Cybersecurity

Goal Leaders:
Tony Scott, Federal Chief Information Officer;
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

FY2016 Quarter 3

Overview

Goal Statement

Improve awareness of cybersecurity practices, vulnerabilities, and threats to the operating environment by limiting access to authorized users and implementing technologies and processes that reduce 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 the Federal Government is not just a technology issue. It is an organizational, people, and performance issue requiring creative solutions to address increasingly sophisticated threats and emerging vulnerabilities introduced by rapidly changing technology.

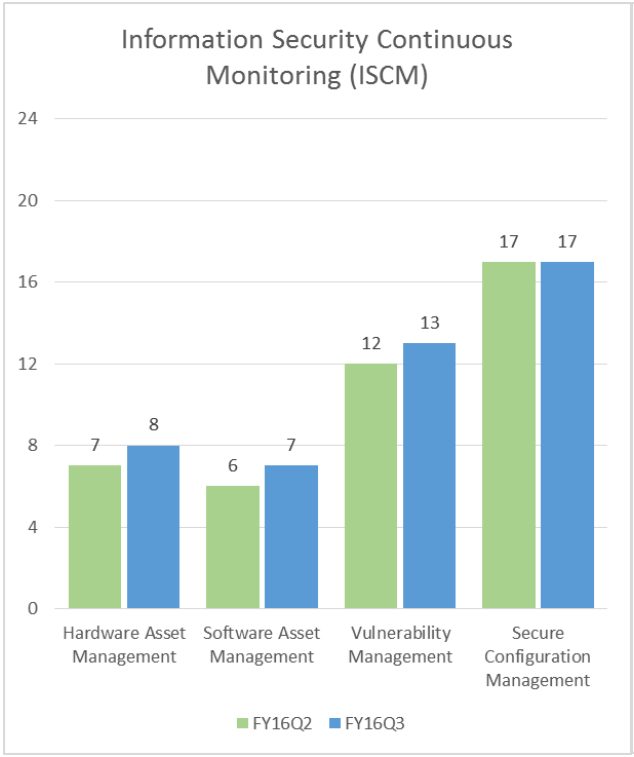
Vision

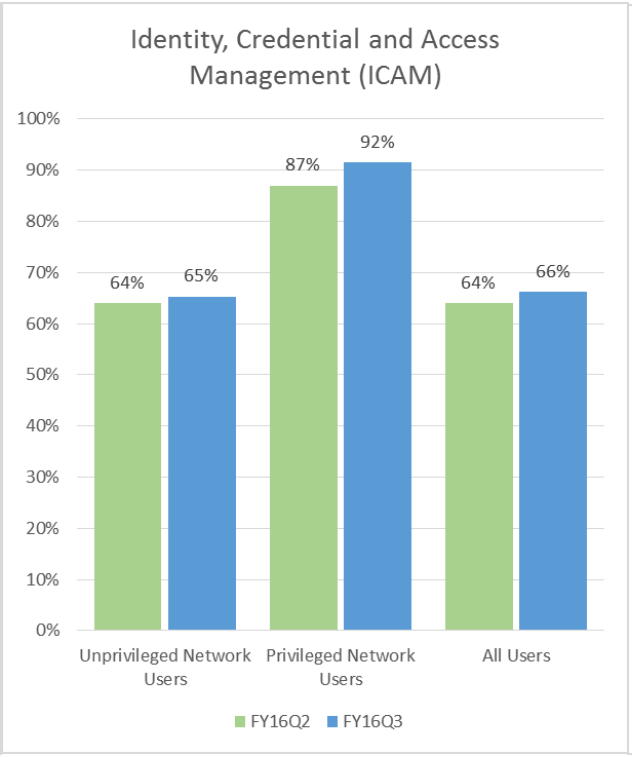
Implement the Administration's priority cybersecurity capabilities and develop performance-based metrics to measure success. The Administration's FY 2015 – FY 2017 Cybersecurity Cross Agency Priority (CAP) goal is comprised of the following initiatives:

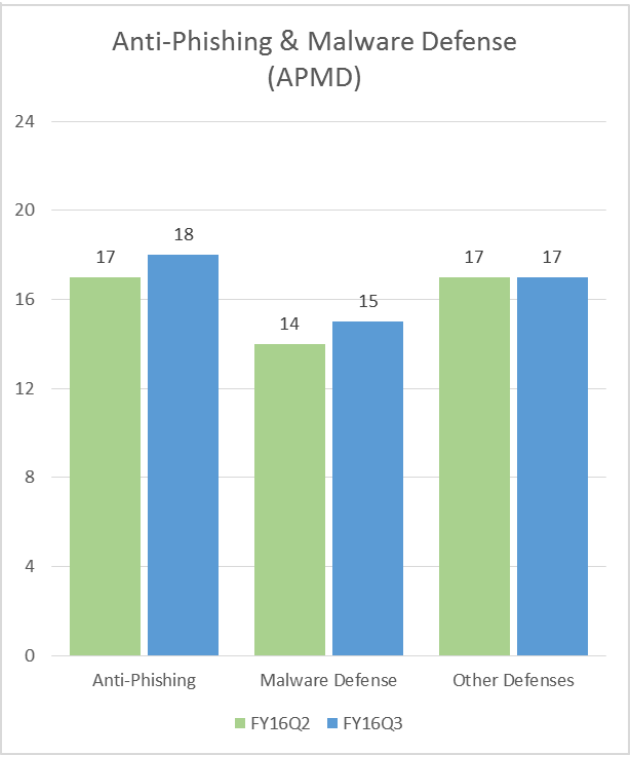
- **Information Security Continuous Monitoring (ISCM)** – Provide ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity.
- **Identity, Credential, and Access Management (ICAM/Strong Authentication)** – Implement a set of capabilities that ensures users must authenticate to information technology resources and have access to only those resources that are required for their job function.
- **Anti-Phishing and Malware Defense (APMD)** – Implement technologies, processes, and training that reduces the risk of malware being introduced through email and malicious or compromised web sites.

Status Update

Civilian CFO Act Agency status toward meeting the Cybersecurity CAP Goal targets in FY 2016 Q3.*







*The number of agencies meeting government-wide targets may vary from quarter to quarter due to fluctuations in the number of information technology assets or number of users at a given agency. This report reflects data from the 23 civilian CFO Act agencies, and therefore excludes information from the Department of Defense and small agencies.

Information Security Continuous Monitoring (ISCM)*
FY 2016 Q2 vs FY 2016 Q3

Hardware Asset Management

Performance must be greater than or equal to 95% for both Hardware Asset Management measures (asset detection, asset meta data collection):

- 8 civilian agencies met both targets in FY 2016 Q3, up from 7 agencies in FY 2016 Q2.

Software Asset Management

Performance must be greater than or equal to 95% for both Software Asset Management measures (software inventory, software whitelisting):

- 7 civilian agencies met both targets in FY 2016 Q3, up from 6 agencies in FY 2016 Q2.

Vulnerability Management

Performance must be greater than or equal to 95%:

- 13 civilian agencies met the target for FY 2016 Q3, up from 12 agencies in FY 2016 Q2.

Secure Configuration Management

Performance must be greater than or equal to 95%:

- 17 civilian agencies met the target for FY 2016 Q3, the same as in FY 2016 Q2.

*For more information on the specific ISCM metrics, see the Appendix A - Key Indicators.

Information Security Continuous Monitoring (ISCM)
FY 2016 Q2 vs FY 2016 Q3

Agency	FY 2016 Q2					FY 2016 Q3				
	Hardware Asset Management	Software Asset Management	Vulnerability Management	Secure Configuration Management (SecCM)	ISCM Avg	Hardware Asset Management	Software Asset Management	Vulnerability Management	Secure Configuration Management (SecCM)	ISCM Avg
SSA	100	100	100	99	*100*	100	100	100	100	*100*
OPM	100	100	98	98	*99*	100	96	98	99	*98*
USDA	91	93	85	100	*92*	95	100	95	100	*97*
Justice	93	97	97	100	*97*	95	97	97	100	*97*
NRC	98	93	100	99	*97*	97	91	100	99	*97*
GSA	73	98	100	96	*92*	73	96	100	96	*91*
Labor	65	99	96	100	*90*	66	99	95	100	*90*
Treasury	87	93	99	98	*94*	87	93	100	98	*95*
ED	96	80	100	99	*94*	83	91	100	100	*93*
HUD	87	82	100	100	*92*	85	86	100	99	*93*
State	81	96	68	99	*86*	81	96	88	100	*91*
DOT	95	89	70	98	*88*	99	90	76	98	*91*
NSF	100	0	93	100	*73*	100	0	90	100	*72*
SBA	99	7	100	2	*52*	99	7	100	2	*52*
VA	0	3	98	99	*50*	7	4	98	99	*52*
DHS	47	73	92	82	*74*	47	92	100	85	*81*
HHS	69	32	96	90	*72*	77	34	94	98	*76*
USAID	91	75	0	96	*66*	90	76	0	96	*66*
EPA	0	69	0	98	*42*	51	67	0	97	*54*
Commerce	55	55	76	99	*71*	58	58	81	94	*73*
Energy	68	38	61	82	*62*	59	45	66	81	*63*
Interior	26	34	76	77	*53*	20	52	85	77	*59*
NASA	2	10	89	85	*46*	2	0	89	85	*44*
Civilian CFO Act Avg	54%	58%	86%	93%		56%	61%	90%	93%	
# Agencies Meeting Targets	7	6	12	17		8	7	13	17	

Key
Meets or exceeds CAP targets

Source: FISMA Data Agency Level Questions 1.2, 1.4, 1.5, 2.2, 2.3.1, 2.3.4, 3.16, 3.17 from CyberScope.

Notes: Agencies are sorted by number of CAP Goal targets met

Civilian CFO Act averages are weighted by the number of hardware assets.

Identity, Credential and Access Management (ICAM)*
FY 2016 Q2 vs FY 2016 Q3

Unprivileged Network Users

Performance must be greater than or equal to 85%.

- Unprivileged user PIV-usage for civilian agencies increased from 64% in FY 2016 Q2 to 65% in FY 2016 Q3.
- 18 civilian agencies met the Unprivileged Network Users PIV-usage target in FY 2016 Q3, which is the same as FY 2016 Q2.

Privileged Network Users

Performance must be equal to 100%.

- Civilian agencies' privileged user PIV-usage increased from 87% in FY 2016 Q2 to 92% in FY 2016 Q3.
- 16 civilian agencies met the Privileged Network Users PIV-usage target in FY 2016 Q3, up from 15 agencies in FY 2016 Q2.

*For more information on the specific ICAM metrics, see the Appendix A - Key Indicators.

Identity, Credential and Access Management (ICAM)
FY 2016 Q2 vs FY 2016 Q3

Agency	FY 2016 Q2			FY 2016 Q3		
	Unprivileged Network Users	Privileged Network Users	All Users	Unprivileged Network Users	Privileged Network Users	All Users
OPM	100	100	100	100	100	100
State	100	100	100	100	100	100
USAID	100	100	100	100	100	100
EPA	98	99	98	99	100	99
GSA	99	100	99	99	100	99
NSF	99	100	99	98	100	98
Labor	97	99	97	98	100	98
DOT	98	100	98	98	100	98
SBA	88	100	89	97	100	97
Treasury	92	100	92	95	100	95
SSA	87	100	88	94	100	95
NRC	92	100	92	93	100	93
HUD	90	100	91	90	100	91
ED	87	100	90	87	100	90
Interior	88	100	89	88	100	89
DHS	97	93	97	99	99	99
USDA	87	100	88	89	95	89
HHS	86	97	86	87	97	88
NASA	78	100	79	82	100	82
Commerce	82	79	82	83	87	83
Justice	57	57	57	58	58	58
Energy	19	28	20	25	61	27
VA	12	99	13	12	96	13
Civilian CFO Act Avg	64%	87%	64%	65%	92%	66%
# Agencies Meeting Targets	18	15		18	16	

Key
Meets or exceeds CAP targets

Source: FISMA Data Agency Level Questions 2.4, 2.4.1, 2.5, 2.5.1 from CyberScope.

Notes: Agencies are sorted by number of CAP Goal targets met

Civilian CFO Act averages are weighted by the number of users.

Anti-Phishing & Malware Defense (APMD)*
FY 2016 Q2 vs FY 2016 Q3

Anti-Phishing

Performance on Anti-Phishing measurements must be greater than or equal to 90% on at least 5 of 7 capabilities:

- 18 civilian agencies met the CAP Goal targets in in FY 2016 Q3, up from 17 agencies in FY 2016 Q2.

Malware Defense

Performance on Malware Defense measurements must be greater than or equal to 90% on at least 3 of 5 capabilities:

- 15 civilian agencies met the CAP Goal targets in FY 2016 Q3, up from 14 agencies in FY 2016 Q2.

Other Defenses (capabilities related to Anti-Phishing & Malware)

Performance on these measurements must be greater than or equal to 90% on at least 2 of 4 capabilities:

- 17 civilian agencies met the CAP Goal targets in FY 2016 Q3, the same as in FY 2016 Q2.

*For more information on the Anti-Phishing and Malware Defense metrics, see the Appendix A - Key Indicators.

Anti-Phishing & Malware Defense (APMD)
FY 2016 Q2 vs FY 2016 Q3

Agency	FY 2016 Q2			FY 2016 Q3		
	# Capabilities required to have >=90% coverage					
	Anti-Phishing	Malware Defense	Other Defenses	Anti-Phishing	Malware Defense	Other Defenses
	5	3	2	5	3	2
HUD	7	4	4	7	4	4
OPM	6	5	4	6	5	4
State	5	5	3	6	5	4
Treasury	6	4	4	6	4	4
USDA	6	5	2	7	4	3
Interior	6	1	2	7	4	2
SSA	5	4	3	6	4	3
DOT	6	3	2	6	4	2
NRC	5	3	2	5	3	4
SBA	4	4	2	5	4	2
USAID	6	3	2	6	3	2
GSA	6	3	2	5	3	2
VA	5	3	2	5	3	2
ED	7	1	4	7	2	4
DHS	7	0	1	6	2	2
NSF	4	1	2	5	1	2
HHS	6	2	1	5	2	1
Justice	4	3	1	4	3	1
NASA	5	2	1	5	2	1
Commerce	4	0	3	4	0	3
EPA	3	0	0	3	3	0
Labor	5	4	2	4	2	1
Energy	4	0	1	2	0	1
# Agencies Meeting Targets	17	14	17	18	15	17

Key
Meets or exceeds CAP targets

Source: FISMA Data Agency Level Questions 2.19, 2.19.1, 3.1 through 3.15 from CyberScope.

Notes: Agencies are sorted by number of CAP Goal targets met

Action Plan Summary

Initiative*	Major Actions to Achieve Impact	Key Indicator/Targets for FY 2015 Q3 thru FY 2017
Information Security Continuous Monitoring (ISCM)	• Understand the hardware and software on Federal networks and the risks that they pose; and • Maintain ongoing, near real-time awareness of information security risks and have the capability to rapidly respond to support organizational risk management decisions.	• **Hardware Asset Management:** Detection of devices or device hardware characteristics must be greater than or equal 95%. • **Software Asset Management:** Detection of software inventory or base level application configurations (whitelisting) must be greater than or equal 95%. • **Vulnerability Management:** Detection of hardware or software vulnerabilities must be greater than or equal 95%. • **Secure Configuration Management:** Validation of select OS software configurations must be greater than or equal 95%.
Identity, Credential, and Access Management (ICAM/ Strong Authentication)	• Ensure only authorized users have access to Federal information systems; and • Ensure only authorized users have access to information needed for designated business functions.	• **Unprivileged Network Users:** Unprivileged users required to use PIV for network log-on must be greater or equal to 85%. • **Privileged Network Users:** Privileged users required to use PIV for network log-on must be equal to 100%.
Anti-Phishing & Malware Defense (APMD)	• Implement technologies, processes, and training to reduce the risk of malware introduced through email and malicious or compromised web sites.	• **Anti-Phishing:** 5 of 7 capabilities with anti-phishing toolsets must be greater than or equal to 90%. • **Malware Defense:** 3 of 5 capabilities with malware toolsets must be greater than or equal to 90%. • **Other Defense** *(capabilities related to Anti-Phishing & Malware)*: 2 of 4 capabilities with a blended toolset must be greater than or equal to 90%.

* The corresponding indicators for these CAP Initiatives are captured in the Key Indicators section of this report.

Work Plan

Milestone Summary			
Key Milestones	**Milestone Date**	**Milestone Status**	**Issues / Comments**
OMB FY 2015 – FY 2016 FISMA reporting guidance released	10/30/15	Complete	http://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf
FY 2016 CIO FISMA/CAP metrics published	10/30/15	Complete	http://www.dhs.gov/publication/fy16-fisma-documents
FY 2015 FISMA annual/Q4 metrics reports due	11/13/15	Complete	https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy_2015_fisma_report_to_congress_03_18_2016.pdf
FY 2016 Q1 CAP metrics updates due	1/15/16	Complete	https://www.performance.gov/node/3401?view=public#progress-update
FY 2016 Q2 CAP metrics updates due	04/15/16	Complete	https://www.performance.gov/node/3401?view=public#progress-update
FY 2016 Q3 CAP metrics updates due	07/15/16	Complete	https://www.performance.gov/node/3401?view=public#progress-update
FY 2016 Annual/Q4 CAP metrics updates due	11/10/16		Also known as the FY 2016 FISMA annual report due date

Appendix A - Key Indicators

CAP Initiatives	Area	Question No.	Question
Information Security and Continuous Monitoring	Hardware Asset Management	1.2	Number of the organization's hardware assets connected to the organization's unclassified network(s).
		1.4	Number of GFE hardware assets (from 1.2.) covered by an automatic (e.g. scans/device discovery processes) hardware asset inventory capability at the enterprise-level. (CAP)
		3.16	Percent (%) of the organization's unclassified network that has implemented a technology solution to detect and alert on the connection of unauthorized hardware assets. (CAP)
	Software Asset Management	1.2.1	Percent (%) of endpoints from 1.1.1 covered by an automated software asset inventory capability to scan the current state of installed software (e.g., .bat, .exe, .dll).
		1.2.2	Percent (%) of endpoints from 1.1.1 covered by a desired-state software asset management capability to detect and block unauthorized software from executing (e.g. AppLocker, certificate, path, hash value, services, and behavior based whitelisting solutions).
		1.5	Number of GFE endpoints and mobile assets (from 1.2.1. and 1.2.2.) covered by an automated software asset inventory capability at the enterprise-level. (CAP)
		3.17	Number of GFE endpoints and mobile assets (from 1.2.1. and 1.2.2.) covered by a software asset management capability to detect, alert, and/or block unauthorized software from executing (e.g., certificate, path, hash value, services, and behavior based whitelisting solutions). (CAP)
	Vulnerability Management	2.2	Percent (%) of the organization's unclassified network(s) assessed for vulnerabilities using Security Content Automation Protocol (SCAP) validated products3. (CAP)
	Secure Configuration Management	2.3.1	Number of hardware assets with each OS. (Base)
		2.3.4	Number of assets in 2.3.1 covered by auditing for compliance with 2.3.2. (CAP)

Source: FISMA Data Agency Level Questions from Cyberscope.

Appendix A - Key Indicators (cont.)

CAP Initiatives	Area	Question No.	Question
Identity Credential and Access Management	Unprivileged users	2.4	Number of users with unprivileged network accounts.4 (Exclude privileged network accounts and non-user accounts.) (Base)
		2.4.1	Number of users (from 2.4.) technically required to log onto the network with a two-factor PIV card5 or NIST Level of Assurance (LOA) 4 credential.6 (CAP)
	Privileged users	2.5	Number of users with privileged network accounts. (Exclude unprivileged network accounts and non-user accounts.) (Base)
		2.5.1	Number of users (from 2.5.) technically required to log onto the network with a two-factor PIV card7 or NIST LOA 4 credential. (CAP)
Anti-Phishing & Malware Defense	Anti-Phishing	2.19	Number of users that participated in exercises focusing on phishing that are designed to increase awareness and/or measure effectiveness of training, (e.g. organization conducts spoofed phishing emails, clicking links leading to phishing information page). (Base)
		2.19.1	Number of users (from 2.19.) that successfully passed the exercise. (CAP)
		3.1	Percent (%) of incoming email traffic passing through anti-phishing and anti-spam filtration at the outermost border mail agent or server. (CAP)
		3.2	Percent (%) of incoming email traffic analyzed using sender authentication protocols (e.g., DKIM, ADSP, DMARC, VBR, SPF, iprev). (CAP)
		3.3	Percent (%) of incoming email traffic analyzed using a reputation filter (to perform threat assessment of sender). (CAP)
		3.4	Percent (%) of incoming email traffic analyzed for detection of clickable URLs, embedded content, and attachments. (CAP)
		3.5	Percent (%) of incoming email traffic analyzed for suspicious or potentially nefarious attachments opened in a sandboxed environment or detonation chamber. (CAP)
		3.6	Percent (%) of outgoing email traffic that enables the recipients to verify the originator using sender authentication protocols (e.g., DKIM, ADSP, DMARC, VBR, SPF, iprev). (CAP)

Source: FISMA Data Agency Level Questions from Cyberscope.

Appendix A - Key Indicators (cont.)

CAP Initiatives	Area	Question No.	Question
Anti-Phishing & Malware Defense	Malware Defense	3.7	Number of GFE endpoints (from 1.2.1.) covered by an intrusion prevention system. (CAP)
		3.8	Number of GFE endpoints (from 1.2.1.) covered by an antivirus (AV) solution using file reputation services, checking files against cloud-hosted, continuously updated malware information. (CAP)
		3.9	Number of GFE endpoints (from 1.2.1.) covered by an anti-exploitation tool (e.g., Microsoft's Enhanced Mitigation Experience Toolkit (EMET) or similar). (CAP)
		3.10	Number of GFE endpoints (from 1.2.1.) protected by a browser-based (e.g., Microsoft SmartScreen Filter, Microsoft Phishing Filter, etc.) or enterprise-based tool to block known phishing websites and IP addresses. (CAP)
		3.11	Number of GFE endpoints and mobile assets (from 1.2.1. and 1.2.2.) authorized for remote access connection to the unclassified network. (Base)
		3.11.1	Number of assets (from 3.11.) scanned for malware prior to an authorized remote access connection to the unclassified network. (CAP)
	Other Defenses (capabilities related to Anti-Phishing & Malware)	3.12	Percent (%) of privileged user network accounts (from 2.5.) that have a technical control limiting access to only trusted sites. (CAP)
		3.13	Percent (%) of inbound network traffic that passes through a web content filter, which provides anti-phishing, anti-malware, and blocking of malicious websites (e.g., fake software updates, fake antivirus offers, and phishing offers). (CAP)
		3.14	Percent (%) of outbound communications traffic checked at the external boundaries to detect encrypted exfiltration of information (i.e. D/A's capability to decrypt/interrogate and re-encrypt). (CAP)
		3.15	Percent (%) of email messages processed by systems that quarantine or otherwise block suspected malicious traffic. (CAP)

Source: FISMA Data Agency Level Questions from Cyberscope.

Acronyms

APMD	Anti-Phishing and Malware Defense
CAP	Cross Agency Priority
CFO	Chief Financial Officer
Commerce	Department of Commerce
DHS	Department of Homeland Security
DOT	Department of Transportation
ED	Department of Education
Energy	Department of Energy
EPA	Environmental Protection Agency
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GSA	General Services Administration
HHS	Department of Health and Human Services
HUD	Department of Housing and Urban Development
ICAM	Identity, Credential, and Access Management
Interior	Department of the Interior
ISCM	Information Security Continuous Monitoring
Justice	Department of Justice
Labor	Department of Labor
NASA	National Aeronautics and Space Administration
NRC	Nuclear Regulatory Commission
NSF	National Science Foundation
OPM	Office of Personnel Management
PIV	Personal Identity Verification
SBA	Small Business Association
SSA	Social Security Administration
State	Department of State
Treasury	Department of the Treasury
USAID	United States Agency for International Development
USDA	Department of Agriculture
VA	Department of Veterans Affairs