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

FY2015 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 the Federal Government is not just a technology issue. It is an organizational, people, and performance issue requiring creative solutions to address emerging and increasingly sophisticated threats and new vulnerabilities introduced by rapidly changing technology.

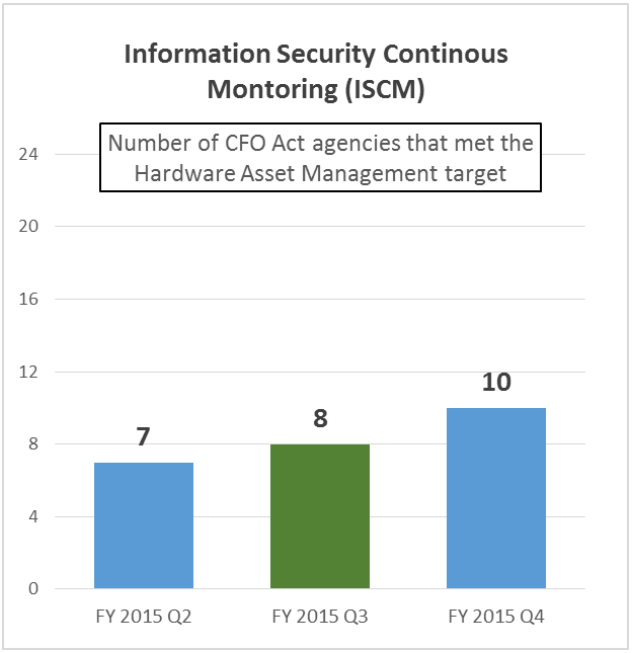
Vision

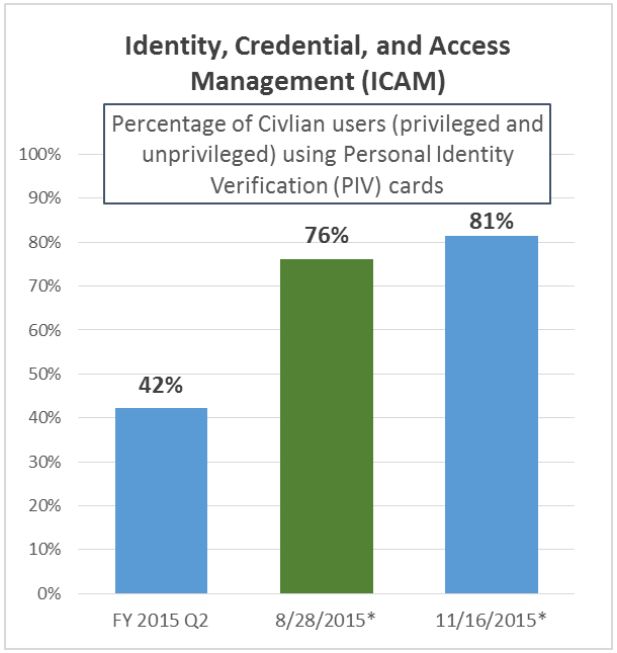
Implement the Administration's priority cybersecurity capabilities and develop performance-based metrics to measure success. The Administration's FY 2014 – FY 2017 Cybersecurity Cross Agency Priority (CAP) goal is comprised of the following initiatives:

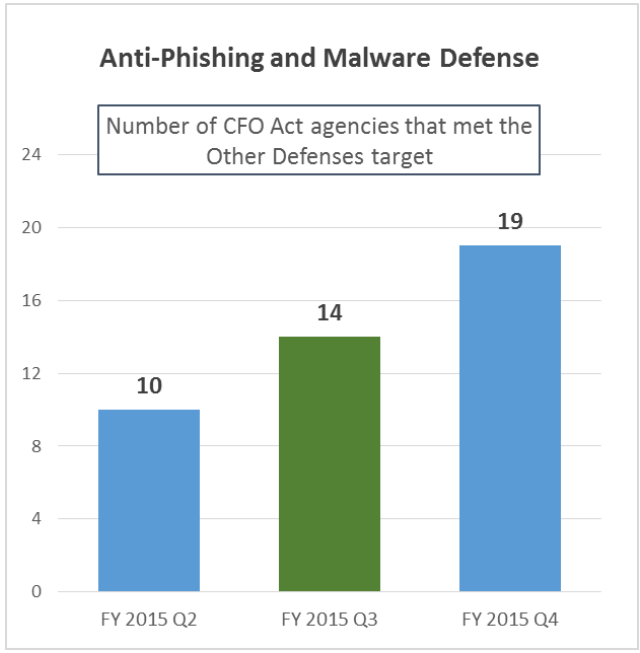
- **Information Security Continuous Monitoring (ISCM)** – Provide ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity.
- **Identity, Credential, and Access Management (ICAM/Strong Authentication)** – Implement a set of capabilities that ensures users must authenticate 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.

Progress Update

Agencies made significant progress meeting the Cybersecurity CAP Goal targets in FY 2015 Q4.







* Cyber Sprint updates

Information Security Continuous Monitoring (ISCM)
FY 2015 Q3 vs FY 2015 Q4

Hardware Asset Management*

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

- 10 agencies met both targets in Q4, up from 8 agencies in Q3.

Software Asset Management*

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

- 7 agencies met both targets in Q4, the same as in Q3.

Vulnerability Management*

Performance must be greater than or equal to 95%:

- 9 agencies met the target for Q4, up from 8 agencies in Q3.

Secure Configuration Management*

Performance must be greater than or equal to 95%:

- 15 agencies met the target for Q4, the same as in Q3.

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

Information Security Continuous Monitoring (ISCM)
FY 2015 Q3 vs FY 2015 Q4

	FY 2015 Q3					FY 2015 Q4				
	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
Agency	Min of 1.2-%, 1.3-%	Min of 1.5-%, 1.6-%	1.8.-%	1.7.6.-%		Min of 2.2-%, 2.3-%	Min of 2.6%, 2.7-%	2.11.-%	2.10.6.-%	
OPM	100	98	95	98	*98*	100	100	95	99	*99*
SSA	100	100	100	100	*100*	100	100	100	100	*100*
NRC	100	85	100	99	*96*	100	92	96	99	*97*
NSF	100	0	88	98	*72*	100	0	88	98	*72*
Labor	95	97	97	99	*97*	99	96	99	100	*99*
DOT	94	90	30	21	*59*	99	90	30	21	*60*
SBA	99	0	99	98	*74*	98	2	99	97	*74*
Justice	97	97	97	99	*98*	97	97	97	99	*98*
USDA	90	90	70	100	*87*	95	100	85	100	*95*
USAID	100	96	100	100	*99*	95	0	100	75	*68*
HHS	91	35	82	76	*71*	92	32	82	75	*70*
Energy	83	39	34	90	*61*	87	39	31	91	*62*
Treasury	17	18	93	100	*57*	83	91	98	99	*93*
DOD	70	79	0	0	*37*	83	82	20	0	*46*
State	81	98	90	96	*91*	81	98	82	95	*89*
ED	73	77	86	94	*82*	77	17	85	94	*68*
GSA	70	94	93	94	*88*	73	96	98	95	*91*
Commerce	51	38	61	94	*61*	66	72	74	91	*76*
HUD	81	98	83	100	*90*	62	0	76	100	*60*
DHS	46	33	95	84	*65*	54	58	93	87	*73*
Interior	75	57	71	98	*75*	46	57	68	99	*68*
EPA	3	79	1	97	*45*	2	67	0	98	*42*
NASA	0	0	84	85	*42*	0	2	82	86	*43*
VA	0	75	94	99	*67*	0	0	49	99	*37*
Govt-Wide Avg	61%	68%	51%	58%		68%	62%	52%	58%	
# Agencies Meeting Targets	8	7	8	15		10	7	9	15	

Key

Meets or exceeds FY15 target

Source: FISMA Data Agency Level Questions 1.2, 1.3, 1.5, 1.6, 1.8, 1.7.6 (FY 2015 Q3) and 2.2, 2.3, 2.6, 2.7, 2.11, 2.10.6 (FY 2015 Q4) from CyberScope

Notes:
Data sorted based on results of FY 2015 Q4 Hardware Asset Management question 2.2.

For hardware and software asset management, which include two metrics, this report displays government-wide weighted averages of the lower of the two metrics.

Identity, Credential and Access Management (ICAM)
August 28, 2015 vs November 16, 2015 *(Cyber Sprint Update)*

Unprivileged Network Users*

Performance must be greater than or equal to 85%.

- Unprivileged user PIV-usage for civilian agencies increased from 76% on August 28, 2015, to 81% on November 16, 2015.
  - The percentage increases to 84% when the Department of Defense is included.
- Number of CFO Act agencies that met the Unprivileged Network Users PIV-usage target increased from 9 on August 28, 2015, to 16 on November 16, 2015.

Privileged Network Users*

Performance must be equal to 100%.

- Civilian agencies' privileged user PIV-usage increased from 73% on August 28, 2015, to 81% on November 16, 2015.
- Number of CFO Act agencies that met the Privileged Network Users PIV-usage target increased from 9 on August 28, 2015, to 13 on November 16, 2015.

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

Sources: August 28, 2015, and November 16, 2015, updates are based on the agency's Cyber Sprint Update

Identity, Credential and Access Management (ICAM)
August 28, 2015 vs November 16, 2015 *(Cyber Sprint Update)*

	August 28, 2015			November 16, 2015		
	Unprivileged Network Users	Privileged Network Users	All Users	Unprivileged Network Users	Privileged Network Users	All Users
Agency	2.1.1.-%	2.2.1.-%	%	3.1.1.-%	3.2.1.-%	%
GSA	**99**	**100**	99	**99**	**100**	99
OPM	**97**	**100**	97	**99**	**100**	99
DOT	**97**	**100**	97	**97**	**100**	97
Interior	**94**	**100**	95	**96**	**100**	97
DHS	**92**	99	93	**95**	99	95
Treasury	**92**	**100**	92	**97**	**100**	97
HUD	**91**	**100**	91	**95**	**100**	95
NSF	**87**	**100**	88	**87**	**100**	88
HHS	**87**	99	88	**87**	99	88
SSA	83	99	84	**86**	99	87
EPA	82	96	84	**97**	**100**	97
SBA	82	80	82	**89**	**100**	89
Commerce	82	75	82	82	86	82
VA	80	**100**	81	80	**100**	82
Labor	79	84	79	**92**	95	92
NRC	78	84	78	**93**	97	93
USDA	76	88	77	**86**	89	86
NASA	66	55	66	77	**100**	77
ED	77	12	58	78	27	65
Justice	34	85	35	64	65	64
USAID	28	**100**	30	35	**100**	36
State	26	76	28	38	**100**	40
Energy	11	13	12	11	7	10
Civilian Only	76%	73%	76%	81%	81%	81%
DOD	83	58	82	**86**	51	84
All CFO Act	81%	67%	80%	84%	62%	83%

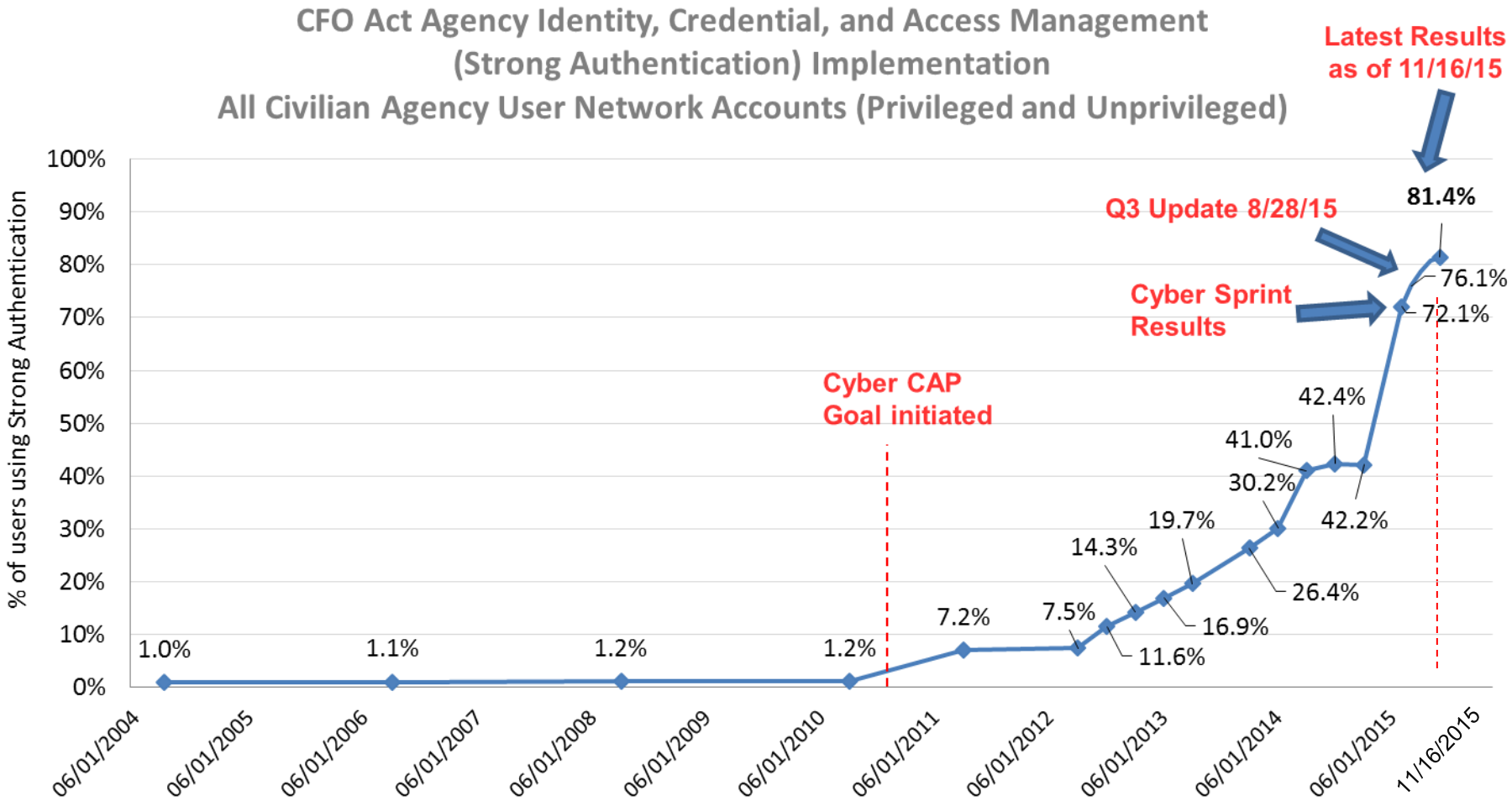
Key

Meets or exceeds FY15 target

Source: FISMA Data Agency Level Questions 2.1.1 and 2.2.1 (FY 2015 Q3) and 3.1.1 and 3.2.1 (FY 2015 Q4) from CyberScope

Note: The Civilian and CFO Act totals are weighted by the number of users

Identity, Credential, and Access Management (ICAM) Trend Civilian Agencies* Only



Source: FISMA Data Agency Level Questions submitted to CyberScope.
*Note: This graph excludes the Department of Defense (DOD), due to the large number of users at DOD.
** Cyber Sprint Update

Anti-Phishing & Malware Defense
FY 2015 Q3 vs FY 2015 Q4

Anti-Phishing*

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

- 14 agencies met the CAP Goal targets in Q4, up from 12 agencies in Q3.

Malware Defense*

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

- 9 agencies met the CAP Goal targets in Q4, up from 8 agencies in Q3.

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:

- 19 agencies met the CAP Goal targets in Q4, up from 14 agencies in Q3.

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

Anti-Phishing & Malware Defense
FY 2015 Q3 vs FY 2015 Q4

	FY 2015 Q3			FY 2015 Q4		
	Anti-Phishing	Malware Defense	Other Defenses	Anti-Phishing	Malware Defense	Other Defenses
# Capabilities required to have >=90% coverage	5	3	2	5	3	2
Agency						
HUD	3	2	2	6	4	4
SSA	6	3	3	6	3	3
GSA	6	2	2	6	3	2
Labor	6	2	1	6	3	2
VA	6	3	1	6	2	2
USDA	4	1	2	6	0	2
State	5	5	3	5	4	3
OPM	5	5	2	5	4	3
DOT	5	3	2	5	3	2
USAID	4	2	3	5	2	3
Interior	5	0	1	5	2	2
NSF	5	1	2	5	1	2
ED	5	0	0	5	1	0
HHS	5	0	2	5	0	2
Treasury	4	3	4	4	3	4
Justice	5	3	1	4	3	1
NRC	4	2	2	4	2	2
DHS	4	1	1	4	1	2
SBA	4	1	1	4	1	2
EPA	2	0	0	4	0	0
NASA	3	1	0	3	2	0
DOD	4	4	2	3	1	2
Energy	3	1	0	3	0	0
Commerce	2	0	3	2	1	2

Key

Meets or exceeds CAP goal targets

Source: FISMA Data Agency Level Questions 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.12, 3.13, 3.14, 3.15, 3.16 (FY 2015 Q3) and 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13, 4.14, 6.1.4, 8.2.1 (FY2015 Q4) from CyberScope

Note: Data sorted based on the number FY 2015 Q4 Anti-Phishing Capabilities.

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	
FY 2016 Q1 CAP metrics updates due	1/15/16	Complete	
FY 2016 Q2 CAP metrics updates due	04/15/16		
FY 2016 Q3 CAP metrics updates due	07/15/16		
FY 2016 Annual/Q4 CAP metrics updates due	10/30/16		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	2.2	Percent (%) of the organization's network fabric covered by a capability to detect and alert on the addition of unauthorized hardware assets onto the organization's network.
		2.3	Percent (%) of the organization's network fabric covered by an automatic capability (scans/device discovery processes) that provides enterprise-level visibility into the current state of all hardware assets.
	Software Asset Management	2.6	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).
		2.7	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).
	Vulnerability Management	2.11	Percent (%) of hardware assets listed in 1.1 assessed using credentialed scans with Security Content Automation Protocol (SCAP) validated vulnerability tools.
	Secure Configuration Management	2.10.6	Percent (%) of assets that are covered by audit activities
Identity Credential and Access Management	Unprivileged users	3.1	How many users have unprivileged network accounts (Exclude privileged user accounts and non-user accounts.)
		3.1.1	Percent (%) of unprivileged users technically required to log onto the network with a two-factor PIV card.
	Privileged users	3.2	How many users have privileged network accounts? (Exclude unprivileged network accounts and non-user accounts.)
		3.2.1	Percent (%) of privileged users technically required to log onto the network with a two-factor PIV card.

Source: FISMA Data Agency Level Questions 2.2, 2.3, 2.6, 2.7, 2.10.6, 2.11, 3.1.1, 3.2.1 from CyberScope

Appendix A - Key Indicators (cont.)

CAP Initiatives	Area	Question No.	Question
Anti-Phishing & Malware Defense	Anti-Phishing	4.2	Percent (%) of incoming email traffic analyzed for clickable URLs, embedded content, and attachments.
		4.5	Percent (%) of email attachments opened in sandboxed environment or detonation chamber.
		4.6	Percent (%) of incoming emails using email sender authentication protocols such as Domain Keys Identified Mail (DKIM), Author Domain Signing Practices (ADSP), Domain-based Message Authentication, Reporting & Conformance (DMARC), Vouch by Reference (VBR), or IP Reverse (iprev).
		4.7	Percent (%) of incoming emails scanned using a reputation filter tool to perform threat assessment of email sender.
		4.9	Percent (%) of inbound email traffic passing through anti-phishing/anti-spam filtration technology at the outermost border Mail Transport Agent or email server.
		4.13	Percent (%) of sent email that is digitally signed.
		8.2.1	Percent (%) of the users that participated in cybersecurity-focused exercises who successfully completed exercises focusing on phishing, designed to increase awareness and/or measure effectiveness of previous training. (e.g., organization conducts spoofed phishing emails, clicking link leads to phishing information page)
	Malware Defense	4.3	Percent (%) of hardware assets covered by a host-based intrusion prevention system.
		4.4	Percent (%) of hardware assets covered by an antivirus (AV) solution using file reputation services, checking files against cloud-hosted, continuously updated malware information.
		4.8	Percent (%) of hardware assets covered by an anti-exploitation tool (e.g., Microsoft's Enhanced Mitigation Experience Toolkit (EMET) or similar).
		4.11	Percent (%) of hardware assets that have implemented a browser-based (e.g. Microsoft Phishing filter) or enterprise-based tool to block known phishing websites and IP addresses.
		6.1.4	Percent (%) of remote access connections scanned for malware upon connection.
	Other Defenses (capabilities related to Anti-Phishing & Malware)	4.1	Percent (%) of privileged user accounts that have a technical control preventing internet access.
		4.1	Percent (%) of inbound network traffic that passes through a web content filter that provides anti-phishing, anti-malware, and blocking of malicious websites (e.g. fake software updates, fake antivirus offers, and phishing offers).
		4.12	Percent (%) of outbound communications traffic checked at the external boundaries to detect covert exfiltration of information.
		4.14	Percent (%) of email traffic quarantined or otherwise blocked.

Source: FISMA Data Agency Level Questions 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13, 4.14, 6.1.4, 8.2.1 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
EMET	Enhanced Mitigation Experience Toolkit
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