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 1

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

Cybersecurity Metrics Transition

- Anti-Phishing and Malware Defense is a new CAP initiative and updates were made to the ISCM and ICAM (Strong Authentication) metrics.
- As such, the federal community is now using new baseline performance data (samples of the baseline data are available in slides #6-14) to develop new Key Performance Indicators (KPIs) and metric targets for FY 2015 – FY 2017.
- To support this effort, the Chief Information Officer (CIO) Council has formulated a working group within the Information Security and Identity Management Committee (ISIMC) to develop KPIs and metric targets.
- The new KPIs and metric targets will be available during the Quarter 3 FY 2015 reporting period.

Action Plan Summary

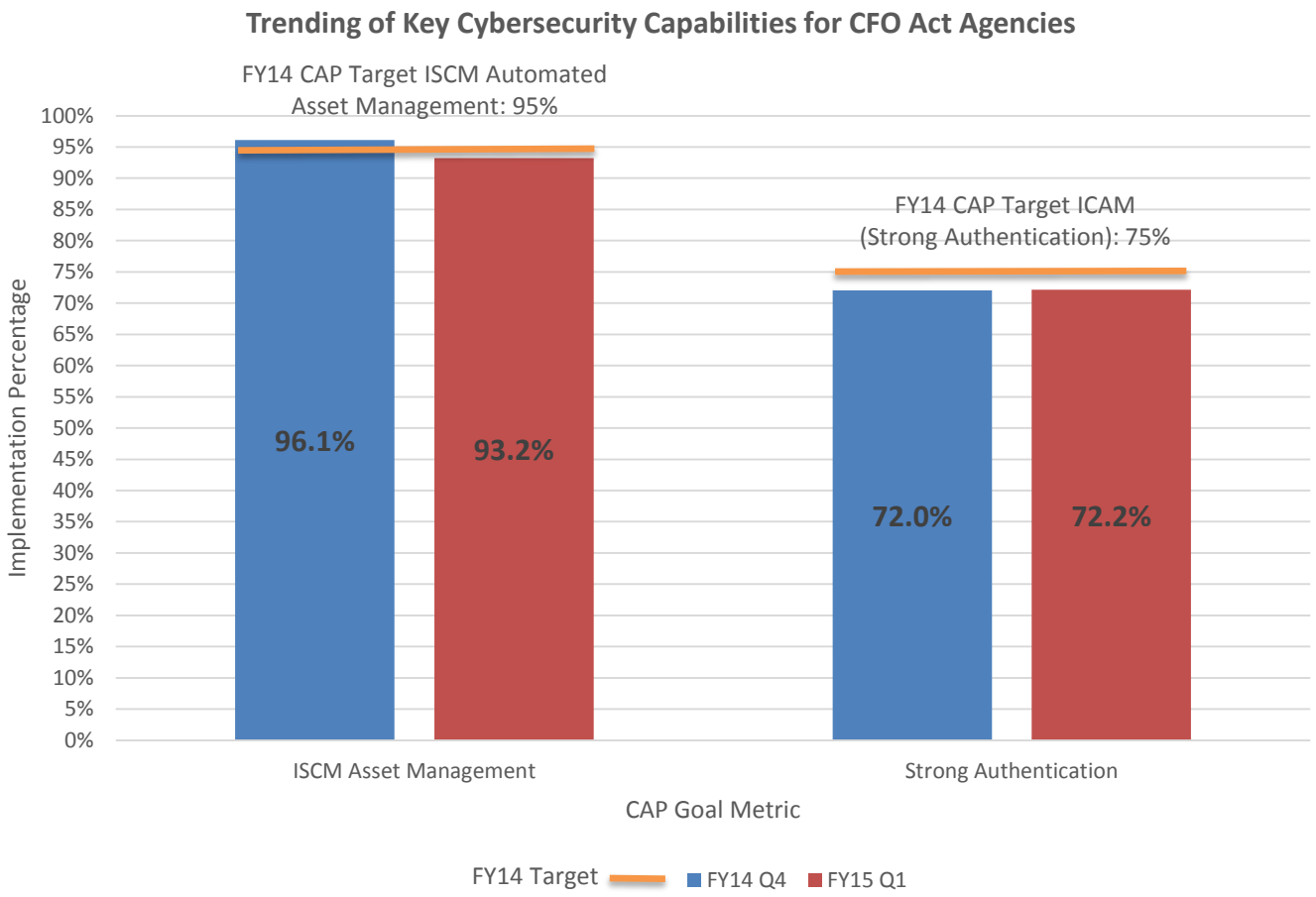
Initiative*	Major Actions to Achieve Impact	Key Indicator/Metrics
Information Security Continuous Monitoring	• Understand the hardware and software on federal networks and the risks that they pose; • Maintain ongoing, near real-time awareness of information security risks and have the capability to rapidly respond to support organizational risk management decisions.	• TBD in Q3 FY 2015 • See slide #6 and slide #8 for trending data
Identity, Credential, and Access Management (ICAM/ Strong Authentication)	• Ensure only authorized users have access to federal information systems; • Ensure only authorized users have access to information needed for designated business functions.	• TBD in Q3 FY 2015 • See slides #6-9 for trending data
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 Q3 FY 2015 • See slides #11-14 for summary preview of data

* Trusted Internet Connections (TIC) initiative from the FY 2012 – FY 2014 CAP goal process is now captured in the annual Federal Information Security Management Act (FISMA) reporting process (http://www.dhs.gov/publication/fy15-fisma-documents)

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	On Track	
FY 2015 CAP Goal agency targets due	07/15/15	On Track	Based on FY15 Q1 metric results, agencies will provide future FY15 and FY16 targets
FY 2015 Q3 CAP metrics reports due	07/15/15	Not Started	
FY 2015 Q4 CAP metrics reports due	11/16/15	Not Started	Also know as the FY15 Annual metrics collection due date

FY 2014 Q4 vs FY 2015 Q1 – Trending of Key Measures



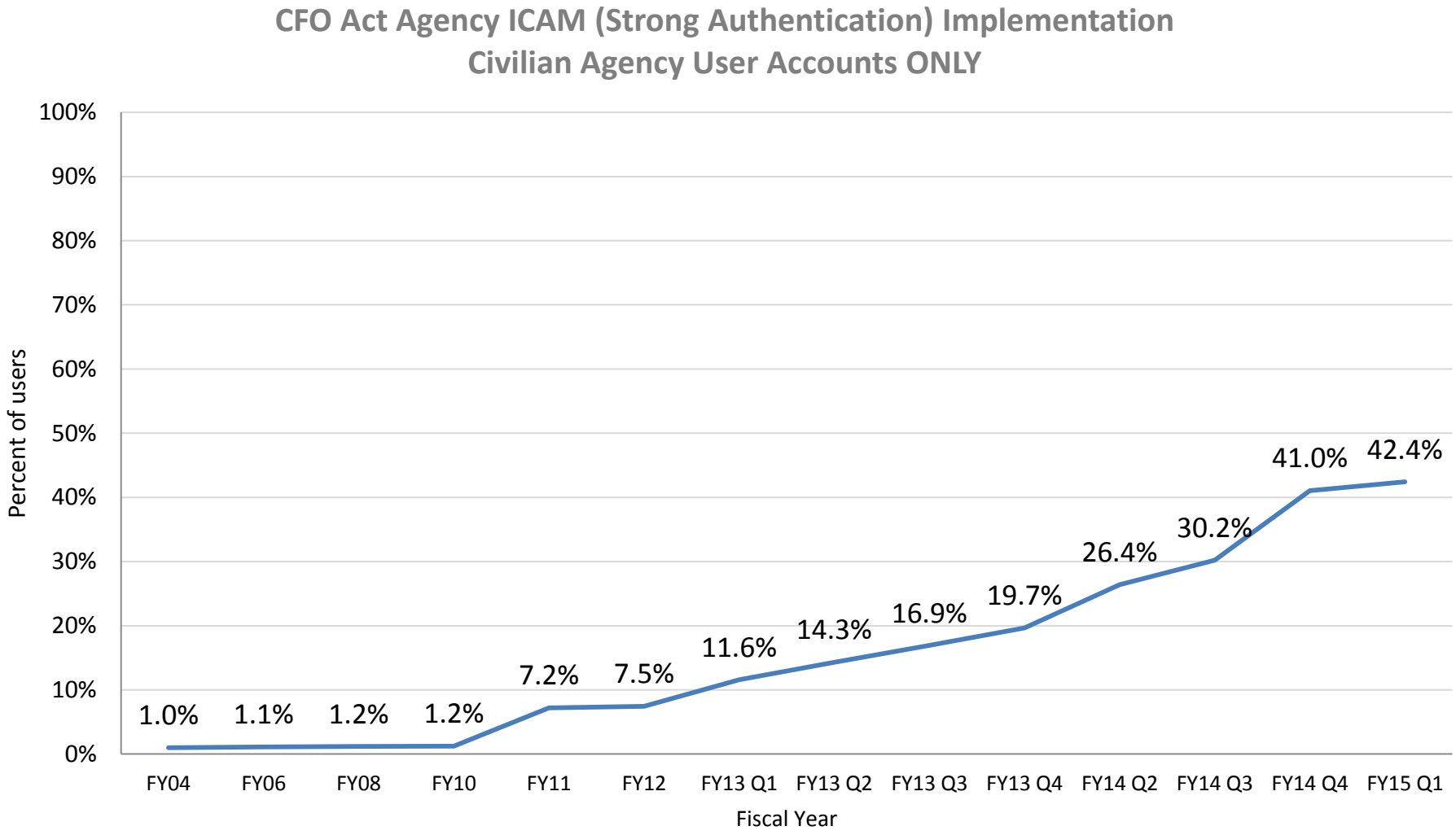
Source:
ISCM Asset Management, FISMA Data Agency Level Questions 2.1 & 2.2 (FY 14 Q4) and 1.1 & 1.3 (FY 15 Q1) from CyberScope

ICAM (Strong Authentication): FISMA Data Agency Level Questions 5.1, 5.2.5, 5.3, & 5.4.5 (FY 14 Q4) and 2.1, 2.1.1, 2.2, 2.2.1(FY 15 Q1) from CyberScope

For more details on the metrics described in this deck see FY 2014 Chief Information Officer Federal Information Security Management Act Reporting Metrics v2.0 for the FY 2014 metrics and the FISMA Quarterly 2015 Q1 CIO Reports in CyberScope for the FY 2015 metrics.

Note: Due to changes in the metrics used to collect data on configuration management and vulnerability management, these metrics cannot be directly compared from FY 2014 Q4 to FY 2015 Q1. In addition, responses to questions on TIC 2.0 Capabilities and TIC Traffic Consolidation are now only collected annually.

ICAM (Strong Authentication) Trend
Civilian Agencies ONLY



Source: FISMA Data Agency Level Questions submitted to CyberScope

FY 2014 Q4 vs FY 2015 Q1
ISCM: Automated Asset Management

	ISCM: Automated Asset Management	
CFO Act Agency	FY14 Q4	FY 15 Q1
Department of Commerce (Commerce)	86	92
Department of Homeland Security (DHS)	99	83
Department of Defense (DOD)	97	97
Department of Transportation (DOT)	96	90
Department of Education (ED)	100	84
Department of Energy (Energy)	94	86
Environmental Protection Agency (EPA)	76	61
General Services Administration (GSA)	100	100
Department of Health and Human Services (HHS)	93	95
Department of Housing and Urban Development (HUD)	93	93
Department of the Interior (Interior)	98	91
Department of Justice (Justice)	99	99
Department of Labor (Labor)	100	96
NASA	93	91
Nuclear Regulatory Commission (NRC)	89	100
National Science Foundation (NSF) NSF	100	100
Office of Personnel Management (OPM)	95	95
Small Business Administration (SBA)	100	100
Social Security Administration (SSA)	100	100
Department of State (State)	87	100
Department of the Treasury (Treasury)	99	100
US Agency for International Development (USAID)	85	90
Department of Agriculture (USDA)	99	60
Department of Veterans Affairs (VA)	94	94

Key - FY 14 Target: 95%
Meets or exceeds target
Does not meet target

Source: FISMA Data Agency Level Questions 2.1 & 2.2 (FY 14 Q4), and Questions 1.1 & 1.3 (FY 15 Q1) from CyberScope

FY 2014 Q4 vs FY 2015 Q1
ICAM (Strong Authentication)

CFO Act Agency	ICAM (Strong Authentication)					
	Unprivileged Users		Privileged Users		All Users	
	FY14 Q4	FY 15 Q1	FY14 Q4	FY 15 Q1	FY14 Q4	FY 15 Q1
Commerce	87	66	95	93	88	90
DHS	81	87	36	38	80	86
DOD	88	88	38	38	87	87
DOT	31	29	13	82	31	30
ED	85	66	84	14	85	75
Energy	29	36	25	21	29	27
EPA	75	84	0	0	69	71
GSA	100	98	0	0	95	92
HHS	73	74	4	11	69	71
HUD	0	0	0	0	0	0
Interior	37	39	16	16	36	34
Justice	44	25	27	29	44	33
Labor	0	0	0	0	0	0
NASA	84	66	1	0	82	82
NRC	0	0	0	0	0	0
NSF	16	33	66	45	19	34
OPM	0	45	100	100	1	43
SBA	0	0	0	0	0	0
SSA	84	82	99	99	85	86
State	0	14	0	4	0	14
Treasury	45	57	2	2	43	55
USAID	3	10	0	0	3	10
USDA	6	13	0	10	6	13
VA	10	10	0	0	10	10

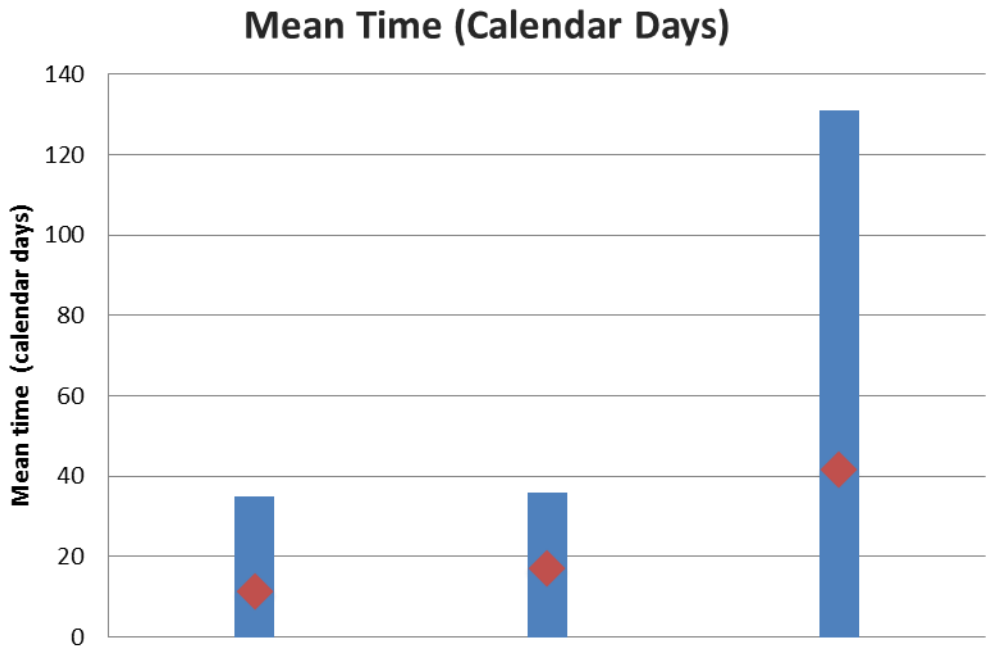
Key - FY 14 target for "All Users": 75%
Meets or exceeds target
Does not meet target

Source: FISMA Data Agency Level Questions 5.1, 5.2.5, 5.3, & 5.4.5 (FY 14 Q4) and 2.1, 2.1.1, 2.2, 2.2.1(FY 15 Q1) from CyberScope

New Metrics

- There are a number of new metrics for the FY 2015 – FY 2017 Cybersecurity CAP Goal
  - The updated ISCM metrics are aligned with the DHS Continuous Diagnostics and Mitigation (CDM) program to better identify and detect risks on agency networks
  - The updated Strong Authentication metrics allow us to better identify and protect access to federal information assets
  - The new Anti-Phishing and Malware Defense metrics were added to ensure agencies implement technologies, processes, and training to protect federal information assets from a growing cyber threat
- Since these metrics are being reported for the first time, there is variability in agency reporting, which is expected to normalize over time
- As mentioned on Slide #3, metric targets will be established by Q3 FY 2015
- The following slides identify initial Anti-Phishing and Malware Defense reporting highlights, such as: High, Low, Mean (Average), and the number of agencies reporting

FY 2015 Q1 FISMA Metrics
Mean Time Metrics

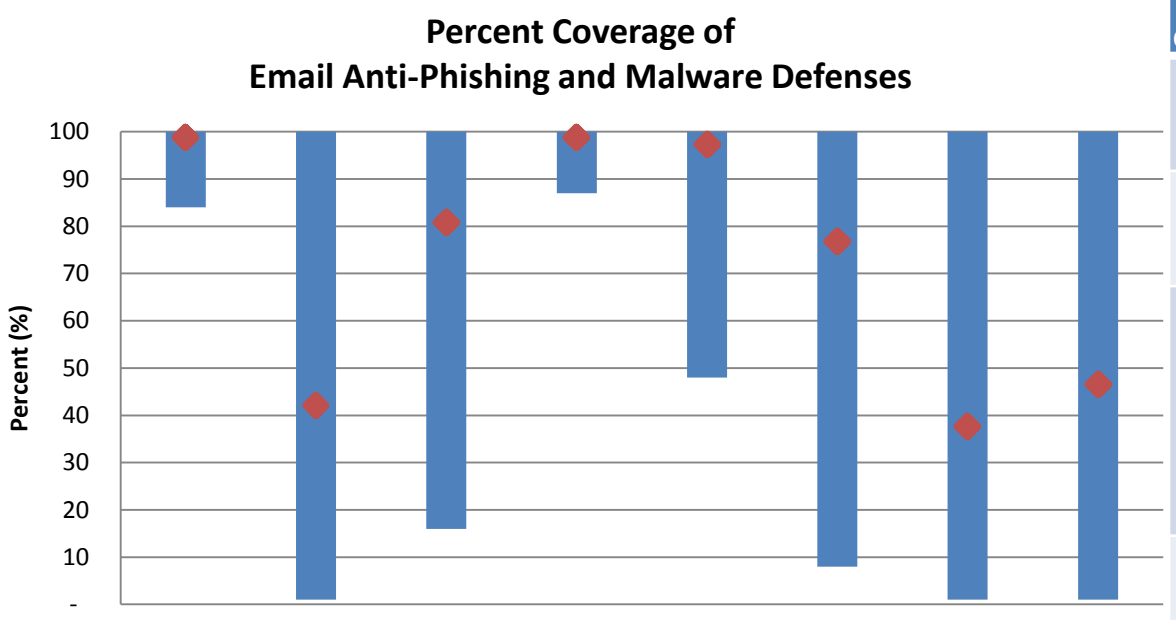


	Q 1.4	Q 1.9	Q 1.10
Agencies reporting non-zero values	20	23	22
High	30	31	126
Low	1	1	4
Mean	11	17	42

FY15 Q1 Question	Mean Time Metric (Calendar days)
Q 1.4	Mean time to detect a new device.
Q 1.9	Mean time between vulnerability scans.
Q 1.10	Mean time to mitigate for high findings.

Source: FISMA Data Agency Level Questions (FY 15 Q1) from CyberScope

FY15 Q1 FISMA Metrics
Email Anti-Phishing and Malware Defense

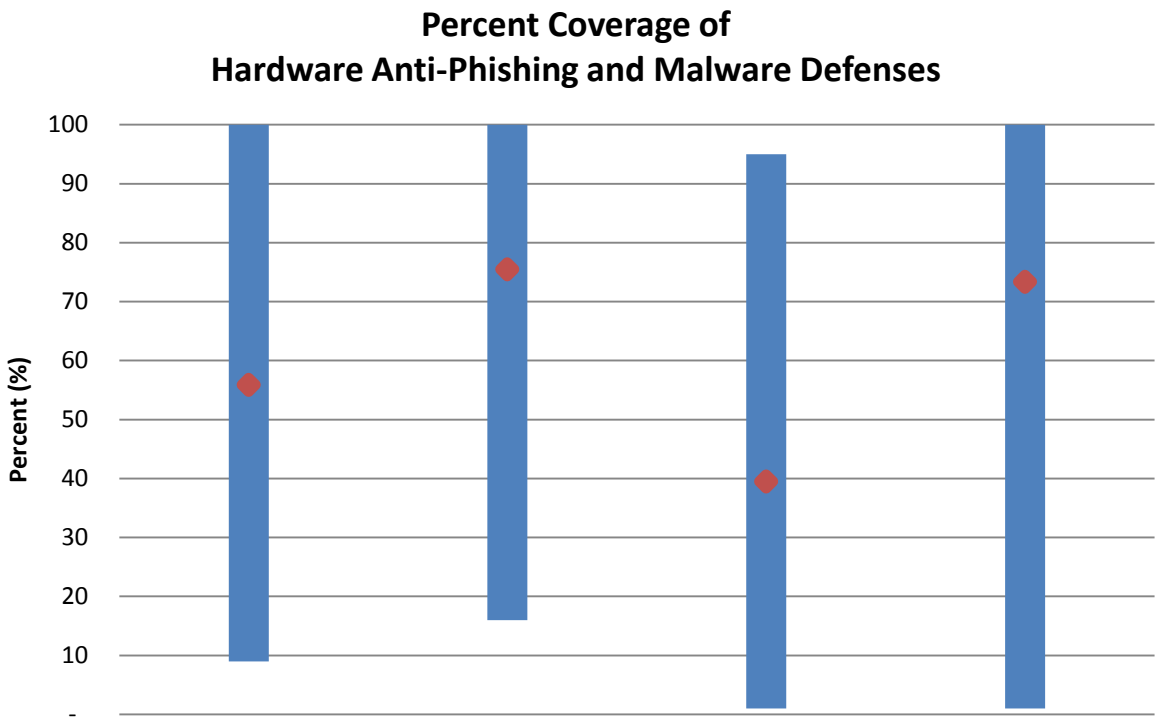


	Q 3.2	Q 3.5	Q 3.6	Q 3.7	Q 3.9	Q 3.12	Q 3.13	Q 3.14
Agencies reporting non-zero values	23	12	19	23	23	15	9	21
High	100	100	100	100	100	100	100	100
Low	84	1	16	87	48	8	1	1
Mean	99	42	81	99	97	77	38	46

FY15 Q1 Question	Anti-Phishing and Malware Defense Metric (Percent of)
Q 3.2	Incoming email traffic analyzed for clickable URLs, embedded content, and attachments.
Q 3.5	Email attachments opened in sandboxed environment or detonation chamber.
Q 3.6	Incoming emails using email sender authentication protocols such as DomainKeys Identified Mail (DKIM), Author Domain Signing Practices (ADSP), Domain-based Message Authentication, Reporting & Conformance (DMARC), Vouch by Reference (VBR), or IP Reverse (iprev).
Q 3.7	Incoming emails scanned using a reputation filter tool to perform threat assessment of email sender.
Q 3.9	Inbound email traffic passing through anti-phishing/ anti-spam filtration technology at the outermost border Mail Transport Agent or email server.
Q 3.12	Outbound communications traffic checked at the external boundaries to detect covert exfiltration of information.
Q 3.13	Sent email that is digitally signed.
Q 3.14	Email traffic quarantined or otherwise blocked.

Source: FISMA Data Agency Level Questions (FY 15 Q1) from CyberScope

FY15 Q1 FISMA Metrics
Hardware Anti-Phishing and Malware Defense

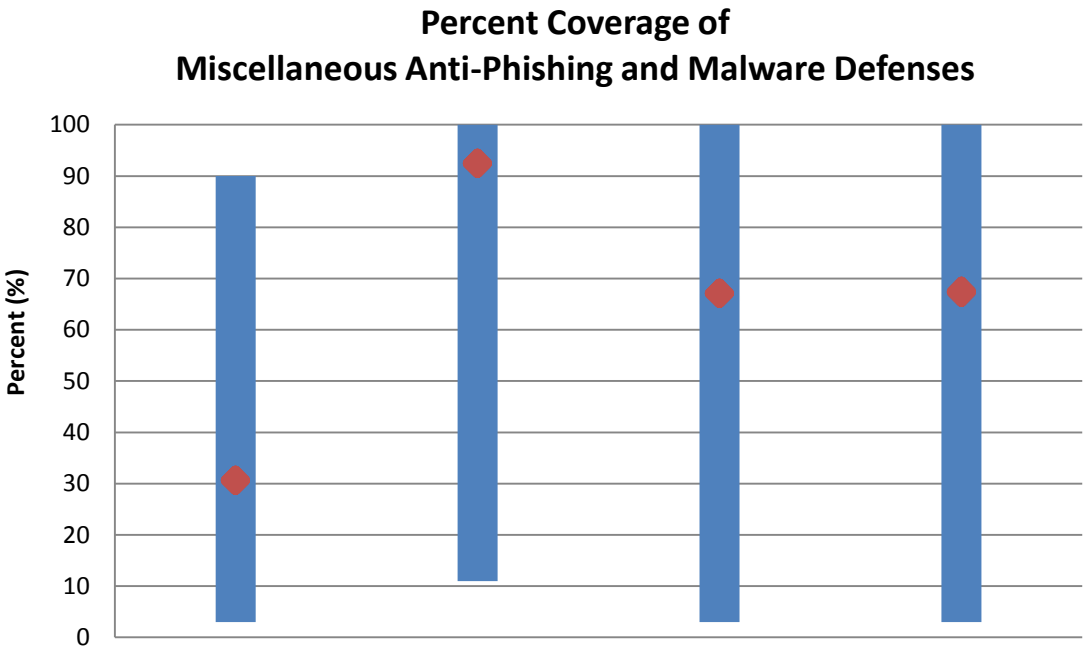


	Q 3.3	Q 3.4	Q 3.8	Q 3.11
Agencies reporting non-zero values	22	23	16	20
High	100	100	95	100
Low	9	16	1	1
Mean	56	75	40	73

FY15 Q1 Question	Anti-Phishing and Malware Defense Metric (Percent of)
Q 3.3	Hardware assets covered by a host-based intrusion prevention system.
Q 3.4	Hardware assets covered by an antivirus (AV) solution using file reputation services, checking files against cloud-hosted, continuously updated malware information.
Q 3.8	Hardware assets covered by an anti-exploitation tool. (e.g., Microsoft's Enhanced Mitigation Experience Toolkit (EMET) or similar)
Q 3.11	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.

Source: FISMA Data Agency Level Questions (FY 15 Q1) from CyberScope

FY15 Q1 FISMA Metrics
Miscellaneous Anti-Phishing and Malware Defense Metrics



	Q 3.1	Q 3.10	Q 3.15	Q 3.16
Agencies reporting non-zero values	9	21	17	13
High	90	100	100	100
Low	3	11	3	3
Mean	31	93	67	68

FY15 Q1 Question	Anti-Phishing and Malware Defense Metric (Percent of)
Q 3.1	Privileged user accounts that have a technical control preventing internet access.
Q 3.10	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).
Q 3.15	Remote access connections scanned for malware upon connection.
Q 3.16	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)

Source: FISMA Data Agency Level Questions (FY 15 Q1) from CyberScope October 1-December 31, 2014