FY15 Quarter 1
Chief Information Officer
Federal Information Security Management Act
Reporting Metrics
V1.0

Prepared by:

US Department of Homeland Security

Office of Cybersecurity and Communications

Federal Network Resilience

November 14, 2014

Document History

Version	Date	Comments	Author	See/Page
0.1	10/29/2014	Initial Draft of FY15 CIO Q1 FISMA Metrics	P. Morimoto B. Frey J. McGrath C. Chase A. Heydman	All
0.2	11/10/2014	Added new appendix with calculations	J. McGrath B. Frey	12
1.0	11/14/2014	Added clarification of remote access	FNR CPM	13

Name:	FY 2015 Chief Information Officer Q1 Federal Information Security Management Act Reporting Metrics
Created:	October 29, 2014
Authors:	Paige Morimoto, Brian Frey, Jim McGrath, Craig Chase, Amy Heydman
Branch:	Cybersecurity Performance Management
Division:	Federal Network Resilience

GENERAL INSTRUCTIONS

RESPONSIBILITIES

Organization[1] heads are responsible for complying with the Federal Information Security Management Act of 2002 (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 (ISCM) 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. However, FNR knows there are opportunities in the short-term to improve the FISMA cybersecurity metrics. This year DHS/FNR did so by facilitating 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 FY 2015 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 B provides a correlation of the Quarterly and Annual metric question sets.

[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 will be used to establish a baseline that will then be used to generate a future scoring methodology for the CAP goals (See Appendix 1). The Administration's Priority (AP) cybersecurity capabilities are currently:

- Information Security Continuous Monitoring—Provide ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity: posture, hygiene, and operational readiness.
- Identity Credential and Access Management—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—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]

In compliance with OMB FISMA guidance (M-11-33, FAQ 15), the D/A head is responsible for determining the acceptable level of risk, with input from system owners, program officials, and CIOs.

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

[2] See Cross-Agency Priority Goals for further details.
[3] Office of Management and Budget (OMB) Circular A-130, Appendix III, definitions

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

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)

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)

[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.

[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 APT threats.

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.

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)

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

[9] Mean time is measured in calendar days.

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

2. IDENTITY CREDENTIAL AND ACCESS MANAGEMENT

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[12]. (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[13]. (AP)

3. ANTI-PHISING AND MALWARE DEFENSE

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)

[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] For a person with one or more unprivileged network accounts, the person should be counted in the percentage only if the person is required to use a two-factor PIV card to authenticate to all network accounts. User-based Enforcement (UBE) at the user account level and Machine-based Enforcement (MBE) solutions that adhere to the principles of Identity and Access Management are counted as PIV-enabled for HSPD-12 reporting.

[13] For a person with one or more privileged network accounts, the person should be counted in the percentage only if the person is required to use a two-factor PIV card to authenticate to all network accounts. User-based Enforcement (UBE) at the user account level and Machine-based Enforcement (MBE) solutions that adhere to the principles of Identity and Access Management are counted as PIV-enabled for HSPD-12 reporting.

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

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[14] 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)

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

Appendix A: Correlation of the Quarterly and Annual Metric Question Sets

FY15 Quarterly FISMA CIO Metrics	FY 15 Annual FISMA CIO Metrics	FY15 Quarterly FISMA Metric
1.1	2.1	What is the total number of the organization's hardware assets connected to the organization's unclassified network(s)? (Base)
1.1.1	2.1.2	What is the total number of endpoints connected to the organization's unclassified network(s)? (Base)
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)
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)
1.4	2.4	What is the mean time to detect a new device (time between scans in 1.2)? (AP)
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)
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)
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.
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)
1.9	2.12	What is the mean time between vulnerability scans? (AP)
1.10	2.14	What is the mean time to mitigate for high findings? (AP)
2.1	3.1	How many users have unprivileged network accounts (Exclude privileged user accounts and non-user accounts.) (Base)
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)

2.2	3.2	How many users have privileged network accounts? (Exclude unprivileged network accounts and non-user accounts.) (KFM)
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)
3.1	4.1	Percent (%) of privileged user accounts that have a technical control preventing internet access. (AP)
3.2	4.2	Percent (%) of incoming email traffic analyzed for clickable URLs, embedded content, and attachments. (AP)
3.3	4.3	Percent (%) of hardware assets covered by a host-based intrusion prevention system. (AP)
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)
3.5	4.5	Percent (%) of email attachments opened in sandboxed environment or detonation chamber. (AP)
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)
3.7	4.7	Percent (%) of incoming emails scanned using a reputation filter tool to perform threat assessment of email sender. (AP)
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)
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)
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)
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)
3.12	4.12	Percent (%) of outbound communications traffic checked at the

		external boundaries to detect covert exfiltration of information. (AP)
3.13	4.13	Percent (%) of sent email that is digitally signed. (AP)
3.14	4.14	Percent (%) of email traffic quarantined or otherwise blocked. (AP)
3.15	6.1.4	Percent (%) of remote access connections scanned for malware upon connection. (AP)
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)

Appendix B: Metric Algorithms/Additional Calculations Context

Metric Number	Metric	Context
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.	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).
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.	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).
1.9	What is the mean time between vulnerability scans?	Based on credentialed scans in 1.8
1.10	What is the mean time to mitigate for high findings?	Based on credentialed scans in 1.8 Time from identification/detection to Mitigated (remediated and/or compensating controls in place).
2.1.1	Percent (%) of users from 2.1 technically required to log onto the network with a two-factor PIV card.	100% = (2.1.1 Percent (%) of users from 2.1 technically required to log onto the network with a two-factor PIV card) + (Percent (%) of users from 2.1 with PIV cards, but not technically required to use it for two-factor authentication)+ (Percent (%) of users from 2.1 without PIV cards)
2.2.1	Percent (%) of users from 2.2 technically required	100% = (2.2.1 Percent (%) of

	to log onto the network with a two-factor PIV card.	users from 2.2 technically required to log onto the network with a two-factor PIV card) + (Percent (%) of users from 2.2 with PIV cards, but not technically required to use it for two-factor authentication)+ (Percent (%) of users from 2.2 without PIV cards)
3.1	Percent (%) of privileged user accounts that have a technical control preventing internet access.	Based on user accounts from 2.2
3.3	Percent (%) of hardware assets covered by a host-based intrusion prevention system.	Based on assets in 1.1
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.	Based on assets in 1.1
3.8	Percent (%) of hardware assets covered by an anti-exploitation tool.	Based on assets in 1.1
3.11	Percent (%) of hardware assets that have implemented a browser-based or enterprise-based tool to block known phishing websites and IP addresses.	Based on assets in 1.1
3.14	Percent (%) of email traffic quarantined or otherwise blocked.	Total Inbound messages
3.15	Percent (%) of remote access connections scanned for malware	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.).

Appendix C: CAP Goal Scoring

This section is a placeholder for FY15Q1 and Q2 reporting periods. By FY15Q3, it is anticipated that scoring and baseline metrics will be developed and documented in this section.