Cross Agency Priority Goal

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 3

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 an organizational, people, and performance issue requiring creative solutions to address emerging and increasingly sophisticated threats and new vulnerabilities introduced by rapidly changing technology.

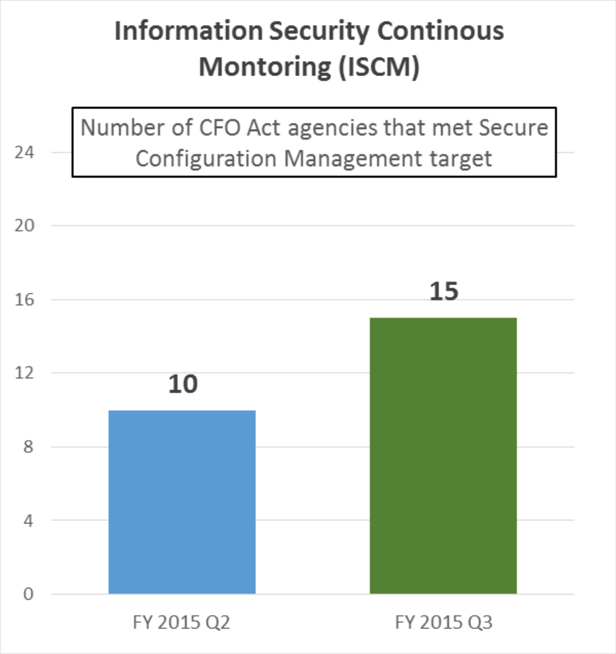
Vision

Implement the Administration's priority cybersecurity capabilities and develop performance based metrics to measure success. The Administration's FY 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.

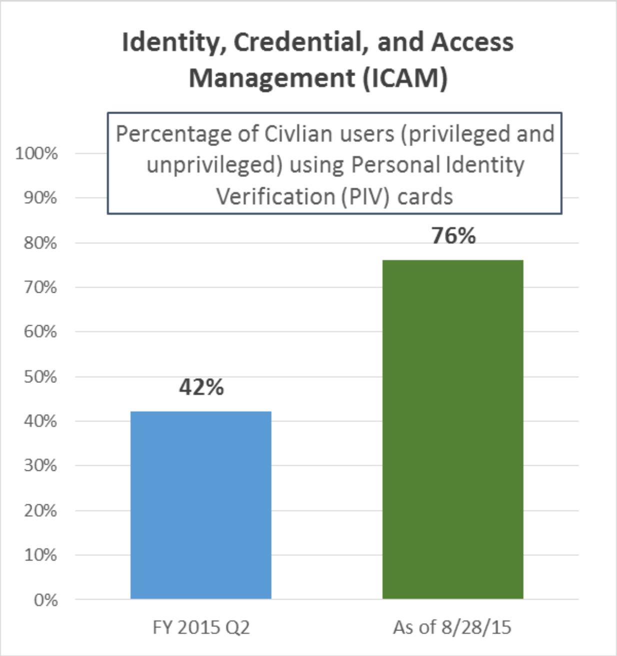
Progress Update

Agencies made significant progress meeting the three Cybersecurity CAP Goal targets in FY 2015 Q3.



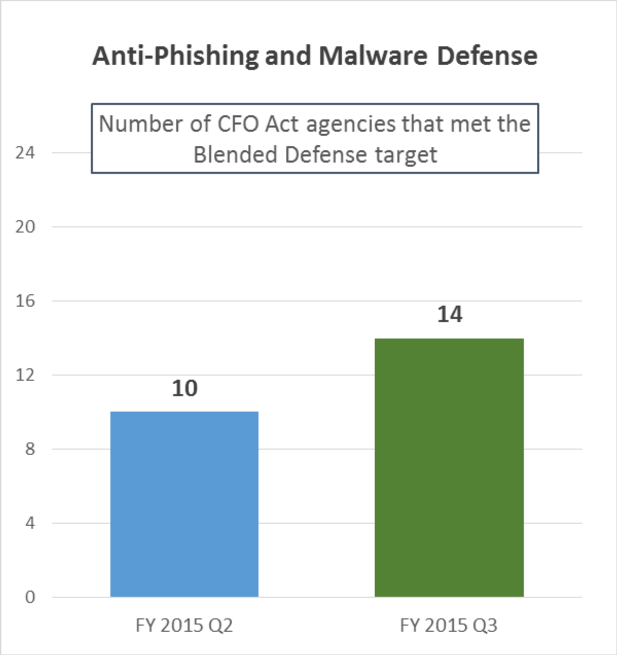
Information Security Continous Montoring (ISCM)

Number of CFO Act agencies that met Secure Configuration Management target



Identity, Credential, and Access Management (ICAM)

Percentage of Civlian users (privileged and unprivileged) using Personal Identity Verification (PIV) cards



Anti-Phishing and Malware Defense

Number of CFO Act agencies that met the Blended Defense target

Information Security Continuous Monitoring (ISCM)
FY 2015 Q2 vs FY 2015 Q3

Hardware Asset Management

Performance for both targets must be greater than or equal to 95%:

- 8 agencies met both targets in Q3, up from 6 agencies in Q2.

Software Asset Management

Performance for both targets must be greater than or equal to 95%:

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

Vulnerability and Weakness Management

Performance must be greater than or equal to 95%:

- 8 agencies met the target for Q3, down from 9 agencies in Q2.

Secure Configuration Management

Performance must be greater than or equal to 95%:

- 15 agencies met the target for Q3, up from 10 agencies in Q2.

Information Security Continuous Monitoring (ISCM)
FY 2015 Q2 vs FY 2015 Q3

	Hardware Asset Management		Software Asset Management		Vulnerability and Weakness Management	Secure Configuration Management (SecCM)	Hardware Asset Management		Software Asset Management		Vulnerability and Weakness Management	Secure Configuration Management (SecCM)
Agency	1.2.-%	1.3.-%	1.5.-%	1.6.-%	1.8.-%	1.7.6.-%	1.2.-%	1.3.-%	1.5.-%	1.6.-%	1.8.-%	1.7.6.-%
USDA	83	83	83	83	75	32	90	90	90	90	70	100
Commerce	48	82	63	34	61	97	51	77	63	38	61	94
DOD	97	93	80	92	0	78	83	70	79	97	0	84
ED	66	82	100	79	82	98	73	100	100	77	86	0
Energy	82	85	61	36	31	90	85	83	71	39	34	21
HHS	99	96	88	29	83	72	91	98	83	35	82	94
DHS	34	92	76	8	95	84	46	99	57	33	95	90
HUD	78	98	98	0	83	95	81	96	98	100	83	97
Justice	99	99	99	99	99	99	97	97	97	97	97	94
Labor	89	99	98	100	97	100	95	98	98	97	97	76
State	82	100	99	99	83	91	81	100	98	98	90	100
Interior	73	88	99	59	67	74	75	98	99	57	71	98
Treasury	11	100	11	18	73	98	17	100	18	19	93	99
DOT	94	95	100	85	21	21	94	99	100	90	30	99
VA	0	100	100	75	100	99	0	94	91	75	94	85
EPA	4	72	79	78	1	94	3	63	80	79	1	99
GSA	50	100	95	95	87	91	70	100	99	94	93	98
NASA	0	93	85	0	86	82	0	93	83	0	84	98
NSF	100	100	100	0	85	99	100	100	100	0	88	98
NRC	100	100	90	85	100	99	100	100	89	85	100	100
OPM	65	95	85	91	95	87	100	100	98	98	95	96
SBA	99	100	96	0	99	89	99	100	96	0	99	100
SSA	100	100	100	100	100	100	100	100	100	100	100	100
USAID	100	100	100	100	100	100	100	100	99	96	100	99

Note: Q2 did not have a specified targets for each metric, and the Q3 target for each metric was 95%.

Key
🟩 Meets or exceeds Q3 target

Source: FISMA Data Agency Level Questions 1.2, 1.3, 1.5, 1.6, 1.8, 1.7.6 (FY 2015 Q2 and FY 2015 Q3) from CyberScope

Identity, Credential and Access Management (ICAM)
FY 2015 Q2 vs FY 2015 Q3

Unprivileged Network Users

Performance must be greater than or equal to 85%.

- Unprivileged user PIV-usage for civilian agencies increased from 43% in Q2 to 76% as of August 28, 2015.
  - The percentage increases to 80% when including the Department of Defense.
- Civilian agency performance increased for unprivileged users from 43% to 72% during the Cybersecurity Sprint from June 12 to July 15, 2015.

Privileged Network Users

Performance must be equal to 100%.

- Civilian agencies privileged user PIV-usage increased from 33% in Q2 to 73% as of August 28, 2015.
- Civilian agency performance increased for privileged users from 33% to 73% during the Cybersecurity Sprint from June 12 to July 15, 2015.

Identity, Credential and Access Management (ICAM)
FY 2015 Q2 vs FY 2015 Q3

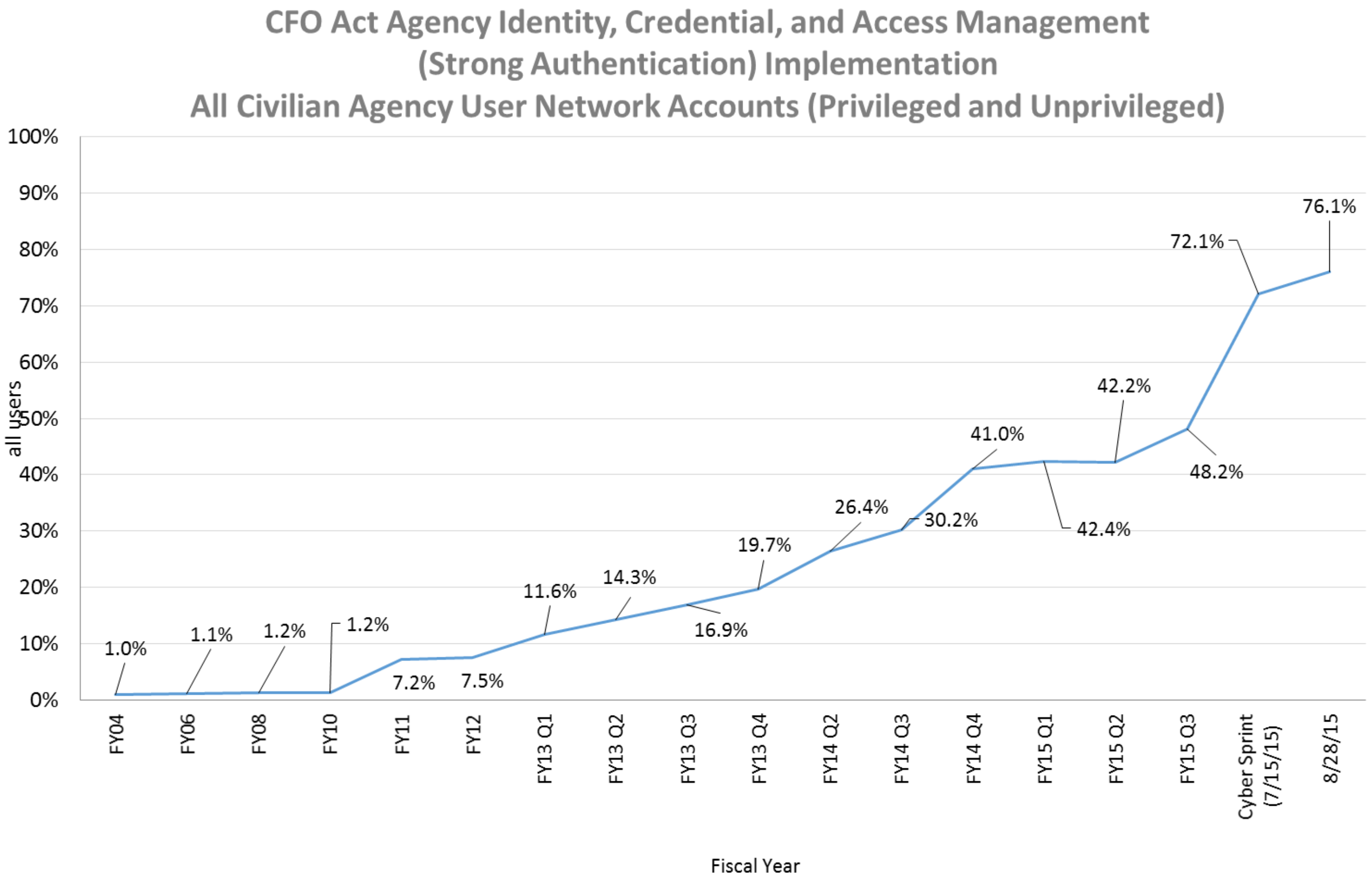
	FY 2015 Q2			August 28, 2015		
	Unprivileged Network Users	Privileged Network Users	All Users	Unprivileged Network Users	Privileged Network Users	All Users
Agency	2.1.1.-%	2.2.1.-%	%	2.1.1.-%	2.2.1.-%	%
USDA	15	6	15	76	88	77
Commerce	76	97	77	82	75	82
ED	76	14	71	77	12	58
Energy	34	8	32	11	13	12
HHS	78	43	76	87	99	88
DHS	88	41	87	92	99	93
HUD	0	0	0	91	100	91
Justice	36	26	36	34	85	35
Labor	0	0	0	79	84	79
State	2	21	3	26	76	28
Interior	45	21	43	94	100	95
Treasury	66	3	63	92	100	92
DOT	32	67	32	97	100	97
VA	10	0	10	80	100	81
EPA	61	0	56	82	96	84
GSA	99	0	94	99	100	99
NASA	0	0	0	66	55	66
NSF	60	51	59	87	100	88
NRC	0	0	0	78	84	78
OPM	41	100	42	97	100	97
SBA	0	0	0	82	80	82
SSA	82	99	84	83	99	84
USAID	20	0	19	28	100	30
Civilian Only	42.52%	32.67%	42.15%	76.24%	73.38%	76.07%
Gov-Wide	72.98%	35.37%	72.03%	80.77%	66.69%	80.28%

*Note: The Q2 target was for 75% of all users, and the Q3 targets were for 85% of unprivileged users and 100% privileged users.

Key
Meets or exceeds Q3 target

Source: FISMA Data Agency Level Questions 2.1.1 and 2.2.1 (FY 2015 Q2 and FY 2015 Q3) from CyberScope

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.

Anti-Phishing & Malware Defense FY 2015 Q2 vs FY 2015 Q3

Anti-Phishing

5 of 7 capabilities must be greater than or equal to 90%:

- 12 agencies met the CAP Goal targets in Q3, up from 8 agencies in Q2.

Malware Defense

3 of 5 capabilities must be greater than or equal to 90%:

- 8 agencies met the CAP Goal targets in Q3, up from 6 agencies in Q2.

Blended Defense (combination of Anti-Phishing & Malware capabilities)

2 of 4 capabilities must be greater than or equal to 90%:

- 14 agencies met the CAP Goal targets in Q3, up from 10 agencies in Q2.

*-"Percent of email traffic processed by email systems with this functionality implemented and in use."

Anti-Phishing & Malware Defense
FY 2015 Q2 vs FY 2015 Q3

Key

Meets or exceeds Q3 target

	FY 2015 Q2			FY 2015 Q3		
	Anti-Phishing Lowest % coverage of Top 5 of 7 capabilities	Malware Defense Lowest % coverage of Top 3 of 5 capabilities	Blended Defense Lowest % coverage of Top 2 of 4 capabilities	Anti-Phishing Lowest % coverage of Top 5 of 7 capabilities	Malware Defense Lowest % coverage of Top 3 of 5 capabilities	Blended Defense Lowest % coverage of Top 2 of 4 capabilities
Agency	3.2, 3.5, 3.6, 3.7, 3.9, 3.13, 3.16	3.3, 3.4, 3.8, 3.11, 3.15	3.1, 3.10, 3.12, 3.14	3.2, 3.5, 3.6, 3.7, 3.9, 3.13, 3.16	3.3, 3.4, 3.8, 3.11, 3.15	3.1, 3.10, 3.12, 3.14
USDA	1	20	100	1	81	100
Commerce	30	50	99	25	63	100
DOD	78	93	100	15	91	100
ED	86	61	68	90	6	49
Energy	38	41	60	38	50	43
HHS	50	79	92	91	80	92
DHS	21	48	16	21	49	16
HUD	0	13	79	0	13	100
Justice	94	100	60	95	100	60
Labor	95	77	76	95	88	76
State	100	100	100	99	100	100
Interior	100	15	50	100	18	50
Treasury	70	72	99	74	94	100
DOT	100	67	85	100	100	100
VA	100	100	75	100	97	75
EPA	0	71	0	0	62	0
GSA	1	82	100	100	82	100
NASA	8	10	11	8	9	11
NSF	0	47	35	90	50	100
NRC	50	48	91	75	46	100
OPM	100	100	60	100	100	90
SBA	0	69	13	0	68	11
SSA	100	100	100	100	100	100
USAID	2	74	100	10	86	100

Note: Q2 did not have a specified targets for each metric, and the Q3 target for each metric was 90%.

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 Q2 and FY 2015 Q3) from CyberScope

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 and Weakness 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 greater than or equal to 85%.
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%. • **Blended Defense** *(combination of Anti-Phishing & Malware capabilities)*: 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**
FY 2015 CIO FISMA Annual/CAP metrics published	10/03/14	Complete	http://www.dhs.gov/publication/fy15-fisma-documents
OMB FY 2014 – FY 2015 FISMA reporting Memo released	10/03/14	Complete	http://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-01.pdf
FY 2015 Q1 FISMA/CAP metrics published	11/14/14	Complete	http://www.dhs.gov/publication/fy15-fisma-documents
FY 2015 Q1 CAP metrics reports due	1/15/15	Complete	
FY 2015 Q2 CAP metrics reports due	04/15/15	Complete	
FY 2015 CAP Goal agency targets due	07/15/15	Complete	
FY 2015 Q3 CAP metrics reports due	07/15/15	Complete	
FY 2015 Q4 CAP metrics reports due	10/31/15	In progress	Also known as the FY 2015 FISMA annual metrics due date

Key Indicators

CAP Initiatives	Area	Question No.	Question
Information Security and Continuous Monitoring	Hardware Asset Management	1.2.	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.
		1.3.	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	1.5.	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).
		1.6.	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	1.8.	Percent (%) of hardware assets listed in 1.1 assessed using credentialed scans with Security Content Automation Protocol (SCAP) validated vulnerability tools.
	Secure Configuration Management	1.7.6	Percent (%) of assets that are covered by audit activities
Identity Credential and Access Management	Unprivileged users	2.1.	How many users have unprivileged network accounts (Exclude privileged user accounts and non-user accounts.)
		2.1.1.	Percent (%) of unprivileged users technically required to log onto the network with a two-factor PIV card.
	Privileged users	2.2.	How many users have privileged network accounts? (Exclude unprivileged network accounts and non-user accounts.)
		2.2.1.	Percent (%) of privileged users technically required to log onto the network with a two-factor PIV card.

Source: FISMA Data Agency Level Questions 1.2, 1.3, 1.5, 1.6, 1.7.6, 1.8, 2.1.1, 2.21 from CyberScope

Key Indicators

CAP Initiatives	Area	Question No.	Question
Anti-Phishing & Malware Defense	Anti-Phishing	3.2.	Percent (%) of incoming email traffic analyzed for clickable URLs, embedded content, and attachments.
		3.5.	Percent (%) of email attachments opened in sandboxed environment or detonation chamber.
		3.6.	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).
		3.7.	Percent (%) of incoming emails scanned using a reputation filter tool to perform threat assessment of email sender.
		3.9.	Percent (%) of inbound email traffic passing through anti-phishing/anti-spam filtration technology at the outermost border Mail Transport Agent or email server.
		3.13.	Percent (%) of sent email that is digitally signed.
		3.16.	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	3.3.	Percent (%) of hardware assets covered by a host-based intrusion prevention system.
		3.4.	Percent (%) of hardware assets covered by an antivirus (AV) solution using file reputation services, checking files against cloud-hosted, continuously updated malware information.
		3.8.	Percent (%) of hardware assets covered by an anti-exploitation tool (e.g., Microsoft's Enhanced Mitigation Experience Toolkit (EMET) or similar).
		3.11.	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.
		3.15.	Percent (%) of remote access connections scanned for malware upon connection.
	Blended Defense	3.1.	Percent (%) of privileged user accounts that have a technical control preventing internet access.
		3.10.	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).
		3.12.	Percent (%) of outbound communications traffic checked at the external boundaries to detect covert exfiltration of information.
		3.14.	Percent (%) of email traffic quarantined or otherwise blocked.

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 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	Departement 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 Admnistration
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