FY14 Q2

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

December 2, 2013

Document History

Version	Date	Comments	Author	Sec/Page
1.0	12/2/13	Initial release of FY14 CIO Q2 FISMA metrics	D. Waller	All

NAME: FY 2014 Chief Information Officer Q2 Federal Information Security Management Act Reporting Metrics

CREATED: December 2, 2013
AUTHORS: Dominique Waller
BRANCH: Federal Network Resilience
PROGRAM: Cybersecurity Performance Management

GENERAL INSTRUCTIONS

The majority of the FY14 Q2 metrics are based on the Administration Priorities. Please see the table below depicting the questions that are aligned to the Administration Priorities.

Administration Priority Area	Section	Performance Metric	Target Level for 2014
Continuous[1] Monitoring – Assets	1.2	% of assets in 1.1, where an automated capability (device discovery process) provides visibility at the organization's enterprise level into asset inventory information for all hardware assets.	95%
Continuous Monitoring – Configurations	2.2	% of the applicable hardware assets (per question 1.1), of each kind of operating system software in 2.1, has an automated capability to identify deviations from the approved configuration baselines identified in 2.1.1 and provide visibility at the organization's enterprise level.	
Continuous Monitoring – Vulnerabilities	3.1	% of hardware assets identified in section 1.1 that are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization's enterprise level.	
Identity Management HSPD-12	4.2, 4.4	% of ALL people required to use Personal Identity Verification (PIV) Card to authenticate.	75%
Boundary Protection CNCI[2] #1	5.2	% of external network traffic passing through a Trusted Internet Connection (TIC[3]).	95%
Boundary Protection CNCI #1 & #2	5.1	% of required TIC capabilities implemented by TIC(s) used by the organization.	100%

Table 1 – Administration Priorities Metrics

[1] Continuous does not mean instantaneous. According to NIST SP 800-137, the term "continuous" means "that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information."

[2] Comprehensive National Cybersecurity Initiative (CNCI)

[3] Not applicable to Department of Defense (DOD).

1. 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)

1.2. What percentage of assets in 1.1 are covered by an automated capability (scans/device discovery processes) to provide enterprise-level visibility into asset inventory information for all hardware assets? (AP)

1.3. For what number of assets in 1.1 has the organization implemented an automated capability to detect and block unauthorized software from executing or for which no such software exists for the device type?[6] (KFM)

2. CONFIGURATION MANAGEMENT

2.1. For each operating system vendor, product, and version report the following:

2.1.1. Has a minimal acceptable security configuration baseline been defined? [7] (KFM)

2.1.2. How many hardware assets (which are covered by this baseline, if it exists) have this software? (KFM)

2.2. What is the percentage of the applicable hardware assets (per question 1.1) of each kind of operating system software in 3.1 that are covered by an automated capability to identify deviations from the approved configuration baselines identified in 2.1.1 and to provide visibility at the organization's enterprise level? (AP)

[4] "Unclassified" means low-impact (non-SBU) and SBU networks. Some organizations incorrectly use "unclassified" to mean not classified and not SBU.

[5] Unless specified otherwise in a footnote, add numbers across networks and organizational components to get the reportable result.

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

[7] "Defined" may include a narrative definition of the desired configuration. In the future, we will expect these standards to be defined directly as (a) data or (b) a test (preferably automated) of the configuration. Consider an organization approved deviation as *part* of the organization standard security configuration baseline.

3. VULNERABILITY AND WEAKNESS MANAGEMENT

3.1. What percentage of hardware assets identified in section 1.1 are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization's enterprise level? (AP)[8]

4. IDENTITY AND ACCESS MANAGEMENT

4.1. How many people have unprivileged network[9] accounts? (Exclude privileged network accounts and non-user accounts.) (Base)

4.2. What percentage of people with an *unprivileged* network account are required to log on with a two-factor PIV card? (AP)
This metric measures the percentage of people who are required to log on using a two-factor PIV card as the normal mode of authentication.

- Percentage should include people currently using temporary credentials if the person's normal mode of authentication is PIV-enforced.
- Percentage should measure people because a person may have multiple accounts.
- For a person with more than one unprivileged network account, 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 accounts.

4.3. How many people have privileged network accounts? (Exclude unprivileged network accounts and non-user accounts.) (Base)

4.4. What percentage of people with a *privileged* network account are required to log on with a two-factor PIV card? (AP)
This metric measures the percentage of people who are required to log on using a two-factor PIV card as the normal mode of authentication.

- Percentage should include people currently using temporary credentials if the person's normal mode of authentication is PIV-enforced.
- Percentage should measure people because a person may have multiple accounts.
- For a person with more than one privileged network account, 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 accounts.

[8] Once all organizations are reporting monthly to CyberScope, this question may become redundant.

[9] An unprivileged network account is an account without elevated privileges.

This section applies to remote access solutions that protect access to the organization's desktop LAN/WAN resources and services. Remote access excludes externally facing applications (e.g., OWA).

4.5. How many people log onto the organization's remote access solution(s) to obtain access to the organization's desktop LAN/WAN resources or services? (Base)

4.6. What percentage of people reported in 4.5 are required to log onto the organization's desktop LAN/WAN resources or services by using a two-factor PIV card? (KFM)
This metric measures the percentage of people who are required to log on using a two-factor PIV card as the normal mode of authentication.

- Percentage should include people currently using temporary credentials if the person's normal mode of authentication is PIV-enforced.
- Percentage should measure people because a person may have multiple accounts.
- People with more than one account should be counted in the percentage only if they are required to use a two-factor PIV card to authenticate to all accounts.

4.7. What is the percentage of an agency's operational PACS that comply with procurement requirements for purchasing products and services from the FIPS 201 Approval Products List maintained by GSA (per OMB M-06-18)? (Base)

4.8. What is the percentage of an agency's operational PACS that electronically accept and authenticate internal users' PIV credentials for routine access in accordance with NIST standards and guidelines (e.g. FIPS 201 and SP 800-116)? (Base)

4.9. What is the percentage of an agency's buildings and facilities for which a current Facility Risk Assessment has been performed in accordance with Interagency Security Committee (ISC) standards? (Base)

4.10. What is the percentage of an agency's operational Physical Access Control systems (PACS) that have been accredited under the NIST Risk Management Framework (i.e. NIST SP 800-37)? (Base)

4. 11. What is the percentage of an agency's operational PACS that electronically accept and authenticate external users' PIV credentials for routine access in accordance with NIST standards and guidelines (e.g. FIPS 201 and SP 800-116)? (Base)

5. BOUNDARY PROTECTION

Instruction: Question 5.1 applies to all 24 CFO Act agencies and TICAPs.

5.1. What percentage of the required TIC 2.0 Capabilities is implemented? (AP)

Instruction: Questions 5.2 applies only to Federal civilian organizations. If the reporting organization is not a Federal civilian organization, answer N/A to these questions.

5.2. What percentage of external network traffic to/from the organization's networks passes through a TIC/MTIPS? (AP)