FY 2012

Chief Information Officer

Federal Information Security Management Act

Reporting Metrics

Prepared by:

US Department of Homeland Security

National Cyber Security Division

Federal Network Security

February 14, 2012

Table of Contents

GENERAL INSTRUCTIONS 4

1. SYSTEM INVENTORY........ 11

2. ASSET MANAGEMENT........ 15

3. CONFIGURATION MANAGEMENT........ 25

4. VULNERABILITY AND WEAKNESS MANAGEMENT 30

5. IDENTITY AND ACCESS MANAGEMENT 34

6. DATA PROTECTION 42

7. BOUNDARY PROTECTION........ 46

8. INCIDENT MANAGEMENT 52

9. TRAINING AND EDUCATION........ 56

10. REMOTE ACCESS 62

11. NETWORK SECURITY PROTOCOLS........ 67

Table of Figures

Figure 1 – Sources of Guidance for the USG-wide FISMA Program........ 4

List of Tables

Table 1 – Administration Priorities Performance Metrics 6
Table 2 – Expected Areas of Future Expansion for System Inventory 12
Table 3 – Expected Areas of Future Expansion for Asset Management........ 17
Table 4 – Expected Areas of Future Expansion for Configuration Management 27
Table 5 – Expected Areas of Future Expansion for Vulnerability and Weakness Management........ 32
Table 6 – Expected Areas of Future Expansion for Identity and Access Management 38
Table 7 – Expected Areas of Future Expansion for Data Protection........ 43
Table 8 – Expected Areas of Future Expansion for Boundary Protection........ 48
Table 9 – Expected Areas of Future Expansion for Incident Management 53
Table 10 – Expected Areas of Future Expansion for Training and Education 59
Table 11 – Expected Areas of Future Expansion for Remote Access........ 64
Table 12 – Expected Areas of Future Expansion for Network Security Protocols 69

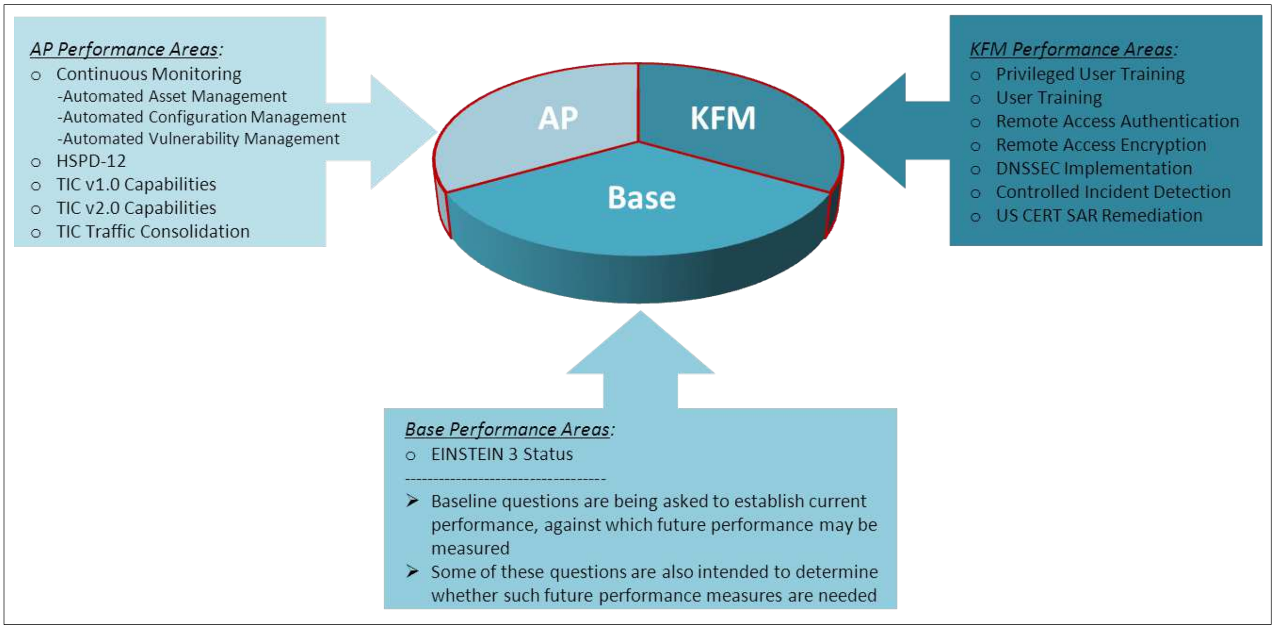
GENERAL INSTRUCTIONS

Instructions provided below pertain to the entire document. Specific directions, pertaining to a subsequent section, are provided within that section.

Sources of Questions and Guidance for the United States Government-wide (USG-wide) Federal Information Security Management Act (FISMA) Program

The questions in this document come from 3 primary sources, and will be marked as such in the document:

- Administration Priorities[1] (AP)
- Key FISMA Metrics[2] (KFM)
- Baseline Questions[3] (Base)



AP Performance Areas:

- ○ Continuous Monitoring
  - -Automated Asset Management
  - -Automated Configuration Management
  - -Automated Vulnerability Management
- ○ HSPD-12
- ○ TIC v1.0 Capabilities
- ○ TIC v2.0 Capabilities
- ○ TIC Traffic Consolidation

KFM Performance Areas:

- ○ Privileged User Training
- ○ User Training
- ○ Remote Access Authentication
- ○ Remote Access Encryption
- ○ DNSSEC Implementation
- ○ Controlled Incident Detection
- ○ US CERT SAR Remediation

Base Performance Areas:

- ○ EINSTEIN 3 Status

- ➢ Baseline questions are being asked to establish current performance, against which future performance may be measured
- ➢ Some of these questions are also intended to determine whether such future performance measures are needed

Figure 1 – Sources of Guidance for the USG-wide FISMA Program

The Federal cybersecurity defensive posture is a constantly moving target. It is constantly shifting because of the relentless dynamic threat environment, emerging technologies, and new vulnerabilities. Many threats can be mitigated by following established cybersecurity best practices, but advanced attackers often search for poor cybersecurity practices and target associated vulnerabilities.

[1] Administration Priorities (AP) will be scored. The sub-categories listed under continuous monitoring are not all areas where continuous monitoring is needed, but they are the AP areas for FY2012.

[2] Key FISMA Metrics (KFM) will be scored.

[3] Baseline Questions (Base) will not be scored.

The FY12 FISMA Metrics, discussed in the following sections, establish baseline security practices as an entry level requirement for all Federal agencies. However, mitigating advanced attackers requires personnel with advanced cybersecurity knowledge and awareness of the agency's enterprise security posture. Because cybersecurity is a very important factor for agencies to be able to provide unimpeded essential services to citizens, in FY11 the Administration identified 3 FISMA priorities. They are defined as: Continuous Monitoring, Trusted Internet Connection (TIC) capabilities and traffic consolidation, and Homeland Security Presidential Directive (HSPD)-12, implementation for logical access control. In FY12, these priorities continue to provide emphasis on FISMA metrics that are identified as having the greatest probability of success in mitigating cybersecurity risks to agency information systems.

Reporting Organizations

The term "Organization" is used consistently herein to refer to a federal agency (or department) which is a reporting unit under CyberScope. Often, those reporting units must collect and aggregate their response from a number of sub-organizations (called "component organizations[4]", herein). The term "network", used herein, refers to a network employed by the organization or one of its component organizations to provide services and/or conduct other business.

Expected Levels of Performance[5]

Administration Priorities: The expected levels of performance for these administrative priority FISMA metrics are based on review and input from multiple cybersecurity experts, considering public, private and intelligence sourced threat information, to select the highest impact controls for USG-wide application. These metrics are still under review, and are described in the table below.

Administration Performance Area	Section	Performance Metric	Minimal Level for 2012	Target Level for 2012
Continuous [6]Monitoring - Assets	2.1a	Provide the number of Organization information technology assets connected to the network(s), (e.g. router, server, workstation, laptop, etc.) where an automated capability provides visibility at the Organization level into asset inventory information.	80%	95%

[4] This is the same as organizational component, like "DoD Components"

[5] The milestones established in this document are not intended to supersede deadlines set by Presidential Directives, OMB policy or NIST standards. As necessary, DHS is working with agencies to establish milestones as part of agency corrective action plans.

[6] Continuous does not mean instantaneous. NIST SP 800-137 say that he 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.

Administration Performance Area	Section	Performance Metric	Minimal Level for 2012	Target Level for 2012
Continuous Monitoring - Configurations	3.1	Provide the number of Organization information technology assets connected to the network(s) where an automated capability provides visibility at the Organization level into system configuration information (e.g. comparison of Organization baselines to installed configurations).		
Continuous Monitoring - Vulnerabilities	4.1	Provide the number of Organization information technology assets connected to the network(s) where an automated capability provides visibility at the Organization level into detailed vulnerability information (Common Vulnerabilities and Exposures (CVE)).		
Identity Management HSPD-12	5.2-5.4 10.1	% of ALL users required to use Personal Identity Verification (PIV) Card to authenticate.	50%	75%
Boundary Protection CNCI #1	7.3	% of total external network traffic passing through a Trusted Internet Connection (TIC[7]).	80%	95%
Boundary Protection CNCI #1 & #2	7.1-7.2	% of required TIC capabilities implemented by TIC(s) used by the Organization.	95%	100%

Table 1 – Administration Priorities Performance Metrics

Key FISMA Metrics: The expected level of performance for these metrics is adequate security.

"Adequate security" means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls. (OMB Circular A-130, Appendix III, definitions.)

Per OMB FISMA guidance (M-11-33, FAQ 15), the agency head is responsible to determine the acceptable level of risk, with input from system owners, program officials, and CIOs.

[7] Not applicable to Department of Defense (DoD).

Baseline Questions: There is no expected level of performance for baseline questions. These are being asked to establish current performance against which future performance may be measured. Some baseline questions are also intended to determine whether such future performance measures are needed. These will be in the CIO questionnaire. They may be reported to Congress at the discretion of DHS. OIGs should not assume that these questions define any specific organizational performance standard for 2012.

Structure and Organization

Each set of questions is organized around a topic, ideally related to security outcome metrics that have been and/or are being developed. This has not changed from prior years.

Each of these areas is now newly supported by an appendix with includes the following sections:

- ***Purpose and Use –*** Explains the importance of the topic area to security for each organization and why it is important enough to be covered in a report which will reach federal-level security managers and Congress.
- ***Expected Areas of Future Expansion –*** Explains what kinds of additional metrics and/or performance goals may be added in the next two years (FY2013-2014) to provide agencies time to plan to meet the kinds of metrics expected.
- ***Definition of Terms –*** This section covers terms where a) comments from agencies suggested that definitions were needed, b) instructions provided by organizations to their component organizations differed across organizations. These definitions are intended to reduce the effort organizations must make interpreting and explaining the questions and to produce a more consistent and valid response to the questions.

Scope of Definitions

Hyperlinks within the text point to operational definitions to clarify how the questions in this report are to be answered. These definitions are not intended to conflict with definitions in law, OMB policy and NIST standards and guidelines, but to add clarity to the terms are used in this document.

Data Aggregation[8] over Component Organizations and Networks

Many Organizations reporting under these instructions will need to aggregate quantitative responses across component organizations and networks. This needs to be done in a consistent and valid manner. Some methods are not applicable to small organizations with no component organizations and only one applicable network.

The aggregated number is to be at a level such that actual performance is better than the aggregate number cited 90% of the time. Thus, if the organization has three components, as follows, with the following size and results the following two examples show how to aggregate the numbers.

Example 1: An Adequate/Inadequate (Yes/No) Metric

In this example, the organization has three components. Component 1 is large with 100,000 computers (or other assets). Components 2 and 3 are much smaller with only 10,000 and 1,000 assets respectively. In this example, neither component 2 nor 3 come close to meeting the standard, and the organization needs to decide how to address this risk. However, the largest network is 95% adequate. Thus, overall, the organization has 99,900 compliant objects out of a total of 111,000, which (barely) meets the 90% “adequate” standard. The organization would report 90% adequate.

	Size	Adequate	Inadequate
Component 1	100,000	95,000	5,000
Component 2	10,000	4,900	5,100
Component 3	1,000	0	1,000
	111,000	99,900	11,100
Standard	99,900		

Example 2: A Quantitative Metric

This example uses the same components from the last example, but the question asks for a particular metric (for example, how fast the organization gets critical patches installed).

In this case computing the 90% compliance factor may require “interpolation”[9]. Consider the data in the table below. Data will probably be collected in “buckets” in this case the number of patches installed in less than 20 days, 30 days, etc.

[8] Aggregation of data may disclose a pattern of weaknesses and/or vulnerabilities that could assist attackers. Appropriate discretion, classification, and/or marking as “sensitive but unclassified” should be used to prevent inappropriate disclosure.

[9] For the definition of “interpolation”, see Wikipedia or a basic algebra textbook. If the organization has detailed data on each metric for each instance (in his example each critical patch on each machine, interpolation would not be necessary.

Less that 90% of the assets (80,900) were patched in <20 days. More than 90% of the assets (103,500) were patched in < 30 days, so the actual number is clearly in between 20 and 30 days. In this case the agency can interpolate assuming a linear distribution between the data points.

In this example, (the standard) 99,900 is 84%[10] of the way between the overall number done in < 20 days (80,900) and the overall number done in < 30 days (103,500). So, the organization may report the time as the number that is 84% of the way between 20 and 30 days, which is approximately 28[11] days.

	Size	< 20 days	<30 days[12]	<40 days
Component 1	100,000	75,000	95,000	98,000
Component 2	10,000	5,000	7,500	8,000
Component 3	1,000	900	1,000	1,000
	111,000	80,900	103,500	107,000
Standard	99,900			

Units of Measure: In many cases we ask for **asset[13] counts,** and therefore, in each section we have defined the "assets" to be counted.[14] However, the questions also ask for measure in terms of **frequency and duration (measured in time).** In these cases time should be treated as a continuous numeric scale. While we ask for the response in days, you may report weeks as 7 days, months as 30 days, quarters as 90 days, years as 365 days, 8 hours as 0.34 days, or any other number of days which is accurate. We will not consider more than 2 decimal places in the response.

Adequate (Adequately): We have used these terms throughout to describe aspects of security; e.g., adequately timely and adequate completeness. Adequate and adequately should be interpreted as adequate security, with regard to the specific attribute to be measured.

NIST SP 800 Revisions: For legacy information systems, agencies are expected to be in compliance with NIST guidelines within one year of the publication date. The one year compliance date for revisions to NIST publications applies only to the new and/or updated material in the publications. For information systems under development or for legacy systems undergoing significant changes, agencies are expected to be in compliance with the NIST publications immediately upon deployment of the information system.

[10] (99,900-80,900)/(103,500-80,900)

[11] = (84% * (30-20))+20

[12] Those patched in <30 days, include those patched in less than 20 days, etc.

[13] An asset may be a) an information system, b) a hardware asset which is connected to the network, c) an operating system, d) an application, etc. As illustrated in the links above, we have defined these assets so that they are countable in each applicable section.

[14] These measures will be a snapshot. An assumption is that the organization should try to build a capability to refresh this snapshot with enough coverage, accuracy and timeliness to make it useful to address the actual rate of attacks. In general we prefer results from a recent snapshot.

FIPS Versions: When references are made to FIPS Standards, we mean the latest (non-draft) published version.

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.)

	1.1a Organization Operated Systems (Base)			1.1b Contractor Operated Systems (Base)			1.1c. Systems (from 1.1a and 1.1b) with Security ATO (KFM)		
FIPS 199 Category	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.

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

Purpose, Future Metrics, and Definitions

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.

Expected Areas of Future Expansion for System Inventory[15]

Area of Expansion	Target for Future Inclusion
• It is expected that Federal agencies are mature in this area and they maintain adequate maturity while moving from periodic to more continuous assessment and authorization.	As soon as FY2013
• Federal agencies are progressing toward more continuous assessment and authorization and are better able to respond to emerging threats and reappearing weaknesses[16].	As soon as FY2014

Table 2 – Expected Areas of Future Expansion for System Inventory

Each of these sections would require agencies to know a) total actual system inventory list, b) authorized system inventory list, c) unauthorized system inventory list (the difference between a and b), and d) a plan to rapidly authorize or remove unauthorized systems.

[15]

[16] Such reappearing weaknesses might include changed configurations, re-installed unapproved software, passwords not reset, training repeatedly missed, etc.

Definitions for FY2012:

Cloud computing resources: Cloud (public or private) is used herein as defined in NIST SP 800-145. The essential parts of this definition follow:

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics.
>
> **Essential[17] Characteristics:**
>
> - **On-demand self-service.** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
> - **Broad network access.** Capabilities are available over the network[18] and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
> - **Resource pooling.** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant[19] model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
> - **Rapid elasticity.** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
> - **Measured service.** Cloud systems automatically control and optimize resource use by leveraging a metering capability[20] at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Cloud Service Provider: An organization (public or private) that provides cloud computing resources over a network (not necessarily the Internet).

[17] All of these must be present to make the service a cloud service.

[18] [The network does not necessarily mean the internet.]

[19] [The reference to multi-tenant model does not necessarily imply a public cloud. The multiple tenants could all be parts of a large Organization, for example in a government dedicated cloud.]

[20] "Typically this is done on a pay-per-use or charge-per-use basis."

Federal Risk and Authorization Management Program (FedRAMP): is defined here.

2. ASSET MANAGEMENT

2.0 Hardware Assets

Provide the total number of organization hardware assets connected to the organization's unclassified[21] network(s).[22] (KFM)

2.1 Provide the number of assets in 2, where an automated capability (device discovery process) provides visibility at the organization's enterprise level into asset inventory information for all hardware assets. (AP)

2.1a How often are these automated capabilities (device discovery processes) conducted on all assets connected to the organization's full network(s)? (frequency in days)[23] (KFM)

2.1a-1 How much time does it take a device discovery tool to complete this process? (Duration in days; e.g. 10 days or 0.2 days)[24] (Base)

2.1b Provide the number of assets in 2.0, where all of the following information is collected: Network IP address, Machine Name, MAC Address (or other hardware identifier like serial number). (KFM)

2.2 Provide the number of assets in 2.0, where the organization has an automated capability to determine whether the asset is authorized and to determine who manages it[25]. (KFM)

2.3 Provide the number of assets in 2.0, where the organization has an automated capability to compare 2.1 and 2.2, to identify and remove (manually or through NAC, etc.) the unauthorized devices. (Base)

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

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

[23] Report the lowest frequency of complete discovery on any applicable network of the organization. In the comments you may include an average time weighted by assets per discovery frequency, if desired.

[24] Report the shortest period in which all applicable networks typically complete the discovery process. This is typically the longest discovery duration of all the component networks, assuming all processes can run in parallel. In the comments you may include an average frequency weighted by assets per discovery duration, if desired.

[25] "Who manages it" means the organization can define this at a low enough level of detail to be able to effectively assign responsibility and measure performance to obtain adequate security. This clearly does not require knowing the individual who is responsible. In fact, this would be bad practice, because an individual cannot provide 24 x 7coverage. Likewise, it should not correspond to an organization so large (e.g., the Department of Sate) that the work is essentially unassigned. Rather, the granularity needed is closer to that of an "organizational unit" on a windows network which is used to define who has administrative rights to a manageable collection of assets and user accounts. Organizations have considerable flexibility in defining a standard for what constitutes adequately knowing "who manages it" within these extremes.

2.3a For the assets in 2.3, how much time does it actually take to a) assign for management (authorize) or b) remove unauthorized devices once discovered with 95% confidence[26]**?** (Duration in days; e.g. 10.00 days or 0.20 days)[27] (Base)

2.3b Provide the number of assets in 2.0, where the Organization has implemented an automated capability to detect and mitigate unauthorized routes, including routes across air-gapped networks. (Base)

Note: For questions 2.4 – 2.5, if the answer is no, explain why not in the comments.

2.4 Software Assets: Can the organization track the installed operating system[28] Vendor, Product, Version, and patch-level combination(s) in use on the assets in 2. (Base)

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.[29] (Base)

2.5 Does the Organization have a current list of the enterprise-wide COTS general purpose applications (e.g., Internet Explorer, Adobe, Java, MS Office, Oracle, SQL, etc.[30]) installed on the assets in 2.0. (Base)

2.5a For each enterprise-wide COTS general purpose applications in 2.5, can the Organization report the number of assets in 2 on which it is installed by CPE[31] in order to know the number of application vulnerabilities which are present without scanning. (Base)

2.6 Provide the number of assets in 2.0, where the Organization has implemented an automated capability to detect and block unauthorized software from executing[32], or where no such software exists for the device type. (KFM)

[26] With 95% confidence means that 95% of the time it takes less than this amount of time to deal with the anomaly (once discovered). Because some organizations are worried about the cost of measuring this, we note that a reliable estimate of this number based on an adequate sampling method is sufficient. This metric is here because the timeliness of response is important to remove these unmanaged (and therefore probably vulnerable) assets from the network (or to get them managed).

[27] Report the shortest period in which all applicable networks typically complete the removal process. This is typically the longest removal duration of all the component networks, assuming all processes can run in parallel. In the comments you may include an average removal duration weighted by assets per each network's removal duration (with the confidence defined), if desired. If you cannot measure this number, use the comments to explain why, and whether you think this is (or is not) a valuable metric.

[28] 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".

[29] If the number of assets reported is less that 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.

[30] Or other high-risk applications.

[31] NIST's Common Product Enumeration.

Purpose, Future Metrics, and Definitions

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 assets[33] 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"[34] quickly.
- 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.

Expected Areas of Future Expansion for Asset Management

Area of Expansion	Target for Future Inclusion
• Elevate question 2.6 to an Administration Priority as we get better hardware and software inventory as a base. This approach has significant potential to reduce the impact of APTs and zero-day threats. • Provide additional capability and definition around 2.3 for device management and unauthorized (unmanaged) device handling, including non-networked devices such as USB drives. • Expand 2.1 asset discovery to more effectively include virtualized and cloud computing assets and capabilities	As soon as FY2013
• Increased fidelity around nontraditional assets such as virtualized and Bring Your Own Devices (BYOD)	As soon as FY2014

Table 3 – Expected Areas of Future Expansion for Asset Management

[32] This may include software whitelisting tools which identify executables 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.

[33] Or to manage and authorize them.

[34] 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.

Each of these sections would require agencies to know a) total actual inventory list, b) authorized inventory list, c) unauthorized inventory list (the difference between a and b), and d) to rapidly remove unauthorized assets.

Definitions for FY2012:

Authorized Asset:

An asset is authorized when it is:

- Assigned to a particular person or group to manage and/or
- Allowed on the network by a Network Access Control system because it is adequately configured and adequately free of vulnerabilities.

The rationale for this definition is that unauthorized devices are not "managed" to ensure compliance. Therefore they are likely vulnerable, and should be removed from the network or managed. (How well authorized devices are "managed" is reported in other metrics.) Authorizing (assigning a device for management) is a first step in implementing security.

Automated Capability to Detect and Block Unauthorized Hardware from Connecting:

This should be interpreted to include:

- Network access control systems or other comparable technical solutions.
- Similar controls for wireless systems.
- WAR driving to look for unauthorized wireless access points.

This should NOT be interpreted to mean:

- Walking around and physically looking for unauthorized devices and manually removing them, although this may sometimes be useful.

Automated Capability to Detect and Block Unauthorized Software from Executing:

This should be interpreted to include:

- Anti-Virus Software (that blocks software based on signatures)
- Other black-listing software that is of comparable breadth
- White-listing software, that only allows executables with specific digital fingerprints (or comparable verification method) to execute.

In other words, the software may be considered unauthorized:

- Because it is on a blacklist, or
- Because it is not on a whitelist.

This question refers to capability at the device level, not at the network level. If agencies wish to describe capabilities to filter and block malicious code at the network boundary level, they may do so in the applicable comments section, but this is not required.

Automated Capability to Detect Hardware Assets:

Also known as 'automated device discovery process'. Any report of actual assets that can be generated by a computer. This includes:

- Active Scanners (might include a dedicated discovery scan or a vulnerability scan of an IP Range)
- Passive Listeners

- Agent generated data
- Switches and routers reporting connected devices
- Running a script in order to retrieve data
- Any other reliable and valid method
- Some combination of the above

The comments should specify whether the automated device discovery process is limited to:

- A supposed address (e.g., IP) range in which all devices must operate, or
- Finds all addressable devices, independent of address range.

If the discovery process is limited to an IP range, the comment should note whether networking devices on the network (routers, switches, firewalls) will route traffic to/from device outside the designated range (foreign devices) at the LAN, MAN, WAN, etc. levels. Preferably traffic would not be routed to/from such foreign devices.

Connected to the Organization's unclassified Network(s):[35]

This includes mechanical (wired), non-mechanical (wireless), and any other form of connection that allows the electronic flow of information.[36]

You shall exclude the following "networks" and/or stand-alone devices:

- Numbers of standalone devices (not addressable)[37]
- Test and/or development networks if not connected to the Internet, which contain no "sensitive" information (no info above impact level 1)
- Networks hosting "public" non-sensitive websites (no info above impact level 1)
- Classified networks

Connected to the network does not include organization's entire property book. In addition to the items listed above, you shall exclude assets which are:

- In storage,
- De-commissioned, or
- Otherwise not operational

Do not exclude devices that are temporality turned off, for example overnight, or because someone is on leave.[38]

[35] There is no limit on how short (low frequency or low duration) the connection is. Even short and/or infrequent connections should be counted. Regardless of how much these connected devices are intended to process, store, and transmit information, once connected they can be abused to do unintended misuse of the network.

[36] This includes networks which are air-gapped from the internet, but contain sensitive information.

[37] This should not be interpreted to exclude devices that are intermittently connected, which should be included.

[38] These are still important because they may be turned on again tomorrow.

Devices connecting remotely which are allowed to access other devices beyond the DMZ are considered "connected"; e.g., a connection through a Citrix client does not cause the remote device to be included, but a connection through a simple VPN does if the connection goes beyond the DMZ.

The network being considered may be GOGO[39], GOCO[40], COCO[41] on behalf of the government. The form of ownership and operation is not relevant to inclusion.

Enterprise-wide COTS General Purpose Applications:

- Any application that exists on more than 80% of the type of asset to which it applies. For example, MS-Office would only be expected to be on workstations and portable equivalents to a workstation, but not on routers, printers, or servers. Thus, if MS-Office is on 80% of workstations (and equivalents), then it fits this definition.
- Add additional applications (most widespread first) such that the sum of installed application-asset combinations reported, covers >=66% of the total application-asset combinations present over all assets in the asset base reported in 2.0.

These definitions are provided to focus organizations on the most commonly installed software on the network, for now. An Organization that cannot compute these percentages will need to try to report all software, or at least a large enough proportion of the software to be reasonably sure of meeting this standard.

Full Network(s):

The full network refers to the collection of all assets on the unclassified network(s) of the reporting organization, for network(s) that meet the criteria defined in "connected to the network".

Where that organization is large and has many networks, the organization may summarize the response as defined in the footnotes to each question.

General Purpose Applications(s), enterprise-wide:

Applications (COTS, GOTS, custom, etc.) that are typically widely installed on applicable machines (on >= 80% of applicable machines[42]), and which collectively account for >= 90% of installed hardware-asset/software-asset combinations for the organization, component organization, and/or network.

[39] GOGO means Government Owned Government Operated

[40] GOCO means Government Owned Contractor Operated

[41] COCO means Contractor Owned Contractor Operated

[42] Applicable machines means machines on which the software is capable of running and intended to run by the software vendor. Thus office automation software would be able to run on workstations and servers, but is only intended to run on workstations, and is unable to run on routers. Thus it would be applicable to workstations, but not to servers and routers.

Hardware Assets:

Agencies have tended to divide these assets into the following categories for internal reporting. (Note: Those that don't meet the criteria defined below should be excluded) The detailed lists under each broad category are illustrative and not exhaustive. Note the last category which is "other addressable devices on the network" is to indicate the criterion for including other kinds of specialized devices not explicitly called out.

- Non-Portable Computers[43]
  - Servers
  - Workstations (Desktops)
- Portable Computers
  - Laptops
  - Net-books
  - Tablets (iPad)
- Mobile Devices - Personal Digital Assistants (PDAs)
  - Smartphones (iPhone, Android)
  - Blackberry
  - Personal Digital Assistants
- Networking Devices[44]
  - Routers
  - Switches
  - Gateways, Bridges, Wireless Access Points (WAPs)
  - Firewalls
  - Intrusion Detection/Prevention Systems
  - Network Address Translators (NAT devices)
  - Hybrids of these types (like a NAT router)
- Other Communication Devices
  - Encryptors
  - Decryptors
  - VPN endpoints[45]
  - Medical Devices
  - Alarms and Physical Access Control Devices
  - PKI Infrastructure[46]

[43] Multi-purpose devices need only be counted once per device. Devices with multiple IP connections need only be counted once per device, not once per connection. This is an inventory of hardware assets, not data.

[44] This list is not meant to be exhaustive, as there are many types of networking devices. If they are "connected" they are to be included.

[45] VPN endpoints generally mean the encryptors/decryptors at each end of the VPN tunnel.

- Other Input/Output devices if they appear with their own address
  - Network Printers/Plotters/Copiers/Multi-function Devices (MFDs).
  - Network Fax Portals
  - Network Scanners
  - Network Accessible Storage Devices
  - VOIP Phones
  - Others Network I/O devices
- Virtual machines that can be addressed[47] as if they are a separate physical machine should be counted as separate assets.[48]
- Other Devices addressable on the network.
- USB Devices connected to any device addressable on the network.

Both Government Furnished Equipment (GFE) and non-GFE assets are included if they meet the other criteria for inclusion listed here[49]. Mobile devices that receive federal e-mail are to be considered to be connected. Note: If non-GFE is allowed to connect, it is especially important that it be inventoried, authorized, and correctly configured prior to connection[50].

Only devices connected to the network(s) of your organization should be reported, and only if they are addressable[51] for network traffic (except USB connected devices are included). The reason we limit this to addressable devices, is that from a network point of view, only addressable devices are attackable. For example, a monitor (not addressable, thus not included) can only be attacked through the addressable computer it is connected to. USB devices are added because they are a source of attacks.

[46] PKI assets should be included in the network(s) on which it resides. Special methods may be needed to adequately check it for vulnerabilities, compliance, etc. as described in subsequent sections, or if these are not done, it should be included among the assets not covered.

[47] "Addressable" means by IP address or any other method to communicate to the network.

[48] Note that VM "devices" generally reside on some hardware server(s). Assuming that both the hardware server and the VM server are addressable on the network, both kinds of devices are counted in inventory, because each needs to be managed and each is open to attack. (Things like multiple CPUs, on the other-hand, do not create separate assets, generally, because the CPUs are not addressable, and are only subject to attack as part of the larger asset). If you have issues about how to apply this for specific cloud providersplease ask for further guidance.

[49] If this NON-GFE connects in a limited way such that it can only send and receive presentation layer data from a virtual machine on the network, and this data has appropriate encryption (such as a Citrix connection), the NON-GFE does not have to be counted.

[50] If this NON-GFE connects in a limited way such that it can only send and receive presentation layer data from a virtual machine on the network, and this data has appropriate encryption (such as a Citrix connection), the NON-GFE does not have to be counted.

[51] Addressable means that communications can be routed to this asset, typically because it has an assigned IP address. Devices connecting via mechanisms like Citrix where only limited traffic can be allowed to pass do not need to be counted if justified by an adequate risk assessment, approved by the AO and/or approved federally by DHS/FNS (in consultation with federal agencies generally, and NIST and NSA specifically).

Visibility at the Organization’s Enterprise Level:

The information about hardware assets can be:

- Viewed at the level of the whole reporting organization or
- Viewed at the level of each organizational component, and long as the organizational components are operated as semi-independent units and are large enough to provide reasonable economies of scale, while remaining manageable. (Organizations should consult with DHS/FNS on the appropriateness of these components, if in doubt.)

3. CONFIGURATION MANAGEMENT

3.1 For each operating system Vendor, Product, Version, and patch-level[52] combination referenced in 2.4, report the following:

3.1a Whether an adequately secure configuration baseline has been defined[53]. (KFM)

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

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? (AP)

3.1d How frequently is the identification of deviations conducted? (Answer in days, per General Instructions) (Base)

3.2 For each of the enterprise-wide COTS general purpose applications Vendor, Product, Version, and patch-level[54] combination referenced in question 2.5., report:

3.2a Whether an adequately secure configuration baseline has been defined.[55] (KFM)

3.2b The number of hardware assets with this software (which are covered by this baseline, if it exists). (KFM)

3.2c For what percentage of the applicable hardware assets, with each kind of software in 3.2, has an automated capability to identify configuration deviations from the approved defined baselines and provide visibility at the organization's enterprise level? (KFM)

[52] 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.

[53] "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.

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

[55] Consider an Organization approved deviation as ***part*** of the Organization standard security configuration baseline. If the organization chooses to adopt an external configuration baseline without change, that should be counted here as well.

3.2d How frequently is the identification of deviations conducted? (Answer in days, per General Instructions) (Base)

3.3 Report the number of hardware assets from 2.0 to which the FDCC/USGCB baseline applies[56]. (Base)

3.3a Report the number of CCEs in the FDCC/USGCB baselines where the organization has approved deviations from the FDCC/USGCB standard across the organization (or organizational sub-components). List those specific CCEs in the comment. (Base)

3.3b For each CCE in 3.3, indicate in the comment the CCE and the number of assets in 2 (2.1) to which the FDCC/USGCB standard applies, but has been relaxed (through an approved deviation) by the organization. Report the sum of these numbers (count of asset-CCE pairs that have been relaxed) in the response. (Base)

[56] Include Organizational variants of the FDCC/USGCB baseline, if the Organization has reported the variation from the standard to OMB, as required.

Purpose, Future Metrics, and Definitions

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:
  - 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).

Expected Areas of Future Expansion for Configuration Management

Area of Expansion	Target for Future Inclusion
• Specific targets for coverage of the automated detection capability completeness, and baseline for accuracy. • Question 3.2b to an Administration Priority.	As soon as FY2013
• Expectation that desired configurations are well defined for common operating systems and applications, that they are being monitored, and that deviations are found and corrected to an acceptable level.	As soon as FY2014

Table 4 – Expected Areas of Future Expansion for Configuration Management

Each of these sections would require agencies to know a) desired configuration checks for common[57] operating systems and applications to provide adequate security, b)actual automated configuration data[58] to match desired configurations, c) unauthorized configurations list (i.e., the difference between a and b), and d) to rapidly[59] correct configurations to an acceptable level[60].

[57] It may not be practical to have configuration guides for all software. Attention should be focused on the software which is widely targeted (high threat), has known weaknesses which can be fixed through configuration (high vulnerability), and which would cause the most damage if exploited (high impact). Each organization should use risk-based analysis to set these priorities.

[58] Because of limits to the ability to conduct automated checks, this may typically not cover 100% of the desired configurations. If not, the organization should use risk-based analysis to find an adequate way to manage the other checks, or determine that they are not necessary.

[59] Rapidly means fast enough to deter most attacks.

[60] An acceptable level does not mean zero configuration deviations, but rather that the worst are fixed, and that the remainder represents an acceptable risk, as determined by the agency's risk-based analysis.

Definitions for FY2012:

Applicable Hardware Assets:

"Applicable hardware assets" means those hardware assets counted in section 2.0 which have the software being configured and installed on the asset.

Automated Capability to Identify Configuration Deviations from the Approved Baselines:

Any report of assets that can be generated by a computer. This includes:

- Active configuration scanners
- Agents on devices that report configuration
- Reports from software that can self-report its configuration
- Running a script in order to retrieve data
- Any other reliable and valid method
- Some combination of the above

Organization Approved Deviation:[61]

This shall be interpreted to include:

- Deviations approved for specific devices or classes of devices.
- Deviations approved for specific classes of users
- Deviations approved for specific combinations of operating system and/or applications
- Deviations approved for other purposes to meet business needs.

Such deviations should generally be supported by a risk-based analysis[62] which justifies any increased risk of the deviation, based on business needs. The deviation may be approved at the level of the organization, organizational component, or network. The approval should come from the system owner and the designated authorizing authority.

[61] Organizations that adopt generic standard configurations without deviation should be perfectly free to do so, as long as those configurations were developed by a source that adequately addressed security (NSA, NIST, DISA, etc.).

[62] This should not be interpreted as a requirement for overly extensive documentation of these risk-based analyses, but rather for just enough to allow the system owner and AO to make an informed decision.

4. VULNERABILITY AND WEAKNESS MANAGEMENT

4.1 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. (AP)[63]

4.1.1 Provide the number of hardware assets identified in section 2.0 that were evaluated using tools to assess the security of the systems and that generated output compliant with each of the following:

4.1.1a Common Vulnerabilities and Exposures (CVE); (Base)

4.1.1b Common Vulnerability Scoring System (CVSS); (Base)

4.1.1c Open Vulnerability and Assessment Language (OVAL); (Base)

4.2 NVD and the Secure Content Automation Program (SCAP) are focused primarily on common COTS operating systems and applications, after they are released. However, COTS and non-COTS software need to be searched for weaknesses before release. It is often useful to check open –source software for weaknesses, if the developer has not thoroughly done so. What methods has your organization considered using to find, identify, and assess weaknesses that may be in software that your organization develops and uses[64]: (Base)

Identify Universe	Find Instances	Assess Importance
Enumeration	**Tools and Languages**	
• Common Weakness Enumeration (CWE) • Web scanners for web-based applications	• Static Code Analysis Tools Manual code reviews (especially for weaknesses not covered by the automated tools)	• Common Weakness Scoring System (CWSS)
• Common Attack Pattern Enumeration and Classification (CAPEC)	• Dynamic Code Analysis Tools • Web scanners for web-based applications • PEN testing for attack types not covered by the automated tools.	

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

[64] This question is included here to understand the Organization's opinions about the usefulness of these technologies. Please review the link above before answering. Responses will be used to assess the viability of the technologies listed, and/or to determine the need for education in how they may be used. In no way should this question be interpreted to imply a mandate that they all should have been used in FY2012. It is expected that vulnerability scans conducted are based on (at least) the National Vulnerability Database, CVEs, and CVSS. It is at the discretion of DHS whether these responses will be reported to Congress at this time. It would be not to report on individual departments but more on the value of these tools.

See guidance from DHS which describes the purpose and use of these tools, and how they can be used today in a practical way to improve security of software during development and maintenance.

Please describe these and other methods you think are viable (and any experience you have with them) in the comments section. Please describe any significant obstacles to the use of these tools that need to be addressed.(Base)

4.3 For what percentage of information systems does the organization[65]: (Base)

		For system in development and/or maintenance:	**For systems in production:**
		Use methods described in section 4.2 to identify and fix instances of common weaknesses, prior to placing that version of the code into production. Can you find SCAP compliant tools and good SCAP content?	Report on configuration and vulnerability levels for hardware assets supporting those systems, giving application owners an assessment of risk inherited from the general support system (network). Can you find SCAP compliant tools and good SCAP content?
Impact Level	High		
	Moderate		
	Low		

[65] The presence of this question about identifying weaknesses in non-COTS software does not require any organization to use the tools described in section 4.2, as long as some effective method is used to adequately find and remove common weaknesses and prevent common attack patterns from compromising software. Adequate security (not perfection) is the standard of performance.

Purpose, Future Metrics, and Definitions

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).

Expected Areas of Future Expansion for Vulnerability and Weakness Management

Area of Expansion	Target for future inclusion
• The organization knows (with adequate completeness) what vulnerabilities it may be exposed to based on the software installed. • The organization removes detected vulnerabilities in a prioritized and adequately timely manner to provide adequate security. • Evaluate software weakness and vulnerabilities through Software Assurance metrics.	As soon as FY2013
• The overall level of vulnerabilities is adequately low. • Appropriate measures of software assurance for non-COTS software are being implemented. • Enhance the procurement process and supply chain security effort to consider software assurance as part of the acquisition process.	As soon as FY2014

Table 5 – Expected Areas of Future Expansion for Vulnerability and Weakness Management

Each of these sections would require agencies to know a) potential vulnerabilities from NVD for installed[66] operating systems and applications and weaknesses from CWE and CAPEC analysis to provide adequate security[67], b) actual vulnerability/weakness data[68], c) to rapidly[69] reduce vulnerabilities and weaknesses to an acceptable level[70].

Definitions for FY2012:

Automated capability to Identify Vulnerabilities:

Any report of actual assets that can be generated by a computer. This includes:

- Active vulnerability scanners
- Agents on devices that report vulnerabilities
- Reports from software that can self-report its version and patch-level, which is then used to identify vulnerabilities from NVD that are applicable to that version and patch-level
- Any other reliable and valid method
- Some combination of the above

[66] The organization can use this data to verify that it is checking for these vulnerabilities.

[67] See General Instructions

[68] Because of limits to the ability to conduct automated checks, this may typically not cover 100% of the desired devices. If not, the organization should use risk-based analysis to find an adequate way to manage the other checks, or determine that they are not necessary.

[69] Rapidly means fast enough to deter most attacks.

[70] An acceptable level does not mean zero vulnerabilities, but rather that the worst are fixed, and that the remainder represent an acceptable risk, as determined by the organization's risk-based analysis.

5. IDENTITY AND ACCESS MANAGEMENT

5.1 What is the number of Organization unprivileged network user accounts[71]? (Exclude privileged network user accounts and non-user accounts) (AP)

5.2 How many unprivileged network user accounts are configured to:

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

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

5.4 How many privileged network user accounts are configured to:

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

Note: If the organization meets AP for these controls at the network level (questions 5.1 - 5.4), then questions (5.5 - 5.8) at the application level, may be skipped.

[71] The term "network user accounts" intentionally excludes application accounts. For this section, the only relevant networks are SBU (or higher impact) networks.

5.5 What is the number of Organization unprivileged (high and moderate impact) application user accounts[72]? (Exclude privileged application user accounts and non-user accounts) (Base)

5.6 How many unprivileged application user accounts are configured to:

	a. Require the form of identification listed on the left? (Base)	b. Allow, but not require, the form of identification listed on the left? (Base)
5.6a User-ID and Password (Base)		
5.6b Two factor-PIV Card (Base)		
5.6c Other two factor authentication (Base)		

5.7 What is the number of Organization privileged application user accounts (Exclude non-user accounts and unprivileged application user accounts)? (Base)

5.8 How many privileged application user accounts are configured to:

	a. Require the form of identification listed on the left? (Base)	b. Allow, but not require, the form of identification listed on the left? (Base)
5.8a User-ID and Password (Base)		
5.8b Two factor-PIV Card (Base)		
5.8c Other two factor authentication (Base)		

5.9. Provide the percent of privileged network users[73] whose privileges were reviewed this year for a) privileges on that account reconciled with work requirements and b) adequate separation of duties considering aggregated privileges on all accounts for the same person (user). (Base)

[72] For questions 5.5 – 5.8, we ask about application user accounts, because some organizations apply these controls at the application, rather than at the network level. Definitions still link to network accounts. Definitions for this section are analogous to the network definitions, where the word network is replaced by "application".

[73] If the organization conducts its review by network user accounts with elevated privileges, rather than by privileged network users, then count the privileged network users as reviewed if any of their network user accounts with elevated privileges were reviewed.

5.9a Provide the percent of privileged network users whose privileges were adjusted or terminated after being reviewed this year. (Base)

5.10. Please describe in comments any best practices your Organization has developed in any of the following areas which are generally difficult in Federal Organizations. (Base)

- Methods to identify accounts that actually have elevated privileges even though not intended or indicated by the account name.
- Methods used to accurately and automatically identify all of the accounts assigned to the same person.
- Methods used to identify all account holders who have departed location or service and should have their accounts disabled and removed, especially if your method covers all account holders (your organization’s direct hire employees, institutional contractors, persons detailed to your organization from others, locally engaged staff overseas, etc.) by the same method.

Purpose, Future Metrics, and Definitions

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.[74]
- 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).

Expected Areas of Future Expansion for Identity and Access Management

Area of Expansion	Target for Future Inclusion
• PIV – enabled applications • PIV – enabled remote access solutions • PIV Metrics – This will be published as soon as determined by the Strong Logical Access Authentication Tiger Team.	As soon as FY2013
• Add network account asset inventory parallel to the hardware asset inventory.	As soon as FY2014

[74] 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 is to control access.

Table 6 – Expected Areas of Future Expansion for Identity and Access Management

Each of these sections would require agencies to a) know the desired state of the identity and access protections to provide adequate security[75], b) know the actual state of the identity and access protections, c) identify and prioritize the differences between a and b, and d) to rapidly[76] correct differences in a prioritized manner, to an acceptable level[77].

[75] See Definitions section.

[76] Rapidly means fast enough to deter most attacks.

[77] An acceptable level does not mean zero differences, but rather that the worst are fixed, and that the remainder represents acceptable risks, as determined by the organization's risk-based analysis.

Definitions for FY2012:

Allow a Specific Form of Identification:

The specific form of identification (credential) listed in the question may be used for authentication, but this form is not required because at least one other type of credential may also be used. (In this case, the form of authentication chosen may affect privileges to some degree.) Contrast with "Require a Specific Form of Identification".

Network User Accounts:

Network user accounts are user accounts that are defined on the network, rather than on a local machine. It is assumed that these ***network*** accounts are the primary type used, and that ***local*** (machine) accounts are accessed primarily through network level accounts and credentials.

Network User Accounts with Elevated Privileges:

(Also known as "Privileged Network User Accounts".)

A privileged network user account is a network user account which provides access to powers and data within the system/application that are significantly greater than those available to the majority of user accounts.

Such greater powers include, but are not limited to the ability to:

- View/copy/modify/delete sensitive system meta-information[78] and/or network resources.
- The ability to change the access rights to network resources.

At a low level of privilege, the user account with elevated privileges may only be able to perform limited privileged functions on a subset of objects on the network. At the other extreme, the user account with elevated privileges may have full control of all objects on the network. The risk (impact) of compromise is greater, as the account has more privileges.

User accounts with elevated privileges are typically allocated to System Administrators, Network Administrators, DBAs, and others who are responsible for system/application control, monitoring, or administration functions. ***(Exclude system and application accounts utilized by processes as they are not user accounts, and local workstation administrators as they are not network accounts)***

[78] System Meta-Information means the information used to configure the network, a device, an operating system or application on the device, a user-account, a policy object, an executable file, etc. In general it does not include the ability to view/copy/modify/delete the documents and transactions necessary for a person to perform a normal business function. But it does include "super-users" of a business application that have broad rights to view/copy/modify/delete the transactions of multiple other users.

Network User Accounts without Elevated Privileges:

(Also known as “Unprivileged Network User Accounts”.)

Is a network user account that is not a network user account with elevated privileges.

Non-user Account:

Non-user account is an account intended to be controlled directly by a person (or group). The account is either a) intended to be used by the system or an application, which presents credentials and performs functions under the management of the person (or group) that owns the account[79] or b) created to establish a service (like a group mailbox), and no-one is expected to log into the account. Non-user accounts are typically called group mailbox, service and/or system accounts.[80]

Other Two Factor Authentication:

Some other form of two factor authentication (e.g., not involving a PIV Card). For example, a User-ID and password combined with a random token generator (fob).

PIV credentials:

A PIV Card (credential) is a “Personal Identity Verification Card” as defined in NIST FIPS 201. For the purposes of answering this question we only count cards that use three-factor authentication. Typically the card is read through a reader that takes a security certificate from the PIV Card. The same user will then be identified by some other factor. DoD Common Access Cards (CAC Cards) are included in this category for DoD Organizations.

Privileged Network User:

A privileged network user is a user who, by virtue of function, and/or seniority, has been allocated a network user account with elevated privileges. Such persons will include, for example, the system administrator(s) and Network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users.[81]

Require a Specific Form of Identification:

Only this specific form of identification (credential) may be used for authentication. Contrast with “Allow a Specific Form of Identification”.

User Accounts:

A user account is an account that is intended to be controlled directly by a particular person to perform work. The person presents their credential to gain access. Include temporary, guest, and generic “student”, etc. with these accounts.

[79] For example, this includes machine accounts and operating system built-in accounts. More generally, it includes “service” accounts.

[80] This does not include maintenance provider accounts, where the “user” is a person, nor does it include cloud provider system administrators. Those accounts are to be included in “user accounts”.

[81] http://www.yourwindow.to/information-security/gl_privilegeduser.htm

User-ID and Password:

User-ID and password is the traditional credential used on most networks. The USER-ID is public, and the password is private. Therefore this is considered to be one-factor authentication.

6. DATA PROTECTION

6.1. Provide the estimated number of hardware assets from Question 2.0 which have the following characteristics. Enter responses in the table. (KFM)

Mobile Assets Types (each asset should be recorded ***no more than once*** in each column)	a. Estimated number of mobile hardware assets of the types indicated in each row	b. Estimated number assets from column a ***with adequate encryption of data on the device.***[82]
- 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)		

6.2. Provide the percentage of Organization email traffic on systems that implement FIPS 140-2 compliant encryption technologies to protect the integrity of the contents and sender information when sending messages to government agencies or the public, such as S/MIME, PGP, OpenPGP, or PKI. (KFM)

6.3 Select the description that best describes your Organization's PKI Certificate Authority, and respond with the number of that option. (Base) The organization:

1. Self-manages a legacy PKI certificate authority (which is not a *Federal Shared Service Provider)*.
2. Is a *Federal Shared PKI Service Provider.*
3. *Receives PKI support from a Federal or commercial Shared Service Provider, but which is responsible for some portion of the PKI service.*
4. *Other source of PKI Certificate Authority.*

6.4 What percentage of the applicable Security Controls from NIST SP 800-53A (profiled by FPKIPA[83]) does the PKI Certificate Authority and related PKI Infrastructure your organization uses adequately[84] satisfy? (Base)Purpose, Future Metrics, and Definitions

[82] The numbers in column 'b' cannot be larger than the numbers in column 'a'.
[83] FPKIPA (Federal Public Key Infrastructure Policy Authority).
[84] See Definitions

Purpose, Future Metrics, and Definitions

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

Expected Areas of Future Expansion for Data Protection

Area of Expansion	Target for Future Inclusion
• Mandatory use of S/MIME PIV signed email • Data Loss Prevention (DLP)/Digital Rights Management (DRM) • Cloud computing data protection solutions • Mobile device protection capabilities	As soon as FY2013
• Solutions to consider alternative lightweight in transit/storage protection • BYOD mobile data protection capabilities	As soon as FY2014

Table 7 – Expected Areas of Future Expansion for Data Protection

Definitions for FY2012:

Adequate encryption: all user data in encrypted with FIPS 140-2 validated cryptographic modules, or modules approved for classified data. If the device is not allowed to contain sensitive but unclassified information, you should count it as adequately encrypted.

BlackBerry: A brand of smartphone provided by the Canadian Firm Research in Motion (RIM).

Certificate Authority: In cryptography, a **certificate authority**, or **certification authority**, (**CA**) is an entity that issues digital certificates. The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified.

Estimated total number:[85] While it would be better if the organization could accurately count all mobile assets, this may not be feasible for all asset types. The intent is that the organization should know the number of mobile assets with sufficient accuracy to be able to measure progress from year-to-year on managing encryption and other controls. Thus, these estimates should be less than an order of magnitude more accurate than the expected rate of improvement. If the organization made a very small amount of improvement, or cannot tell whether it made improvement for year-to-year because of the inability to count these assets, then this should be indicated in the comments.

Flashdrives: A solid-state drive (SSD), sometimes called a solid-state disk or electronic disk, is a data storage device that uses solid-state memory to store persistent data with the intention of providing access in the same manner as a traditional block I/O hard disk drive. These may connect through a USB port, or sometimes may be plugged directly into a device like a smartphone. In either case, they can leave data in a highly vulnerable state.

Laptop Computer: A computer intended to be carried by the user and used in a wide variety of environments, including public spaces.

Mobile hardware assets: A hardware asset (typically holding data, software, and computing capability) designed to be used in a wide variety of environments, including public spaces, and/or connected to a number of different networks. These often have wireless capability requiring special controls.

Netbook: a category of small, lightweight, and inexpensive laptop computers. They typically lack an internal CD/DVD drive, legacy ports, an ISA bus, or sometimes, any internal expansion bus at all.

[85] Asking for an estimated number does not relieve the Organization for careful management of all "assets", nor change the FISMA requirement to provide security for all "systems".

Personal Digital Assistant: A personal digital assistant (PDA), also known as a palmtop computer, or personal data assistant, is a mobile device that functions as a personal information manager.

PGP and OpenPGP: Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions to increase data security. The goal of the OpenPGP working group is to provide standards for the algorithms and formats of PGP processed objects as well as providing the MIME framework for exchanging them via e-mail or other transport protocols.

Public Key Infrastructure (PKI): collection of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. Ideally these certificates can be recognized widely. In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique within each CA domain. The binding is established through the registration and issuance process, which, depending on the level of assurance the binding has, may be carried out by software at a CA, or under human supervision. The PKI role that assures this binding is called the Registration Authority (RA). The RA ensures that the public key is bound to the individual to which it is assigned in a way that ensures non-repudiation.

PKI Certificate Authority: See Certificate Authority.

Removable Hard Drives: Hard Drives usually connected to the computer through USB ports, which reside external to the computer and allow easy removal and connection to other computers. This category could also include similar drives connected directly to the network which allow easy removal and connection to other networks.

Smartphone: A high-end mobile phone built on a **mobile computing platform**, with more advanced **computing ability and connectivity** than a contemporary feature phone.

S/MIME (Secure/Multipurpose Internet Mail Extensions): A standard for public key encryption and signing of MIME data. S/MIME is on an IETF standards track and defined in a number of documents, most importantly RFCs (3369, 3370, 3850, 3851). S/MIME functionality is built into the majority of modern email software and interoperates between them.

Tablet Computers: A tablet computer, or a tablet, is a mobile computer, larger than a mobile phone or personal digital assistant, integrated into a flat touch screen and primarily operated by touching the screen rather than using a physical keyboard. It often uses an onscreen virtual keyboard, a passive stylus pen, or a digital pen.

7. BOUNDARY PROTECTION

Instruction: Questions 7.1 – 7.2 apply only to Federal Civilian Agency TIC Access Providers (TICAPs). If the reporting organization, is not a) a federal civilian agency and/or b) not a TIC access provider, then answer N/A to these questions.

7.1. Provide the percentage of the required TIC 1.0 Capabilities that are implemented. (AP)

7.1a**.** Provide the percentage of TIC 2.0 Capabilities that are implemented. (AP)

7.2. Provide the percentage of TICs with operational NCPS (Einstein) deployment.

7.2a. Einstein 2? (AP)

7.2b. Einstein 3? (KFM)

Instruction: Questions 7.3-7.4 apply only to Federal Civilian Agency. If the reporting organization, is not a federal civilian agency then answer N/A to these questions.

7.3. Provide the percentage of external network traffic to/from the organization's networks passing through a TIC/MTIPS. (AP)

7.4. Provide the percentage of external network/application interconnections to/from the organization's networks passing through a TIC/MTIPS. (KFM)

Instruction: The Remaining questions apply to all reporting organizations.

7.5. Provide the percentage of Organization email systems that implement sender verification (anti-spoofing) technologies when sending messages. (KFM)

7.6. Provide the percentage of Organization email systems that check sender verification (anti-spoofing) technologies to detect possibly forged messages from outside the network. (KFM)

7.7 Provide the estimated percent of incoming email traffic (measured in messages) where the link/attachment is executed/opened in a sandbox/virtual environment in-line to ascertain whether or not it is malicious, and quarantined as appropriate, before it can be opened by the recipient. (Note: If you consider this to be infeasible, please explain why in the comments.) (Base)

7.8. Provide the frequency (in days, e.g., 30.0 or 0.25) in which the Organization conducts scheduled scans for unauthorized wireless access points (WAP) connected to an Organizational network. (Base)

7.8a. Provide the percentage of hardware assets, identified in section 2.0 (Asset Management), which are in facilities where WAP scans are conducted. (Base)

7.9. Provide the frequency (in days, e.g., 30.0 or 0.25) in which the Organization conducts unscheduled scans for unauthorized wireless access points. (Base)

7.10 Provide the frequency (in days, e.g., 30.0 or 0.25) in which the Organization maps their cyber perimeter (e.g. publically accessible systems, externally visible systems and devices) for each network. (Base)

7.11 Provide the percent of client browsers that are required to run only in a virtual environment. (Base)

7.12 What percentage of network boundary devices are assessed by an automated capability to ensure that they continue to be adequately free of vulnerabilities and are adequately configured as intended, such as to adequately protect security? (Base)

7.13 Provide the number of cloud systems from question 1.2a where traffic entering and exiting the cloud:

7.13a) does not pass through a TIC? (Base)

7.13b) are not required to pass through a TIC? (Base)

7.14 Provide the number of networks with DLP/DRM at the gateway to capture outbound data leakage (e.g., PII). (Base)

Purpose, Future Metrics, and Definitions

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).

Expected Areas of Future Expansion for Boundary Protection

Area of Expansion	Target for Future Inclusion
• Encryption • Knowing desired and actual state over some kinds of boundary protections • Identifying and fixing differences for some boundary protections • Elevate 7.7 to an Administration Priority • Elevate DLP/DRM at the gateway for content inspection	As soon as FY2013
• Timeliness of monitoring and response • Adequate coverage of monitoring and response for all assets, as applicable	As soon as FY2014

Table 8 – Expected Areas of Future Expansion for Boundary Protection

Each of these sections would require agencies to a) know the desired state of the boundary protections to provide adequate security[86], b) know the actual state of the boundary protections, c) identify and prioritize the differences between a and b, and d) to rapidly[87] correct differences in a prioritized manner, to an acceptable level[88].

[86] See Definitions section.

[87] Rapidly means fast enough to deter most attacks.

[88] An acceptable level does not mean zero differences, but rather that the worst are fixed, and that the remainder represents an acceptable risk, as determined by the organization's risk-based analysis.

Definitions for FY2012:

Automated Capability:

An automated capability as defined in the sections on vulnerability and/or configuration management.

Cyber Perimeter:

The boundary of the network as defined in its system security plan. Generally this corresponds to an authorized layer of firewall(s) and other boundary protection devices through which the network communicates with a) the internet, b) other wide-private networks, and/or c) directly to other trusted networks. However, it may also (unintentionally) include unauthorized connections from inside the system to/from the outside of the system, which create significant risk.

E-mail Systems:

Email systems are made up of organizational software, i.e., outlook exchange or Gmail, which provide email accounts that enable people to exchange digital messages. Any e-mail system which will send and receive official mail on behalf of the organization, and which is treated by trusted by the organization should be included. Thus, any e-mail system inside the authorization boundary of an organizational network would be included. An external e-mail system (like Google-mail) would be excluded if mail from it to/from the network is treated as any other untrusted e-mail, while it would be included, otherwise.

Network (aka General Support System, GSS):

Is used as defined in *OMB A-130, Appendix III*

Network boundary Devices:

Devices that are part of the cyber perimeter.

Operational NCPS (Einstein 2/3) Deployment:

National Cyber Protection System, operationally known as EINSTEIN (i.e., “Einstein”, “Einstein v2”, or “Einstein Program”), is a sensor that monitors all external connections at a TIC access point. Agency participation in NCPS, includes, full compliance with the functional requirements to achieve working order and to maintain status of use (as defined by US-CERT/NCPS). These functional requirements are available on the OMB MAX Portal.

Scheduled Scans:

Are scans (or other automated capabilities) in which the person managing the devices to be scanned knows when to expect the scan. Such scans allow the person managing the devices to prepare for the scan.

Sender Verification (anti-spoofing) Technologies:

These include:

- Domain Keys Identified Mail (DKIM)

- Sender Policy Framework (SPF)
- Digital Signing of e-mail using PKI
- Other technologies with abilities to prevent spoofing (described in the comments)

TIC 1.0 Capabilities:

A body of 51 critical capabilities that were collaboratively developed to outline the baseline security requirements set forth by the TIC Reference Architecture V1.0. These are available on OMB's MAX Portal.

TIC 2.0 Capabilities:

This is a body of 60 critical capabilities that were collaboratively developed to improve upon the baseline security requirements in TIC Reference Architecture V1.0. These are available on OMB's MAX Portal.

TIC/MTIPS (Trusted Internet Connections/Managed Trusted Internet Protocol Services):

This is a GSA program described by both DHS and GSA.

Unscheduled Scans:

Scans (or other automated capabilities) in which the person managing the devices to be scanned does not know when to expect the scan. Such scans do not allow the person managing the devices to prepare for the scan, and thus provide a more accurate view of the hardware assets.

Virtual Environment:

Defined as a temporary environment (created on the fly with an adequately correct configuration and low vulnerability rate) that shields the physical machine, and the network it is in, from changes to the virtual machine created by exploits run through the browser.

8. INCIDENT MANAGEMENT

8.1. What is the number of Organization hardware assets (from question 2.0) on networks on which controlled network penetration testing was performed in the reporting period?[89] (KFM)

For the testing conducted above, provide the following information:

8.1a. Percentage of applicable events detected by NOC/SOC[90] during the penetration test. (KFM)	
8.1a (1). Median time to detection of applicable events. (Time in days and fractions of days. See General Instructions.) (KFM)	

8.2. During FY12, for what percentage of US-CERT Security Awareness Reports (SARs), or the equivalent for DoD[91], has the organization adequately remediated[92] or acted upon the actionable recommendations[93] contained in the report? (Base) Please use the Comment function to comment on how the SAR process is meeting its goal and/or could be improved.

8.3 Provide the percentage of incidents that have been detected and attributed to successful phishing attacks. (Base) Please provide a Comment to describe any innovative and effective ways your organization has found to address these attacks.

[89] Section 8.1 is applicable only to reporting **events** (pseudo-incidents) that are discovered during the controlled network penetration test. The question does not address actual security incidents found during routine operation of the incident management process. The intent of this question is to measure the detection and response capabilities of the NOC/SOC under simulated real-time conditions. The measured outcome can be used to determine whether the NOC/SOC is staffed with the correct personnel and technologies. Although the NOC/SOC is tested in real life on a continual basis the controlled nature of these penetration tests allows for the detection and response to be most readily measured.

[90] Some Organizations (especially micro-agencies) may use something other than a NOC/SOC. If so, they may count the detections that it produced, but should clearly describe their alternate methods in the comments.

[91] Information Assurance Vulnerability Alerts (IAVA) for DoD are roughly equivalent to SARs for civilian agencies.

[92] Adequately remediated means that the Organization has conducted a risk based analysis to determine the impact of the threat on that organization, and appropriate action. Appropriate action to provide adequate security (see General Instructions), may range from no action to complete remediation, based on the assessment of risk and cost made by the Organization.

[93] If the report contained no actionable recommendations, then it is considered adequately remediated.

Purpose, Future Metrics, and Definitions

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.
- The question (8.2) about use of SARs is intended to assess the use of this process by Organizations.
- The question (8.3) about phishing is included because of the pervasive nature of this attack vector.

Expected Areas of Future Expansion for Incident Management

Area of Expansion	Target for Future Inclusion
• Increasing levels of detection in shorter periods of time. • Increasing % of incidents "tipped"[94] via: ○ DHS-USCERT/Einstein ○ Internal Threat Analysis ○ Intelligence Threat Analysis ○ Public Threat Analysis ○ Other Threat Analysis	As soon as FY2013
• Metrics related to effective and timely remediation of such applicable events.	As soon as FY2014

Table 9 – Expected Areas of Future Expansion for Incident Management

Each of these sections would require agencies to identify incidents and adequately respond in a timely manner to mitigate the incidents.

[94] A signature or other symptom that indicates a possible incident.

Definitions for FY2012:

Applicable Events: Events generated during a penetration test which would be expected to be detected to demonstrate an adequate level of security[95] on the network.

Event: In this context of penetration testing, an event is an incident-like action, created by the penetration test team. Technically, this not an incident since it was approved by the AO (or other appropriate authority) as part of the test plan, and will generally be designed to stop before compromising mission performance.

Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices (per NIST SP 800-61). While this definition is based on compliance, it is also appropriate to consider a broader definition of incident as being any event which compromises the confidentiality, integrity and availability of the Organization's information to an extent that has a noticeable negative impact on mission performance (See NIST SP 800-39 which justifies this more risk-based definition).

Median: A form of average in which 50% of the items being averaged are smaller, and 50% are larger.

Penetration testing: A testing methodology in which assessors attempt to challenge (circumvent or defeat) the security features of an information system or network. Generally, they are working under specific guidelines that prevent the test from causing a compromise of mission performance.

Controlled penetration testing: Penetration testing sponsored by the Organization or organizational component. The purpose of this test is to determine a) available means of attack, but also b) whether the network defenders (typically the NOC/SOC) detect the attack. Therefore, ideally a controlled penetration test would be known to managers but unannounced to front-line operators.

Network penetration testing: Penetration testing performed on the Organization's network.

Successful Phishing Attack: A network user responds to fraudulent message producing a negative impact on confidentiality, integrity, and/or availability of the Organization's information.

Time to Detection: The time from event occurrence to detection by the network monitors. It does not include time to respond to and defend against the event.

[95] Adequate security is defined in the General Instructions.

US-CERT Security Awareness Reports: Are reports issued by DHS/US-CERT to communicate broad assessments of threats and inform Organizations with actionable recommendations for monitoring and responding to suspicious activity.

9. TRAINING AND EDUCATION

Note: In section 5, you were asked to provide the number of unprivileged and privileged network users. This section assumes that these represent the "universe" of all users for the organization (who thus need training). If this is not the case, please explain in the comments to question 9.1

9.1. Provide the number of the Organization's network users that have been given and successfully completed cybersecurity awareness training in FY2012 (at least annually[96]). (KFM)

9.1a. Provide the estimated percentage of new users to satisfactorily complete security awareness training before being granted network access, or within an organizationally defined time limit, providing adequate security, after being granted access. (KFM)

9.2. To what extent were users given cybersecurity awareness training content more frequently than annually[97] (content could include a single question or tip of the day)?

9.2a. Provide the average frequency in days between content provision. See General Instructions. (Base)	
9.2b. Provide the percentage of this additional content that addresses emerging threats that were not previously covered[98] in the annual training? (Base)	
9.2c. At what frequency is security awareness training content (that is provided to users) updated by the Organization or training provider? (Average frequency in days during FY2012. See General Instructions.) (Base)	
9.2d. Provide the total number of Organization-sponsored emerging threat exercises (such as phishing) designed to increase cybersecurity awareness and/or to measure the effectiveness of cybersecurity awareness training in molding behavior. (Base)	
9.2e. Provide the percentage of exercises in 9.2d where either no problems were found, or in which the problems were addressed through appropriate training within three months. (Base)	

9.3. Provide the number of the Organization's network users and other staff[99] with significant security responsibilities. (Base)

[98] If training is routinely done by periodic training spread over the year, then "not previously covered" means what percentage of the content was added or strengthened during the year.

9.3a. Provide the number of people in 9.3 that have been given training to perform their significant cybersecurity responsibilities at an organizationally defined frequency that has been determined to provide adequate security. (KFM)	
9.3b. Provide the longest organizationally defined frequency that has been determined to provide adequate security for any role among those included in significant security responsibilities. (Days between training events. See general instructions) (Base)	
9.3c. At what frequency is training to perform their significant cybersecurity responsibilities updated by the Organization or training provider? (Average frequency in days across roles during FY2012. See General Instructions.) (Base)	

[99] Other staff here means non-network users who may still have a significant impact on security. This might include senior executives who do not use the network themselves, but affect budget, staffing, priorities, etc. Nevertheless, it is expected that the size of other staff with significant security responsibilities is small.

Purpose, Future Metrics, and Definitions

Purpose and Use

These questions are being asked for the following reasons:

- Some of the most effective attacks on cyber-networks, world-wide currently are directed at exploiting user behavior. These include phishing attacks, social engineering to obtain passwords, and introduction of malware via removable media.
- These threats are especially effective when directed at those with elevated network privileges and/or other elevated cyber responsibilities.
- Training users (privileged and unprivileged) and those with access to other pertinent information and media is a necessary deterrent to these methods. Therefore, Organizations are expected to use risk-based analysis to determine the correct amount, content, and frequency of update to achieve adequate security in the area of influencing these human behaviors that affect cybersecurity.
- DHS has determined that some metrics in this section are prioritized as Key FISMA Metrics.
- Some questions in this section also contain baseline information to be used to assess future improvement in performance.
- The metrics will be used to assess the extent to which Organizations are providing adequate training to address these attacks and threats.[100]

Expected Areas of Future Expansion for Training and Education

Area of Expansion	Target for Future Inclusion
• *Awareness:* Organizations have identified what unprivileged user behaviors most impact security and have incorporated these into an effective annual security program that trains almost all users annually. • *Significant Security Responsibilities:* Organizations have an ongoing training program for a substantial number of these persons. DHS (working with ISIMC and others) provides clear guidance on common roles that fit this category and the common behaviors that should be addressed in training.	FY2012 Base

[100] Even if the organization uses a DHS ISS-LOB, it remains the Organization's responsibility to determine whether the content of the training is adequate to cover the threats being faced by that Organization.

In addition to the goals for 2012, and earlier: • *Awareness:* the Organization has some mechanism to provide awareness of emerging threats throughout the year. • *Significant Security Responsibilities:* The Organization has effective training programs that are adequately complete and timely to address the federally defined common roles. Organizations have adapted the federal guidance from DHS to provide clear guidance on organization specific roles that fit this category and the common behaviors that should be addressed in training.	As soon as FY2013
In addition to the goals for 2013, and earlier: • *Awareness:* The Organization has some mechanism to test the effectiveness of some awareness training through exercises and/or other means. • *Significant Security Responsibilities:* The Organization has effective training programs that are adequately complete and timely to address the federally defined common roles and organization-specific roles. The Organization has some mechanism to test the effectiveness of some role-based training through exercises and/or other means.	As soon as FY2014

Table 10 – Expected Areas of Future Expansion for Training and Education

Successful performance in this area would require the Organization to know a) total inventory of persons needing training, and the content of training needed based on each person's role, b) a list of the actual training provided and the user's performance (usually test) result, c) defect list (the difference between a and b), and d) to have a process to address persons non-adequately trained by providing training or removing access rights and responsibilities.

Definitions for FY2012:

Network Users: Any person who has access to an unprivileged or privileged network account (as defined in Section 5) on any one (or more) of the Organization's networks.

Given and Successfully Completed Cybersecurity Awareness Training: User has received the training resulting in the ability to:

- avoid behaviors that would compromise cybersecurity.
- practice good behaviors that will increase cybersecurity.
- act wisely and cautiously, where judgment is needed, to increase cybersecurity.

in situations that are likely[101] to confront ***unprivileged*** network users.

Successful completion means (at a minimum) that the user has passed a test on the content. Preferably, it means that by some measure, the user's behavior and judgment is adequate to protect security.

Note that such training may be provided via a) periodic awareness training spread over the year, b) an annual course, and/or c) a combination of annual and more frequent training.

Given that the objective of this training is to affect behavior, training about concepts that are not actionable by the user during normal use of the information system is of little benefit.

Emerging Threat Exercises: These exercises include a) simulated threats where the user is not aware that the event is an exercise (user-blind exercise) to b) practice exercises where the user knows that the event is an exercise (non-blind exercise, much like an announced fire drill). Often, these blind exercises are more effective if the person's behavior is not recorded, but a failure takes the person to training material. Examples of this might include:

- A phishing drill that takes the user to material on how to identify and avoid phishing attacks.
- A response to a routine password change that takes the user to training on password complexity, if the provided password is not adequately complex.

Significant Security Responsibilities: *(also known as special cybersecurity roles and responsibilities): A network user has a role and/or responsibility such that cybersecurity awareness training, by itself, fails to describe all the behaviors that user needs to adequately protect cybersecurity. Persons with the following characteristics have "significant security responsibilities":*

[101] Likely here is meant to indicate that organizations should use risk-based analysis to decide what behaviors should be covered in this awareness training. Covering every possible threat could be counter-productive (distracting users from the common threats) and produce excessively long (expensive) training. Organizations are expected to conduct risk based analyses to determine the right level of training needed to most cost-effectively improve security based on identifying the behaviors that have the most impact given current threats and organizational countermeasures.

- *All users with privileged network user account(s)*
- *All other users who have managerial or operational responsibilities that allow them to increase or decrease cyber security.*

Significant Security Responsibility Training:

After receiving the training, the user should be able to:

- avoid behaviors that would compromise cybersecurity.
- practice good behaviors that will increase cybersecurity.
- act wisely and cautiously, where judgment is needed, to increase cybersecurity.

In situations that are likely[102] to confront as ***privileged*** network users or in other roles that materially and substantially affect cybersecurity beyond the behaviors covered in cybersecurity awareness training.

Note that such training may be provided via a) periodic awareness training spread over the year, b) an annual course, and/or c) a combination of annual and more frequent training.

Given that the objective of this training is to affect behavior, training about concepts that are not actionable by the user during performance of their significant cybersecurity responsibilities is of little benefit.

[102] Likely here is meant to indicate that organizations should use risk based analysis to decide what behaviors should be covered in this awareness training. Covering every possible threat could be counter-productive (distracting users from the common threats) and produce excessively long (expensive) training. Organizations are expected to conduct risk based analyses to determine the right level of training needed to most cost-effectively improve security.

10. REMOTE ACCESS

10.1. 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.

10.1a. For those connections counted above in 10.1, provide the estimated number of those connections that: [103] (KFM)

	• 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)					

*** Data from Column 'e)' feeds the table in question 10.1b**

[103] For 10.1a, 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 10.1. If this is not the case, explain the reason in the comments.

10.1b. For those connections counted above in 10.1a column e), provide the estimated number of those connections that:[104] (KFM)

	• Were authenticated by each of the methods listed on the right. • For each Type of connection listed below	a User-ID and Password (KFM)	b Two factor-PIV Card (KFM)	c Other two factor authentication	d Other(s). (Please describe in the comments.)
Type of Connection	1. Dial-up				
	2. Virtual Private Network (***IP SEC or other non-clientless)***				
	3. Virtual Private Network (clientless) including SSL, TLS, etc.				
	4. Citrix				
	5. Other (Add Rows as needed)				

10.1c. For those connections counted above in 10.1, provide the estimated percentage of those connections that:

Have this property:	**Estimated %**
Utilize FIPS 140-2 validated cryptographic modules. (KFM)	
Prohibit split tunneling and/or dual-connected remote hosts where the laptop has two active connections. (KFM)	
Are configured in accordance with OMB M-07-16, to time-out after 30 minutes of inactivity (or less) requiring re-authentication to reestablish session. (KFM)	
Scan for malware upon connection. (KFM)	
Require Government Furnished Equipment (GFE). (Base)	
Assess and correct system configuration upon connection of GFE. (Base)	

[104] For 10.1b, each connection from Table 10.1a column e will be in one or more cells of the same row in table 10.1b. The sum of each row should be greater than or equal to the total in the matching row of 10.1, column e. If this is not the case, explain the reason in the comments.

Purpose, Future Metrics, and Definitions

Purpose and Use

These questions are being asked for the following reasons:

- 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.

Expected Areas of Future Expansion for Remote Access

Area of Expansion	Target for Future Inclusion
• Increases in the number of connections (or connection methods) using better methods of ID and Authentication. • Increases in the number of connections (or connection methods) with better security posture.	FY2012
• Phase out of dial-up access. • Controls to protect against weaknesses in non-GFE devices that may be allowed to connect to the network: aka Bring you own Device (BYOD). • Controls to protect against weaknesses in an increasing number of mobile and wireless devices. • Protection of e-mail servers from being used as relay hosts.	As soon as FY2013
• Elimination of dial-up access.	As soon as FY2014

Table 11 – Expected Areas of Future Expansion for Remote Access

Successful performance in this area would require the Organization to know a) total inventory of remote connection methods and their desired security posture, b) a list of the actual remote connection methods, and their actual security posture, c) defect list (the difference between a and b), and d) to have a process to address the differences by a) removing unauthorized access methods, and b) correcting defects in the remote access method.

Definitions for FY2012:

Clientless-VPN/IPSec VPN: Clientless VPNs, also called SSL VPNs, provide remote workers and business partners with secure access to Web-enabled corporate resources via SSL-secured browser sessions. The technology, offered in various forms from several vendors, is easier to manage and less expensive than traditional IPSec VPNs that require client-side VPN software.

Dual Connected: A dual connected host refers to a situation where the host is connected to more than one network. The connections may be wired or wireless. The other network may be the user's home network or any other network. The area of concern is cross contamination between the other networks and the government network.

Estimated total number/percentage: The estimates are not intended to require the organization to count all connections and provide an exact count of connections. Rather, the intent is that the organization should know the number of connections with sufficient accuracy to be able to measure progress from year to year. Thus, these estimates should be about an order of magnitude more accurate than the expected rate of improvement. If the organization made a very small amount of improvement, or cannot tell whether it made improvement from year to year due to the inability to count the connections, then this should be indicated in the comments.

FIPS 140-2: FIPS 140-2 specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information (hereafter referred to as sensitive information). While many vendors claim their cryptographic modules are FIPS 140-2 compliant, ***only those currently certified*** by NIST as compliant can be reliably counted in this report.

Full access to the Organization's normal desktop LAN/WAN resources/services. Such full access is intended to include connections that provide many or most of the features of a full desktop. You should not exclude connections because of trivial differences from an actual desktop.

This phrasing is primarily intended to exclude the following kinds of more limited connections:

- Web Mail connections
- Smartphones (used only as phones and mail/calendaring connections)
- Tablets

unless these connections provide access to many or most desktop features. Such connections are excluded, for the time being, as they provide less risk and/or the Organization has less control over these resources.

Relay Host: A server that acts as a relay: it's accepting and agreeing to try to deliver a message that's not destined for a domain that the main server hosts.

Remote access connection methods: A set of mutually exclusive and exhaustive categories of methods that may be used to connect to your network, such that connections within each method identified have about the same level of risk and use similar technology.

Split Tunneling: Split tunneling is a method which allows a VPN user to access a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same physical network connection. This connection service is usually facilitated through a program such as a VPN client software application.

11. NETWORK SECURITY PROTOCOLS

11.1. Provide the number of public facing domain names[105] (second-level, e.g. www.dhs.gov). (You should exclude domain names which host only FIPS 199 low-impact information on ISPs.) (KFM)

11.1a. Provide the number of DNS names from 11.1, signed using DNSSEC. (KFM)

11.1b. Provide the percentage of the second-level DNS names from 11.1 and their sub-domains for which all domain names at and under the second level are signed. (KFM)

11.2. Provide the percentage of public facing servers[106] that use IPv6 (e.g., web servers, email servers, DNS servers, etc.). (Exclude low-impact networks, cloud servers, and ISP resources from the numerator and denominator unless they require IPv6 to perform their business function.) (KFM)

[105] The terms DNS names and Domain Names are interchangeable and synonymous.

[106] While the mandate refers to "servers and services", IPv6 addresses apply to hardware assets, not services. Thus, to avoid double counting this question refers to the servers only. The servers included should all host public facing services. The servers considered must include both physical and virtual servers.

Purpose, Future Metrics, and Definitions

Purpose and Use

These questions are being asked for the following reasons:

- The use of Domain Name System Security Extension (DNSSEC) has been mandated at the federal level to prevent the pirating of government domain names. GSA has ensured proper DNSSEC for the top level domain names. Each Organization is responsible for DNSSEC in sub-domain names, which are those below the top-level domain.
- Per the September 2010 IPv6 memo issued by OMB, agencies must upgrade public/external facing servers and services (e.g. web, email, DNS, ISP services, etc) to operationally use native IPv6 by the end of FY 2012; and upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 2014.
- This section is to assess Organizational progress toward meeting these federal level mandates.
- DHS/NPPD/NCSD/FNS offers tools to enable organizations to inspect for DNSSEC and IPv6 compliance. Organizations are expected to use these tools to measure compliance for this report.
- DHS/NPPD/NCSD/FNS also uses those tools to verify Organization self-reported results. In the past, the results have indicated considerable deviation between the self-reported results and the DHS verification results. Organizations are expected to be more aware of the DNSSEC and IPv6 status when reporting.
- Organizations should be aware that a key reason for DNSSEC compliance problems in the past has been expiring certificates which are not updated by the owning Organization.

Expected Areas of Future Expansion for Network Security Protocols

Area of Expansion	Target for Future Inclusion
• The mandate to complete DNSSEC implementation was issued in August 2008, and required compliance by Dec 2009. Thus, full (or near) full compliance is expected in 2012. • Organizations are to effectively manage certificate renewals to keep DNSSEC certificates valid. • Upgrade public/external[107] facing servers and services (e.g. web, email, DNS, ISP services[108], etc.) to operationally use native IPv6 by the end of FY 2012. • To ensure interoperability, it is expected that agencies will also continue running IPv4 into the foreseeable future. • Results of self-reported by the Organization can be verified as accurate by DHS through automated means, indicating that the organization is aware of and effectively maintaining its level of DNSSEC and IPv6 compliance.	FY2012 Base
• No additional DNSSEC requirements. • The Organization has adequate security inspection tools to verify the correct security configuration of the IPv6 devices, and is not limited to tools which only operate correctly in IPv4 address spaces.	As soon as FY2013
• No additional DNSSEC requirements. • Upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 2014. • To ensure interoperability, it is expected that agencies will also continue running IPv4 into the foreseeable future.	As soon as FY2014

Table 12 – Expected Areas of Future Expansion for Network Security Protocols

[107] Public/external should be interpreted to mean servers facing the internet with which general internet users (the public) are expected to interact. Interconnections a) to other federal agencies or b) other "private" interconnection to non-federal business partners are not "public/external".

[108] The ISP Services that require upgrades are those that need to be upgraded in order to perform their business function.

Definitions for FY2012:

DNSSEC: DNSSEC was designed to protect Internet resolvers (clients) from forged DNS data, such as that created by DNS. All answers in DNSSEC are digitally signed. By checking the digital signature, a DNS resolver is able to check if the information is identical (correct and complete) to the information on the authoritative DNS server. While protecting IP addresses is the immediate concern for many users, DNSSEC can protect other information such as general-purpose cryptographic certificates stored in CERT records in the DNS.

DNSSEC is intended to protect the end user from DNS protocol attacks. Unfortunately the current DNS is vulnerable to so-called spoofing or poisoning attacks whereby an attacker can fool a cache into accepting false DNS data. Also various man-in-the-middle attacks are possible. The (DNSSEC) is not designed to end these attacks, but to make them detectable by the end user.

IPv6: Internet Protocol version 6 (IPv6) is a version of the Internet Protocol (IP). It is designed to succeed the Internet Protocol version 4 (IPv4). The Internet operates by transferring data between hosts in small packets that are independently routed across IP networks. Each host or computer on the Internet requires an IP address in order to communicate. The growth of the Internet has created a need for more addresses than are possible with IPv4. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with this long-anticipated IPv4 address exhaustion.

Top Level Domain Name: A name used to indicate a country/region or the type of organization using a name. Examples: ".gov", ".mil", ".fedus" are common top level domains reserved for federal US organizations. [Refer to OMB directive on this.]

Second Level Domain Name: Variable-length names registered to an individual or organization for use on the Internet. These names are always based on an appropriate top-level domain, depending on the type of organization or geographic location where a name is used; examples: "www.nist.gov" or "nist.gov".

Sub-Domain Name: Additional names that an organization can create that are derived from (and below) the registered Top-level domain name. These include names added to grow the DNS tree of names in an organization and divide it by functions or into departments, geographic locations, etc.; example: "csrc.nist.gov". Sub-domain names thus include all domain names below the top-level.

Host or Resource Name: Names that represent a leaf in the DNS tree of names and identify a specific resource. Typically, the leftmost label of a DNS domain name identifies a specific computer on the network. For example, if a name at this level is used in a host (A) resource record, it is used to look up the IP address of computer based on its host name. Example - "host-A.csrc.nist.gov", where host-A is a specific computer on the network.