FY15 Quarter 3
Chief Information Officer
Federal Information Security Modernization Act
Reporting Metrics
v3.1

Prepared by:

US Department of Homeland Security

Office of Cybersecurity and Communications

Federal Network Resilience

June 1, 2015

Document History

Version	Date	Comments	Author	See/Page
1.0	11/14/2014	Added clarification of remote access.	DHS FNR	13
2.0	02/06/2015	Updated all references to FY15 CIO Q2 Metrics. No other reporting changes.	DHS FNR	All
3.0	02/10/2015	Updated all references to FY15 CIO Q3 Metrics. No other reporting changes.	DHS FNR	All
3.1	06/01/2015	Updated Appendix A and added Appendices B and C.	DHS FNR	11-18

GENERAL INSTRUCTIONS

Responsibilities

Organization[1] heads are responsible the Federal Information Security Modernization Act of 2014 (FISMA) and have full authority to require reporting by their components that form their enterprise.

Fiscal Year (FY) 15 FISMA Metric Development Process

While we move the Federal government toward information security continuous monitoring solutions, such as Continuous Diagnostics and Mitigation (CDM), it is important that we take appropriate actions to continue making the current direct-entry reporting methods less burdensome to Departments and Agencies (D/As) and to improve the quality of the data being reported. The current FISMA Chief Information Officer (CIO) metrics have been improved to provide more value to congressional and executive audiences, as well as, individual D/As.

In coordination with the Office of Management and Budget (OMB) and the National Security Council (NSC) staff, the Federal Network Resilience (FNR) Division of the Department of Homeland Security (DHS) is developing long-term solutions to automate the CIO reporting process by leveraging the benefits of emerging continuous monitoring capabilities and other data collection mechanisms. This year DHS/FNR facilitated an online collaborative effort incorporating the input of more than 100 cybersecurity professionals from over 24 D/As utilizing an Agile methodology. The goal of this effort was to improve the validity, quality, and efficiency of cybersecurity governance data and collection efforts. The participating cybersecurity professional made over 200 recommendations, and the DHS/FNR cybersecurity experts incorporated these recommendations into this set of FY15 CIO Annual FISMA Metrics.

This set of metrics, for use in FY15 Quarterly reporting, represents a selection of Administration Priority metrics derived from the FISMA FY15 CIO Annual metrics. OMB requires CFO-Act agencies report quarterly per OMB M-15-01. A full set of the Annual CIO Metrics, with accompanying definitions, references, and guidance may be found here. Appendix A provides a correlation of the Quarterly and Annual metric question sets and additional metric context. Appendix B provides the summary of the CAP Goal Targets and Methodology for FY15 through FY17. Additionally, Appendix C captures the D/As' quarterly and annual FISMA CAP Goal targets from Q3 FY15 through Q4 FY17. This Action Plan performance data will be submitted to CyberScope during Q3 FY15 quarterly FISMA reporting period of July 1, 2015 through July 15, 2015.

[1] The term "organization" refers to each Federal D/A that is a reporting unit under CyberScope.

Expected Levels of Performance

Cross-Agency Priorities (CAP)

The expected levels of performance for CAP FISMA metrics are based on review and input from multiple cybersecurity experts as well as threat information from public, private, and intelligence sources.[2] Q1 and Q2 FY15 were used to establish a baseline to generate a scoring methodology and targets for the CAP goals (See Appendix B: Summary of FISMA CAP Goal Targets and Methodology). The Administration's Priority (AP) cybersecurity capabilities are currently:

- Information Security Continuous Monitoring (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.
- Anti-phishing and Malware Defense (APMD)—Implement technologies, processes and training that reduce the risk of malware introduced through email and malicious or compromised web sites.

Key FISMA Metrics (KFM)

The expected level of performance for these metrics is defined as "adequate security," which means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of government information. This includes assuring that systems and applications used by the organization operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.[3]

[2] See Cross-Agency Priority Goals for further details.
[3] Office of Management and Budget (OMB) Circular No. A-130, Appendix III.

Baseline Questions

These questions establish current performance against which future performance may be measured. There is no expected level of performance for baseline questions. Some baseline questions are also intended to determine whether such future performance measures are needed. Offices of the Inspector General (OIG) should not assume that these questions define any specific organizational performance standard for 2015.

National Institute of Standards and Technology Special Publication (NIST SP) 800 Revisions

For legacy information systems, D/As are expected to be in compliance with NIST guidelines within one year of the publication date. D/As must become compliant with any new or updated materials in revised NIST guidelines within one year of the revision. For information systems under development or for legacy systems undergoing significant changes, D/As are expected to be in compliance with the NIST publications immediately upon deployment of the information system. Each D/A should consider its ability to meet this requirement when developing the Plan of Action and Milestones (POA&M).

Federal Information Processing Standards (FIPS) Versions

References in this document to FIPS Standards refer to the latest (non-draft) published version.

1. INFORMATION SECURITY CONTINUOUS MONITORING

Purpose and Use

- OMB M-14-03 directs D/As to implement continuous monitoring of security controls as part of a phased approach through FY17.
- At the level of the Federal enterprise, the current metrics aim to provide situational awareness as to where agencies stand with implementing and operating continuous monitoring as it is envisioned by NIST SP 800-137, DHS Continuous Diagnostics and Mitigation (CDM), and the Information Security Continuous Monitoring (ISCM) Concept of Operations (CONOPS).
- The ISCM CONOPS recommends that asset management is one of the first areas where continuous monitoring needs to be developed. Organizations must first know about devices and software (both authorized/managed and unauthorized/unmanaged) before they can manage the devices/software for configuration and vulnerabilities.
- A key goal of ISCM is to make hardware assets harder to exploit through hardware asset management, software asset management, secure configuration management, and vulnerability management.

Hardware Asset Management

1.1. What is the total number of the organization's hardware assets connected to the organization's unclassified[4] network(s)?[5] (Base)

1.1.1. What is the total number of endpoints connected to the organization's unclassified network(s)? (Base)

1.2. 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. (AP)

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. (AP)

1.4. What is the mean time[6] to detect a new device (time between scans in 1.2)? (AP)

[4] "Unclassified" refers to low impact (non-sensitive) and sensitive but unclassified (SBU) data.
[5] Unless specified otherwise in a footnote, add numbers across networks and organizational components to get the reportable result.
[6] Mean time is measured in calendar days.

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). (AP)

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).[7] (AP)

Secure Configuration Management (SecCM)

1.7. Please complete Table 1. Future configurations will be added as needed. Data calls for layer 2, layer 3, mobile, printers, or other devices or operating systems will be used as needed.

List of top U.S. Government Operating Systems, as reported in SCAP feeds	1.7.1 What is the number of hardware assets with each OS? (Base)	1.7.2 What is the common security configuration baseline for each OS listed? (Base) (e.g. USGCB)	1.7.3 How many configuration exceptions are granted by the enterprise? (Base)	1.7.4 What is organization's enterprise policy for maximum audit interval (target)? (Base)	1.7.5 What is organization's enterprise average audit interval (actual)? (AP)	1.7.6 Percent (%) of assets in 1.7.1 covered by the auditing activities described in 1.7.4 and 1.7.5. (AP)
Windows 8.x						
Windows 7.x						
Windows Vista						
Windows Unsupported (include XP)						
Windows Server 2003						
Windows Server 2008						
Windows Server 2012						
Linux (all versions)						
Unix / Solaris (all versions)						
Mac OS X						

Table 1: Metric 1.7.1-1.7.6

[7] This may include software whitelisting tools that identify executable software by a digital fingerprint and selectively block these. It might also include sandboxing of mobile code to determine before execution whether to allow it to run, where static files do not allow whitelisting. In general, any method included should be able to block zero-day and Advanced Persistent Threats (APT).

Vulnerability and Weakness Management

1.8. Percent (%) of hardware assets listed in 1.1 assessed using credentialed scans with Security Content Automation Protocol (SCAP) validated vulnerability tools. (AP)[8]

1.9. What is the mean time[9] between vulnerability scans? (AP)

1.10. What is the mean time[10] to mitigate for high[11] findings? (AP)

2. IDENTITY CREDENTIAL AND ACCESS MANAGEMENT

Purpose and Use

- Strong information system and physical access authentication requires multiple factors to securely authenticate a user. A single-factor authentication mechanism, such as a username and password, is insufficient to block even basic attackers.
- Enhanced identity management solutions also support the adoption of additional non-security benefits, such as single sign-on, more accountable and efficient use of systems, and enhanced identity capabilities through use of electronic signatures for legal and non-repudiation needs.
- A key goal of ICAM is to strike a proper balance between data access "need-to-know" and "need-to-share" making sure that access rights are given only to the intended individuals and/or processes.[12]
- For more information regarding PIV eligibility, please see the OPM's Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12 here.

[8] Vulnerability scanning tools are SCAP validated – assets are not.

[9] Mean time is measured in calendar days.

[10] Mean time is measured in calendar days.

[11] The National Vulnerability Database (NVD) provides severity rankings of "Low" "Medium" and "High" for all Common Vulnerabilities and Exposures (CVE) in the database. The NVD is accessible at http://nvd.nist.gov.

[12] The process to establish an individual's access rights first determines that the individual has a need to know, assigns appropriately restricted access rights, and uses the individual's digital identity to authenticate the individual, then grants access rights.

Unprivileged Network Users

2.1. How many users have unprivileged network accounts (Exclude privileged user accounts and non-user accounts.) (Base)

2.1.1. Percent (%) of users from 2.1 technically required to log onto the network with a two-factor PIV card.[13] (AP)

Privileged Network Users

2.2. How many users have privileged network accounts? (Exclude unprivileged network accounts and non-user accounts.) (KFM)

2.2.1. Percent (%) of users from 2.2 technically required to log onto the network with a two- factor PIV card.[14] (AP)

[13] For a person with one or more unprivileged network accounts, the person should be counted in the percentage only if a two-factor PIV card is necessary to authenticate to all network accounts. The enforcement of authentication may be accomplished via either user based or machine based configuration settings.

[14] For a person with one or more privileged network accounts, the person should be counted in the percentage only if a two-factor PIV card is necessary to authenticate to all network accounts. The enforcement of authentication may be accomplished via either user based or machine based configuration settings.

3. ANTI-PHISHING AND MALWARE DEFENSE

Purpose and Use

- Due to the preponderance of phishing attacks and their steadily increasing frequency and sophistication, anti-phishing and malware defense was added as a Cross-Agency Priority (CAP) goal beginning in FY15. United States Computer Emergency Readiness Team (US-CERT) and National Security Agency (NSA) both identified phishing as one of the top threat vectors putting Federal Departments and Agencies at risk.
- Phishing metrics are designed to assess maturity across a variety of anti-phishing techniques, including filtering of emails used to deliver malicious content, network-level defenses, endpoint-level defenses[15], and training.
- Gateway defenses are the first line of defense in protecting organization networks, and enterprise level solutions are necessary to block/filter the majority of phishing attempts, including web content filtering, mail filtering, and mail verification.
- Phishing attacks seek to convince users to provide information or access needed for an attacker to steal information or compromise a network. It is important for users to understand, be able to identify, and be able to protect themselves from phishing attacks.

3.1. Percent (%) of privileged user accounts that have a technical control preventing internet access. (AP)

3.2. Percent (%) of incoming email traffic analyzed for clickable URLs, embedded content, and attachments. (AP)

3.3. Percent (%) of hardware assets covered by a host-based intrusion prevention system. (AP)

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. (AP)

3.5. Percent (%) of email attachments opened in sandboxed environment or detonation chamber. (AP)

[15] Endpoint-level defenses provide another layer in a defense-in-depth approach to help mitigate phishing attacks in the event that an attack gets through gateway defenses.

3.6. Percent (%) of 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). (AP)

3.7. Percent (%) of incoming emails scanned using a reputation filter[16] tool to perform threat assessment of email sender. (AP)

3.8. Percent (%) of hardware assets covered by an anti-exploitation tool (e.g., Microsoft's Enhanced Mitigation Experience Toolkit (EMET) or similar). (AP)

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. (AP)

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). (AP)

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. (AP)

3.12. Percent (%) of outbound communications traffic checked at the external boundaries to detect covert exfiltration of information. (AP)

3.13. Percent (%) of sent email that is digitally signed. (AP)

3.14. Percent (%) of email traffic quarantined or otherwise blocked. (AP)

3.15. Percent (%) of remote access connections scanned for malware upon connection. (AP)

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). (AP)

[16] Outer layer of email protection filters potentially malicious email based on sender reputation, sender IP address, or other sender information.

Appendix A: Quarterly to Annual CIO Metric Correlation and Additional Metric Context

FY15 Quarterly FISMA CIO Metrics	FY15 Annual FISMA CIO Metrics	Metric	Context
Information Security Continuous Monitoring (ISCM)			
1.1	2.1	What is the total number of the organization's hardware assets connected to the organization's unclassified network(s)? (Base)	N/A
1.1.1	2.1.2	What is the total number of endpoints connected to the organization's unclassified network(s)? (Base)	N/A
1.2	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. (AP)	As it relates to FISMA, network fabric is defined as the overall total of the Agency's networked hardware assets. This includes the network topology of the organization, such as servers, storage, client machines, and other networked assets in a cohesive switched infrastructure. This may also be referred to as the Agency's network infrastructure(s). Portions of the network fabric that implement compensating controls such as disabling unused ports should be counted as meeting the intent of this metric.
1.3	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. (AP)	As it relates to FISMA, network fabric is defined as the overall total of the Agency's networked hardware assets. This includes the network topology of the organization, such as servers, storage, client machines, and other networked assets in a cohesive switched infrastructure. This may also be referred to as the Agency's network infrastructure(s).

FY15 Quarterly FISMA CIO Metrics	FY15 Annual FISMA CIO Metrics	Metric	Context
1.4	2.4	What is the mean time to detect a new device (time between scans in 1.2)? (AP)	N/A
1.5	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). (AP)	N/A
1.6	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). (AP)	N/A
1.7	2.10	Please complete Table 1. Future configurations will be added as needed. Data calls for layer 2, layer 3, mobile, printers, or other devices or operating systems will be used as needed.	N/A
1.8	2.11	Percent (%) of hardware assets listed in 1.1 assessed using credentialed scans with Security Content Automation Protocol (SCAP) validated vulnerability tools. (AP)	Credentialed scans are only required for assets that recognize credentials. For other assets (e.g., printers), agencies should include the percentage of these assets that undergo any vulnerability scan with Security Content Automation Protocol (SCAP) validated vulnerability tools.
1.9	2.12	What is the mean time between vulnerability scans? (AP)	Based on credentialed scans in 1.8
1.10	2.14	What is the mean time to mitigate for high findings? (AP)	Based on credentialed scans in 1.8
Identity and Credential Access Management (ICAM)			
2.1	3.1	How many users have unprivileged network accounts (Exclude privileged user accounts and non-user accounts.) (Base)	Total (2.1) = (number of users technologically required to log onto the network with a two-factor PIV card) + (number of users with PIV cards, but not required to use it) + (number of users without PIV cards).

FY15 Quarterly FISMA CIO Metrics	FY15 Annual FISMA CIO Metrics	Metric	Context
2.1.1	3.1.1	Percent (%) of users from 2.1 technically required to log onto the network with a two-factor PIV card. (AP)	100% (2.1.1) = Percent (%) of users from 2.1 technologically required to log onto the network with a two-factor PIV card. Please note the context information for 2.1. A policy document requiring PIV use is not sufficient.
2.2	3.2	How many users have privileged network accounts? (Exclude unprivileged network accounts and non-user accounts.) (KFM)	Total (2.2) = (number of users technologically required to log onto the network with a two-factor PIV card) + (number of users with PIV cards, but not required to use it) + (number of users without PIV cards).
2.2.1	3.2.1	Percent (%) of users from 2.2 technically required to log onto the network with a two-factor PIV card. (AP)	100% (2.2.1) = Percent (%) of users from 2.2 technologically required to log onto the network with a two-factor PIV card. Please note the context information for 2.2. A policy document requiring PIV use is not sufficient.
Anti-Phishing and Malware Defense (APMD)			
3.1	4.1	Percent (%) of privileged user accounts that have a technical control preventing internet access. (AP)	Based on user accounts from 2.2
3.2	4.2	Percent (%) of incoming email traffic analyzed for clickable URLs, embedded content, and attachments. (AP)	Percent of email traffic processed by email systems with this functionality implemented and in use.
3.3	4.3	Percent (%) of hardware assets covered by a host-based intrusion prevention system. (AP)	Based on assets in 1.1
3.4	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. (AP)	Based on assets in 1.1.1 Percent (%) of hardware assets covered by an antivirus (AV) or "intrusion prevention solution" using file reputation services, checking files against cloud-hosted, continuously updated malware information.

FY15 Quarterly FISMA CIO Metrics	FY15 Annual FISMA CIO Metrics	Metric	Context
3.5	4.5	Percent (%) of email attachments opened in sandboxed environment or detonation chamber. (AP)	Percent of email traffic processed by email systems with this functionality implemented and in use.
3.6	4.6	Percent (%) of 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). (AP)	Percent of email traffic processed by email systems with this functionality implemented and in use.
3.7	4.7	Percent (%) of incoming emails scanned using a reputation filter tool to perform threat assessment of email sender. (AP)	Percent of email traffic processed by email systems with this functionality implemented and in use.
3.8	4.8	Percent (%) of hardware assets covered by an anti-exploitation tool (e.g., Microsoft's Enhanced Mitigation Experience Toolkit (EMET) or similar). (AP)	Based on assets in 1.1
3.9	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. (AP)	Percent of email traffic processed by email systems with this functionality implemented and in use.
3.10	4.10	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). (AP)	N/A
3.11	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. (AP)	Based on assets in 1.1.1
3.12	4.12	Percent (%) of outbound communications traffic checked at the external boundaries to detect covert exfiltration of information. (AP)	N/A

FY15 Quarterly FISMA CIO Metrics	FY15 Annual FISMA CIO Metrics	Metric	Context
3.13	4.13	Percent (%) of sent email that is digitally signed. (AP)	This is not to collect the percent of email messages digitally signed by individuals' certs; rather, it is the outbound equivalent to "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)". This metric is to track the percent of email processed by email systems with this functionality implemented and in use.
3.14	4.14	Percent (%) of email traffic quarantined or otherwise blocked. (AP)	Percent of email traffic processed by email systems with this functionality implemented and in use.
3.15	6.1.4	Percent (%) of remote access connections scanned for malware upon connection. (AP)	Remote access connections are defined as the ability for an organization's users to access its non-public computing resources from locations external to the organization's facilities. This applies to remote access solutions that protect access to the organization's desktop LAN/WAN resources and services. Remote access excludes non-GFE systems using externally facing applications (e.g., Outlook Web Access, Remote Desktop/Citrix Solutions, Good Messaging, etc.).

FY15 Quarterly FISMA CIO Metrics	FY15 Annual FISMA CIO Metrics	Metric	Context
3.16	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). (AP)	N/A

Table 2: FY15 FISMA Metrics and Context

Appendix B: Summary of FISMA CAP Goal Targets & Methodology

Appendix B provides a summary of the FISMA CAP Goal Metric Targets and methodology for Information Security Continuous Monitoring (ISCM), Strong Authentication (ICAM), and Anti-Phishing and Malware Defense.

Summary of FISMA CAP Goal Targets & Methodology				
Capability	**Target %**	**FY15 Quarterly FISMA CIO Metrics**	**FY15 Annual FISMA CIO Metrics**	**Agency Calculation**
Information Security Continuous Monitoring (ISCM)				
Hardware Asset Management	≥ 95%	1.2, 1.3	2.2, 2.3	Both results must be greater than or equal to target
Software Asset Management	≥ 95%	1.5, 1.6	2.6, 2.7	Both results must be greater than or equal to target
Vulnerability and Weakness Management	≥ 95%	1.8	2.11	Result must be greater than or equal to target
Secure Configuration Management:	≥ 95%	1.7.6	2.10.6	Result must be greater than or equal to target
Identity and Credential Access Management (ICAM)				
Unprivileged Network Users	≥ 85%	2.1.1.	3.1.1	Result must be greater than or equal to target
Privileged Network Users	> 85%	2.2.1	3.2.1	Result must be greater than target
Anti-Phishing and Malware Defense				
Anti-Phishing Defense	≥ 90%	3.2, 3.5, 3.6, 3.7, 3.9, 3.13, 3.16	4.2, 4.5, 4.6, 4.7, 4.9, 4.13, 8.2.1	Top 5 results must be greater than or equal to target
Malware Defense	≥ 90%	3.3, 3.4, 3.8, 3.11, 3.15	4.3, 4.4, 4.8, 4.11, 6.1.4	Top 3 results must be greater than or equal to target
Blended Defense	≥ 90%	3.1, 3.10, 3.12, 3.14	4.1, 4.10, 4.12, 4.14	Top 2 results must be greater than or equal to target

Table 3: Summary of CAP Goal Target & Methodology

Appendix C: Agency Plan of Action for CAP Cybersecurity Capabilities

Agencies are asked to populate Section I (refer to Figure 1) to demonstrate D/A progress in working towards implementation maturity of the FISMA CAP Goal Targets (refer to Appendix B) through FY17. For Hardware Asset Management, Software Asset Management, Anti-Phishing Defense, Malware Defense, and Blended Defense, the lowest performing metric applicable to the Cybersecurity Capability shall be used to determine the Agency's internal target. The D/As' action plan performance data will be submitted to CyberScope during Q3 FY15 quarterly FISMA reporting period of July 1, 2015 through July 15, 2015.

Agencies should indicate their planned percentage complete for the capability in Section 1 for each fiscal year quarter indicated through Q4 FY17 or through the quarter when the respective targets are to be met. The space in the last column in Section 1 is allocated for agency comments in regards to their implementation schedule.

Below is a copy of the FY15-FY17 Action Plan template that agencies are required to populate in CyberScope with their performance plan data.

AGENCY PLAN OF ACTION TEMPLATE FOR CYBERSECURITY CAPABILITIES												
SECTION 1. AGENCY PROGRESS												
Agency Internal Target												
CAPABILITIES	CAP Goal Targets	Q3FY15	Q4FY15	Q1FY16	Q2FY16	Q3FY16	Q4FY16	Q1FY17	Q2FY17	Q3FY17	Q4FY17	AGENCY COMMENTS
Hardware Asset Management	95%											
Software Asset Management	95%											
Vulnerability and Weakness Management	95%											
Secure Configuration Management	95%											
Unprivileged Network Users	85%											
Privileged Network Users	85%											
Anti-Phishing Defense	90%											
Malware Defense	90%											
Blended Defense	90%											

Figure 1: Agency Plan of Action Template for Cybersecurity Capabilities