99	✓ 100	✓ 100	✗ 6	✓ 75	✗ 89	✓ 100	! 82.3
VA	✓ 96.0	! 94	✓ 100	! 94	✗ 10	N/A	✗ 93	✗ 57	✗ 74.7

Source: From FISMA reporting in CyberScope.

* - The ISCM average is the average of Asset, Configuration, and Vulnerability Management. The CAP average is the average of PIV, TIC 2.0 Capabilities, TIC Consolidation, and Asset, Configuration, and Vulnerability Management.

Agency Data

Improving Agencies (≥10% increases from Q3 FY2014)

Information Security Continuous Monitoring

Asset Management: DOC (86%), EPA (76%)

Configuration Management: DOD (77%), DOI (87%), STATE (98%)

Vulnerability Management: DOC (90%), DOI (99%), EDU (100%), EPA (74%), USDA (100%)

PIV: DHS (80%), DOC (88%), DOI (36%), DOT (31%), EDU (85%), EPA (69%), NASA (82%), NSF (19%), TREASURY (43%)

TIC 2.0 Capabilities: HUD (98%)

Traffic Consolidation: EDU (95%), HHS (98%), USDA (100%), VA (57%)

Regressing Agencies (≥10% decreases from Q3 FY2014)

Information Security Continuous Monitoring

Asset Management: None

Configuration Management: HHS (69%)

Vulnerability Management: HHS (77%)

PIV: None

TIC 2.0 Capabilities: HHS (74%)

Traffic Consolidation: None