

FY 2012

Federal Information Security Management Act
Reporting Metrics for Micro Agencies

Prepared by:

US Department of Homeland Security

National Cyber Security Division

Federal Network Security

March 6, 2012

GENERAL INSTRUCTIONS

Refer to the FY12 CIO Metrics for Definitions pertaining to each section.

1. System Inventory

1.1 For each of the FIPS 199 systems categorized impact levels (H = High, M = Moderate, L = Low) in this question, provide the total number of Organization information systems by Organization component (i.e. Bureau or Sub-Department Operating Element) in the table below. (Organizations with below 5000 users may report as one unit.)

FIPS 199 Category	1.1a Organization Operated Systems			1.1b Contractor Operated Systems			1.1c. Systems (from 1.1a and 1.1b) with Security ATO		
	H	M	L	H	M	L	H	M	L
Component 1									
Component 2									
[Add rows as needed for Organization components]									

1.2 For each of the FIPS 199 system categorized impact levels in this question, provide the total number of Organization operational, information systems using cloud services by Organization component (i.e. Bureau or Sub-Department Operating Element) in the table below.

FIPS 199 Category	1.2a Systems utilizing cloud computing resources		1.2b Systems utilizing cloud computing resources (1.2a) with a Security Assessment and Authorization		1.2c. Systems in 1.2a utilizing a FedRAMP authorized Cloud Service Provider (CSP)	
	M	L	M	L	M	L
Component 1						
Component 2						
[Add rows as needed for Organization components]						

Purpose and Use

These questions are being asked for the following reasons:

- System inventory is a basic tool to identify systems (and their boundaries).

- A key goal of this process is to ensure that systems are acquired/engineered, operated and maintained to provide adequate security.

2. Asset Management

2.0 Provide the total number of organization hardware assets connected to the organization’s unclassified¹ network(s).²

2.1 Provide the number of assets in 2.0, where an automated capability (device discovery process) provides visibility at the organization’s enterprise level into asset inventory information for all hardware assets.

2.2 Software Assets: Can the organization track the installed operating system³ Vendor, Product, Version, and patch-level combination(s) in use on the assets in 2.0.

2.4 Software Assets: Can the organization track the installed operating system Vendor, Product, Version, and patch-level combination(s) in use on the assets in 2.0.

2.4.a Can the organization track, (for each installed operating system Vendor, Product, Version, and patch-level combination in 2.4) the number of assets in 2 (2.1) on which it is installed in order to assess the number of operating system vulnerabilities which are present without scanning.⁴

Purpose and Use

These questions are being asked for the following reasons:

- The federal CMWG has determined that Asset Management is one of the first areas where continuous monitoring needs to be developed. Organizations must first know about devices (both authorized/managed and unauthorized/unmanaged) before they can manage the devices for configuration, vulnerabilities, and reachability.
- A key goal of hardware asset management is to identify and remove unmanaged assets⁵ before they are exploited and used to attack other assets. An underlying assumption is that if they are unmanaged, then they are probably vulnerable, and will be exploited if not removed or “authorized”⁶ quickly.

¹ “Unclassified” means low impact (non-SBU) and SBU networks. Some organizations incorrectly use “unclassified” to mean not classified AND not SBU.

² Unless specified otherwise in a footnote, add numbers across networks and organizational components to get the result to enter for the organization.

³ We assume one operating system per device. Report the number of devices that can boot with multiple operating systems in the comments. Note that virtual machines should be counted as “assets”.

⁴ If the number of assets reported is less than the total on the network, we should assume that the OS information for the others is not available. If this is not the case, please clarify in the comments.

⁵ Or to manage and authorize them.

⁶ In the context of asset management (as opposed to systems inventory) “authorize” has nothing to do with NIST SP 800-37, but rather a CCB or CCB-like authorization.

- A second goal is to provide the universe of assets to which other controls need to be applied. These other controls include SW asset management, boundary protection (network and physical), vulnerability management, and configuration management. These other areas of monitoring assess how well the hardware assets are managed.

3. Configuration Management

3.1 For each operating system Vendor, Product, Version, and patch-level⁷ combination referenced in 2.2, report the following:

3.1a Whether an adequately secure configuration baseline has been defined⁸.

3.1b The number of hardware assets with this software (which are covered by this baseline, if it exists).

3.1c For what percentage of the applicable hardware assets (per question 2.0), of each kind of operating system software in 3.1, has an automated capability to identify deviations from the approved configuration baselines identified in 3.1a and provide visibility at the organization's enterprise level?

Purpose and Use

These questions are being asked for the following reasons:

- The federal CMWG has determined that continuous monitoring (CM) of configurations is one of the first areas where CM capabilities need to be developed. This applies to both operating systems, and widely used applications.
- Even with a completely hardened system, exploitation may still occur due to zero day vulnerabilities. However, this forces attackers to elevate their sophistication for successful attacks.
- Rather, a robust continuous monitoring solution will be able to provide additional visibility for organizations to identify signs of compromise, though no single indicator may identify a definitive incident.
- A key goal of configuration management is to make assets **harder to exploit** through better configuration.
- A key assumption is that configuration management covers the universe of assets to which other controls need to be applied (controls that are defined under asset management).
- To have a capable configuration management program, the configuration management capability needs to be:

⁷ Knowing version and patch-level is critical to knowing the CVEs these operating systems have, knowing whether adequate configuration baselines have been defined, and knowing on what machines those baselines should be used.

⁸ "Defined", for now, may include a narrative definition of the desired configuration. But, in the next few years, we will expect these standards to be defined directly as a) data, b) a (preferably automated) test of the configuration. Consider an Organization approved deviation as **part** of the Organization standard security configuration baseline.

- Relatively complete, covering enough of the software base to significantly increase the effort required for a successful attack.
- Relatively timely, being able to find and fix configuration deviations faster than they can be exploited.
- Adequately accurate, having a low enough rate of false positives (to avoid unnecessary effort) and false negatives (to avoid unknown weaknesses).

4. Vulnerability Management

4. Provide the number of hardware assets identified in section 2.0 that are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization’s enterprise level.

Purpose and Use

These questions are being asked for the following reasons:

- The federal CMWG has determined that vulnerability management is one of the first areas where continuous monitoring needs to be developed.
- A key goal of vulnerability management is to make assets **harder to exploit** through mitigation of vulnerabilities identified in NIST’s National Vulnerability Database.
- A key assumption is that vulnerability management covers the universe of applicable assets to which other controls need to be applied (defined under asset management). The [SCAP](#) standard can support this process.
- Add weakness items.
- To have a capable vulnerability management program, the vulnerability management capability needs to be:
 - Relatively complete, covering enough of the software base to significantly increase the effort required for a successful attack.
 - Relatively timely, being able to find and fix vulnerabilities faster than they can be exploited.
 - Adequately accurate, having a low enough rate of false positives (to avoid unnecessary effort) and false negatives (to avoid unknown weaknesses).

5. Identity and Access Management

5.1 Provide the number of Organization unprivileged network user accounts⁹? (Exclude privileged network user accounts and non-user accounts)

5.2 How many unprivileged network user accounts are configured to:

⁹ The term “network user accounts” intentionally excludes application accounts. For this section, the only relevant networks are SBU (or higher impact) networks.

	a. Require the form of identification listed on the left?	b. Allow, but not require, the form of identification listed on the left?
5.2a User-ID and Password		
5.2b Two factor-PIV Card		
5.2c Other two factor authentication		

5.3 Provide the number of Organization privileged network user accounts (Exclude non-user accounts and unprivileged network user accounts)?

5.4 How many privileged network user accounts are configured to:

	a. Require the form of identification listed on the left?	b. Allow, but not require, the form of identification listed on the left?
5.4a User-ID and Password		
5.4b Two factor-PIV Card		
5.4c Other two factor authentication		

Purpose and Use

These questions are being asked for the following reasons:

- OMB and DHS have determined that Federal Identity Management ([HSPD-12](#)) is among the areas where additional controls need to be developed. See also [OMB M-04-04](#) for web based systems.
- Strong information system authentication requires multiple factors to securely authenticate a user. Secure authentication requires something you have, something you are, and something you know. A single-factor authentication mechanism, such as a username and password, is insufficient to block even basic attackers.
- The USG will first move to a two factor authentication using PIV cards, though a stronger authentication solution would include all three factors.
- Enhanced identity management solutions also support the adoption of additional non-security benefits, such as Single Sign On, more useable systems, and enhanced identity capabilities for legal and non-repudiation needs.

- A key goal of identity and access management is to make sure that access rights are only given to the intended individuals and/or processes.¹⁰
- To have a capable identity management program, this capability needs to be:
 - Relatively complete, covering all accounts.
 - Relatively timely, being able to find and remove stale or compromised accounts faster than they can be exploited.
 - Adequately accurate, having a low enough rate of false positives (to avoid unnecessary effort and reduce denial of service) and false negatives (to avoid unknown weaknesses).

6. Data Protection

6. Provide the estimated number of hardware assets from Question 2.0 which have the following characteristics. Enter responses in the table.

Mobile Assets Types (each asset should be recorded <i>no more than once</i> in each column)	a. Estimated number of mobile hardware assets of the types indicated in each row	b. Estimated number assets from column a <i>with adequate encryption of data on the device.</i> ¹¹
• Laptop Computers, Netbooks, and Tablet-Type Computers		
• Personal Digital Assistant		
• BlackBerries and Other Smartphones		
• USB connected devices (e.g., Flashdrives and Removable Hard Drives)		
• Other mobile hardware assets (describe types in comments field)		

Purpose and Use

These questions are being asked for the following reasons:

- Mobile devices and unencrypted e-mail are a primary source of loss for sensitive data because they move outside the protection of physical and electronic barriers that protect other hardware assets. These devices are also vectors to carry malware back into the intranet environment. The use of encryption of data at rest or in motion is vital to protect that data's confidentiality, integrity and/or availability.
- For PKI systems to adequately protect data, their certificate authority needs to adequately meet certain security controls. This is increasingly important for remote access, identity management, and data protection.

¹⁰ This is done, of course, by establishing a process to assign attributes to a digital identity, and by connecting an individual to that identity; but this would be pointless, without subsequently using it to control access.

¹¹ The numbers in column 'b' cannot be larger than the numbers in column 'a'.

- The purpose of this section is to assess the security of federal data in these environments.

7. Boundary Protection

7. Provide the percentage of external connections passing through a TIC/MTIPS.

Instruction: The question applies to all Federal Civilian Agencies. All others should respond N/A.

Purpose and Use

These questions are being asked for the following reasons:

- Trusted Internet Connection (TIC) is an Administration Priority, and the federal Continuous Monitoring Working Group (CMWG) has determined that it is among the areas where continuous monitoring needs to be developed.
- Email protections are directed to reduce the number of phishing attacks, which currently represent a high risk threat.
- A key goal of boundary protection is to make assets harder to exploit by outsiders, by keeping them outside the network perimeter.
- A key assumption is that boundary protections occur centrally, and covers the universe of applicable hardware assets (defined under asset management). A key risk is that someone inside the perimeter creates an unapproved hole in the perimeter defenses.
- To have a capable boundary protection program, this capability needs to be:
 - Relatively complete, covering all avenues of access to/from the network.
 - Relatively timely, being able to find and fix attacks and intrusions faster than they can be completed.
 - Adequately accurate, having a low enough rate of false positives (to avoid unnecessary effort) and false negatives (to avoid unknown weaknesses).

8. Training and Education

8. Provide the number of the Organization's network users that have been given and successfully completed cybersecurity awareness training in FY2012 (at least annually).

Purpose and Use

These questions are being asked for the following reasons:

- Given real world realities, it is reasonable to expect that some attacks will succeed. Organizations need to be able to detect those attacks. Ideally, Organizations would defend against those attacks in real time, but at a minimum, we expect Organizations to determine the kinds of attacks that are most successful.
- This allows the Organization to use this information about successful attacks and their impact to make informed risk-based decisions about where it is most cost-effective and essential to focus security resources.
- Penetration testing allows Organizations to test their network defenses and estimate the extent to which they are able to detect and respond to actual threats. This also provides useful information to the risk management process to determine the level of cyber resources to invest in incident detection and response.

9. Remote Access / Telework

9.1. Provide the estimated total number of annual remote connections the Organization provides to allow users to connect to near-full access to the Organization’s normal desktop LAN/WAN resources/services.

9.1a. For those connections counted above in 9.1, provide the estimated number of those connections that:¹²

	<ul style="list-style-type: none"> • REQUIRE the kind (and only the kind) of authentication indicated in 10.1a columns a-d. (List all other connections by connection method in 10.1a column e) • For each Type of connection listed below 	a) ONLY User-ID and Password (KFM)	b) ONLY Two factor-PIV Card (AP)	c) ONLY Other two factor authentication	d) ONLY one other method. (Please describe in the	e) Connections that may have been authenticated
Type of Connection	1. Dial-up					
	2. Virtual Private Network (not clientless)					
	3. Virtual Private Network (clientless) including SSL, TLS, etc.					
	4. Citrix					
	5. Other (Add Rows as needed)					

Purpose and Use

These questions are being asked for the following reasons:

¹² For 9.1a, each connection will appear in one and only one cell of the table. The sum of connections listed in each cell should match the total from 9.1. If this is not the case, explain the reason in the comments.

- Adequate control of remote connections is a critical part of boundary protection.
- Attackers exploit boundary systems on Internet-accessible DMZ networks (and on internal network boundaries), and then pivot to gain deeper access on internal networks. Responses to the above questions will help agencies deter, detect, and defend against unauthorized network connections/access to internal and external networks.
- Remote connections allow users to access the network without gaining physical access to Organization space and the computers hosted there. Moreover, the connections over the Internet provide opportunities for compromise of information in transit. Because these connections are beyond physical security controls, they need compensating controls to ensure that only properly identified and authenticated users gain access, and that the connections prevent hijacking by others.