FY 2013

Chief Information Officer

Federal Information Security Management Act

Reporting Metrics

Prepared by:

US Department of Homeland Security

Office of Cybersecurity and Communications

Federal Network Resilience

November 30, 2012

Table of Contents

List of Tables

PURPOSE STATEMENT

This document contains the annual security posture questions for FY13. These questions address areas of risk and are designed to assess the implementation of security capabilities and measure their effectiveness.

GENERAL INSTRUCTIONS

Instructions provided below pertain to the entire document. Individual sections may provide instructions specific to 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 three primary sources and will be marked accordingly. In priority order, the sources are the following:

1. Administration Priorities (AP): These questions are determined by OMB and the National Security Staff and will be scored for the following Performance Areas:
    - Continuous Monitoring:
        - Automated Asset Management
        - Automated Configuration Management
        - Automated Vulnerability Management
    - HSPD-12
    - TIC v2.0 Capabilities
    - TIC Traffic Consolidation

2. Key FISMA Metrics (KFM): These questions are based on the FISMA regulation and will be scored for the following Performance Areas:
    - FedRAMP Authorized CSP Use
    - Privileged User Training
    - Device Discovery Management
    - Remote Access Authentication
    - Remote Access Encryption
    - DNSSEC Implementation
    - Controlled Incident Detection

3. Baseline Questions (Base): These questions are derived from NIST guidelines and will not be scored. The purpose of baseline questions is 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.

The Federal cybersecurity defensive posture is a constantly evolving environment because of the relentless and dynamic threat environment, emerging technologies, and new vulnerabilities. Many threats can be mitigated by following established cybersecurity best practices, but attackers often search for organizations with poor cybersecurity practices and target associated vulnerabilities. The objective of the AP and KFM metrics is to improve the security posture of Federal Departments/Agencies (D/As) in this ever-changing environment.

Reporting Organizations

This document uses the term "organization" to refer to each Federal D/A that is a reporting unit under CyberScope. Often, those organizations must collect and aggregate their response from a number of subordinate organizational "components." The term "network" refers to a network employed by the organization or one of its divisions to provide services and/or conduct other business. These generic terms are used throughout the document with the understanding that each D/A might use other terms to refer to itself, its networks, and its components.

Reporting Responsibilities

Organization heads are responsible for and have full authority to require reporting by lower level organizations that form their enterprise. Lower levels of the organization must report their FISMA metric results to their organization head, who will consolidate the results into one report. For the FY2013 FISMA metrics, a question will be added to CyberScope for organizations to declare which other areas of the organization may have failed to report. This will allow the analysis to account for the percentage of the organization represented by the responses (percentage of organization less than 100).

Terminology and Definitions

This document uses terms such as "adequate," "timely," "complete," and "appropriate." Each organization should interpret these terms in the context of its own determined security and risk acceptance.

Each section includes definitions with interpretations and examples that are specific to the section. Generic definitions of terms are not repeated in each section. Refer to NIST publications for these generic definitions.

Expected Levels of Performance[1]

Administration Priorities: The expected levels of performance for AP FISMA metrics are based on review and input from multiple cybersecurity experts as well as threat information from public, private, and intelligence sources, and they are built to select the highest impact areas for USG-wide application. OMB has set minimum and target levels for the AP metrics for FY2013. See Table 1.

[1] The milestones established in this document are not intended to supersede deadlines set by Presidential Directives, OMB policy, or NIST standards. As requested, DHS will work with organizations to establish milestones as part of their POA&M.

Administration Priority Area	Section	Performance Metric	Minimal Level for 2013	Target Level for 2013
Continuous[2] Monitoring – Assets	2.2	% of assets in 2.1, where an automated capability (device discovery process) provides visibility at the organization's enterprise level into asset inventory information for all hardware assets.	80%	95%
Continuous Monitoring – Configurations	3.1.3	% of the applicable hardware assets (per question 2.1), of each kind of operating system software in 3.1, has an automated capability to identify deviations from the approved configuration baselines identified in 3.1.1 and provide visibility at the organization's enterprise level.		
Continuous Monitoring – Vulnerabilities	4.2	% of hardware assets identified in section 2.1 that are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization's enterprise level.		
Identity Management HSPD-12	5.2.5, 5.4.5, 10.2.5	% of ALL people required to use Personal Identity Verification (PIV) Card to authenticate.	50%	75%
Boundary Protection CNCI[3] #1	7.2	% of external network traffic passing through a Trusted Internet Connection (TIC[4]).	80%	95%
Boundary Protection CNCI #1 & #2	7.1	% of required TIC capabilities implemented by TIC(s) used by the organization.	95%	100%

Table 1 – Administration Priorities Metrics

Key FISMA Metrics: The expected level of performance for these metrics is defined as "adequate security," which means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the organization operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls (OMB Circular A-130, Appendix III, definitions).

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

[3] Comprehensive National Cybersecurity Initiative (CNCI)

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

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

Baseline Questions: These questions establish current performance against which future performance may be measured. There is no expected level of performance for baseline questions. Some baseline questions are also intended to determine whether such future performance measures are needed. Each baseline question is marked as "Base" and will be in the CIO questionnaire. They may be reported to Congress at the discretion of OMB. OIGs should not assume that these questions define any specific organizational performance standard for 2013.

All questions have been established so that organizations can demonstrate improved security over time. New questions are introduced at the Base level unless otherwise directed by OMB.

Scope of Definitions

To clarify the questions, hyperlinks within this document point to operational definitions. These definitions are not intended to conflict with definitions in law, OMB policy, or NIST standards and guidelines, but to add clarity to the terms used in this document.

Reuse of Data

Organizations are encouraged to automate the collection of this information to the extent possible and reuse these reports due to the overlapping of the AP and FISMA requirements with other mandates such as OMB A-130 and Trusted Internet Connection (OMB M-08-05).

Data Aggregation[5] over Organizations and Networks

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

The aggregated number should be the total percentage of the reporting organizations. The following two examples show how to aggregate the numbers for organizations with three reporting components.

Example 1: An Adequate/Inadequate Metric

In this example, the organization has three components. Reporting organization 1 is large with 100,000 computers (or other assets). Reporting organizations 2 and 3 are much smaller with only 10,000 and 1,000 assets respectively. In this example, neither reporting organization 2 nor 3 come close to meeting

[5] 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.

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. See Table 2.

	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
Total	111,000	99,900	11,100
Standard	99,900		

Table 2 – Metric of Network Adequacy

Example 2: A Quantitative Metric

This example uses the same reporting organizations 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[6]. In mathematics, interpolation is defined as: a. the process of determining the value of a function between two points at which it has prescribed values; b. a similar process using more than two points at which the function has prescribed values; c. the process of approximating a given function by using its values at a discrete set of points.

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.

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 organization can interpolate assuming a linear distribution between the data points.

In this example, (the standard) 99,900 is 84%[7] 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[8] days. See Table 3.

[6] For additional information about interpolation and methods, see Wikipedia. If the organization has detailed data on each metric for each instance (in this example each critical patch on each machine, interpolation would not be necessary.

[7] (99,900-80,900)/(103,500-80,900)

[8] = (84% * (30-20))+20

	Size	< 20 days	<30 days[9]	<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
Total	111,000	80,900	103,500	107,000
Standard	99,900			

Table 3 – Quantitative Metric of Speed of Critical Patch Installation

Units of Measure: Many questions ask the organization for **asset[10] counts**, so each section of this document defines the assets to be counted.[11] However, some questions also ask for measures of **frequency and duration** (measured in time). In these cases, time should be treated as a continuous, numeric scale. The questions ask for the response in days, but you may report 8 hours (considered 0.34 days), weeks (7 days), months (30 days), quarters (90 days), or years (365 days). No more than three decimal places in the response will be considered.

In some cases, rolling the reporting organization's frequency and duration into a single number might skew the results. If the majority of reporting organizations provide results that are within 1 to 2 days of each other, report the average of the results. If one reporting organization's results are much larger or smaller than the average of the majority, then report both results (outlier and majority average).

In the context of continuous monitoring, "near-real-time" is defined as within 72 hours. For example, discovery of hardware assets should be automated to occur in near-real-time. An estimated three near-real-time discovery scans should account for 95% of discoverable hardware assets.

NIST SP 800 Revisions: For legacy information systems, D/As are expected to be in compliance with NIST guidelines within one year of the publication date. D/As must become compliant with any new or updated materials in revised NIST guidelines within one year of the revision. For information systems under development or for legacy systems undergoing significant changes, D/As are expected to be in compliance with the NIST publications immediately upon deployment of the information system. Each D/A should consider its ability to meet this requirement when developing the POA&M.

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

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

[10] Assets include objects such as information systems, hardware assets that connect to the network, operating systems, applications, and so on. As illustrated in the links above, we have defined these assets so that they are countable in each applicable section.

[11] 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, results from a recent snapshot are preferred.

1. SYSTEM INVENTORY

Purpose and Use

- 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.

1.1. For each of the FIPS 199 systems' categorized impact levels (H = High, M = Moderate, L = Low) in this question, what is the total number of information systems by organization (i.e., Bureau or Sub-Department Operating Element)? Answer in Table 4. (Organizations with fewer than 5,000 users may report as one unit.)

	1.1.1. Organization-Operated Systems (Base)			1.1.2. Contractor-Operated Systems (Base)			1.1.3. Systems (from 1.1.1 and 1.1.2) with Security ATO (KFM)		
FIPS 199 Category	**H**	**M**	**L**	**H**	**M**	**L**	**H**	**M**	**L**
Reporting Organization 1									
Reporting Organization 2									
[Add rows as needed for organization]									

Table 4 – Responses to Questions 1.1.1–1.1.3

Future Metrics

Expected Areas of Future Expansion for System Inventory

Area of Expansion	Target for Future Inclusion
• It is expected that Federal D/As are already mature in this area and that they maintain adequate maturity while moving from periodic to automated, continuous assessment and authorization.	As soon as FY2014
• Federal D/As are progressing toward automated, continuous assessment and authorization and are better able to respond to emerging threats and weaknesses.[12]	As soon as FY2015

Table 5 – Expected Areas of Future Expansion for System Inventory

Each of these expanded areas would require D/As to know all of the following:

1. total actual system inventory list
2. authorized system inventory list
3. unauthorized system inventory list (the difference between *a* and *b*)
4. ability to authorize systems or remove unauthorized systems in near-real-time (less than 72 hours)

[12] Such weaknesses might include changed configurations, re-installed unapproved software, passwords not reset, training repeatedly missed, and so on.

2. ASSET MANAGEMENT

Purpose and Use

- The Federal CMWG has recommended that asset management is one of the first areas where continuous monitoring needs to be developed. Organizations must first know about devices and software (both authorized/managed and unauthorized/unmanaged) before they can manage the devices/software for configuration and vulnerabilities.
- A key goal of hardware asset management is to identify and remove unmanaged hardware assets/components[13] 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"[14] in near-real-time (less than 72 hours).
- Another goal is to define the universe of assets to which other controls need to be applied. These other controls include software 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.

Hardware Assets/Components

2.1. What is the total number of the organization's hardware assets connected to the organization's unclassified[15] network(s)?[16] (Base)

2.2. What percentage of assets in 2.1 have an automated capability (scans/device discovery processes) to provide enterprise-level visibility into asset inventory information for all hardware assets? (AP)

2.2.1. How often are these automated capabilities (scans/device discovery processes) conducted on all assets connected to the organization's full network(s)? Report the lowest frequency of automated device 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. (KFM)

2.3. For how many assets in 2.1 does the organization have an automated capability to determine both whether the asset is authorized and to whom management has been assigned?[17] (KFM)

[13] Remove or approve/authorize.

[14] "Authorize" here means to assign management ownership, approve for use, and associate with a previously authorized information system.

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

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

[17] The organization is expected to be able to define management of each at a low enough level of detail to be able to effectively assign responsibility and measure performance to ensure adequate security and management.

2.4. For how many assets in 2.1 does the organization have an automated capability to compare assets from 2.2 and 2.3 in order to identify and remove (manually or through NAC, etc.) the unauthorized devices? (Base)

2.4.1. For the assets in 2.4, how much time does it actually take to assign an asset for management (authorize)? (Base)

2.4.2. For the assets in 2.4, how much time does it actually take to remove unauthorized devices, once discovered, with 95% confidence?[18] Report the shortest period in which the removal process is typically completed for all applicable networks. The roll-up of this information is typically the longest time for removal based on all the organization networks, assuming all portions of the organization are using consistent processes. 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 duration, use the comments to explain why, and whether you think this is or is not a valuable metric. (Base)

2.4.3. On how many assets in 2.1 has the organization implemented an automated capability to detect and mitigate unauthorized routes, including routes across air-gapped networks? (Base)

Software Assets

2.5. Can the organization track the installed operating system's vendor, product, version, and patch-level combination(s) in use on the assets in 2.1? If yes, report the number of patch-level combinations. We assume one operating system per device. In the comments, report the number of devices that can boot with multiple operating systems. Note that virtual machines should be counted as assets. (Base)

2.6. 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.[19]) installed on the assets in 2.1? If yes, report the number of general-purpose applications. (Base)

2.7. For what percentage of applicable assets in 2.1 has the organization implemented an automated capability to detect and block unauthorized software from executing, or for what percentage does no such software exist for the device type? This may include software whitelisting tools that identify executable software by a digital fingerprint and selectively block these. It might also

[18] "With 95% confidence" means that in 95% of instances 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 characteristic, we note that a reliable estimate of this number based on an adequate sampling method is sufficient. This metric reflects the timeliness of response, which is important for removing these unmanaged assets from the network (or to get them managed).

[19] Or other software and applications that are regularly the vector of attacks.

include sandboxing of mobile code to determine before execution whether to allow it to run, where static files do not allow whitelisting. In general, any method included should be able to block zero-day and APT threats. (KFM)

Future Metrics and Definitions

Expected Areas of Future Expansion for Asset Management

Area of Expansion	Target for Future Inclusion
• Elevate question 2.5 to a Key FISMA Metric 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 asset discovery (2.1) to more effectively include virtualized and cloud computing assets and capabilities. • Expand whitelisting/blacklisting and automated identification and removal of unauthorized software and hardware.	As soon as FY2014
• Increased fidelity around nontraditional assets such as virtualized and bring-your-own devices (BYOD).	As soon as FY2015

Table 6 – Expected Areas of Future Expansion for Asset Management

Each of these expanded areas would require D/As to have all of the following:

1. total actual inventory list
2. authorized inventory list
3. unauthorized inventory list (the difference between *a* and *b*)
4. ability to remove unauthorized or approve/authorize assets in less than 72 hours (near-real-time)

Definitions for FY2013 Asset Management Section

authorized asset

An asset is authorized when it is approved for use, assigned to a person or group to manage, and associated with a previously authorized information system.

The rationale for this definition is that unauthorized devices are not managed to ensure compliance and may not have been reviewed or approved for use. Therefore they are likely vulnerable and should be removed from the network or identified for review, approval, and addition to managed inventory. (How well authorized devices are managed is reported in other metrics.) Authorizing implies approval at appropriate management levels.

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. 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, it is not an automated capability.

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 executable software with specific digital fingerprints (or comparable verification method) to execute

In other words, the software may be considered unauthorized if it is on a blacklist or not on a whitelist.

This question refers to capability at the device level, not at the network level. If D/As wish to describe capabilities to filter and block malicious code at the network boundary level, they may do so in the applicable comments section.

automated capability to detect hardware assets

Automated detection of hardware assets is also known as "automated device discovery processes." This is defined as any report of actual assets that can be generated by a computer and 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 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 a device outside the designated range (foreign devices) at the level of LAN, MAN, WAN, and so on. Preferably traffic would not be routed to/from such foreign devices.

connected to the organization's unclassified network(s)[20]

This includes mechanical (wired), non-mechanical (wireless), and any other form of connection that allows the electronic flow of information. Exclude the following:

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

- stand-alone devices (not addressable)[21]
- test and/or development networks not connected to the internet and that contain no sensitive information (no information above the low-impact level)
- networks hosting public, non-sensitive websites (no information above the low-impact level) unless access to internal networks can be accomplished by attacking the public website
- classified networks

Assets connected to the network do not include the organization's entire property book. In addition to the items listed above, exclude assets that 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.[22] For cloud services that may be connected only when demanded, the connection should be counted as an operational asset.

Devices connecting remotely and 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,[23] GOCO,[24] or COCO[25] on behalf of the government. The form of ownership and operation is not relevant to inclusion if the network is primarily for government use.

enterprise-wide COTS general-purpose applications

This is any application that is widely installed in the enterprise. For reporting purposes, a threshold of 80% should be used to determine if an application is widely installed.

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." Large organizations with many networks may summarize the response as defined in the footnotes to each question.

[21] This should not be interpreted to exclude devices that are intermittently connected, which should be included.
[22] These are still important to include because they may soon be turned on again.
[23] Government Owned Government Operated
[24] Government Owned Contractor Operated
[25] Contractor Owned Contractor Operated

general-purpose applications(s), enterprise-wide

Applications (COTS, GOTS, custom, etc.) that are typically widely installed on applicable machines (on at least 80% of applicable machines[26]) and that collectively account for at least 90% of installed hardware-asset/software-asset combinations for the organization and/or network.

hardware assets/components

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

- non-portable computers[27]
  - servers
  - workstations (desktops)
- portable computers
  - laptops
  - net-books
  - tablets (iPad, Kindle, other Android)
- mobile devices
  - smartphones (iPhone, Android)
  - cell phones
  - BlackBerry
- networking devices[28]
  - routers
  - switches
  - gateways, bridges, wireless access points (WAPs)
  - firewalls
  - intrusion detection/prevention systems
  - network address translators (NAT devices)
  - hybrids of these types (e.g., NAT router)
  - load balancers
  - modems

[26] "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.

[27] A multi-purpose device need only be counted once. A device with multiple IP connections need only be counted once, not once per connection. This is an inventory of hardware assets, not data.

[28] 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.

- other communication devices
    - encryptors
    - decryptors
    - VPN endpoints[29]
    - medical devices that are part of a patient monitoring network
    - alarms and physical access control devices
    - PKI infrastructure[30]
- 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[31] as if they are a separate physical machine should be counted as separate assets,[32] including dynamic and on-demand virtual environments.
- other devices addressable on the network
- USB devices connected to any device addressable on the network

Both Government Furnished Equipment (GFE) assets and non-GFE assets are included if they meet the other criteria for inclusion listed here.[33] Mobile devices that receive Federal email are considered to be connected. Note: If a non-GFE asset is allowed to connect, it is especially important that it be inventoried, authorized, and correctly configured prior to connection.[34]

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

[30] PKI assets should be included in the network(s) on which they reside. Special methods may be needed to adequately check them for vulnerabilities, compliance, etc. as described in subsequent sections. If this is not done, PKI assets should be included among the assets not covered.

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

[32] Note that VM "devices" generally reside on 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 the 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 providers, please contact FedRAMP for further guidance: http://www.gsa.gov/portal/category/102371.

[33] If a non-GFE asset 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), it does not have to be counted.

[34] If a 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), it does not have to be counted.

Only devices connected to the network(s) of the organization should be reported, and only if they are addressable[35] for network traffic (except USB-connected devices, which are included). We limit this definition to addressable devices because, 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. Connected USB devices are included because they are a source of attacks.

visibility at the organization's enterprise level

The information about hardware assets can be viewed at one of two levels:

- the whole reporting organization
- the lower levels of the organization, as long as they are operated as semi-independent units and are large enough to provide reasonable economies of scale while remaining manageable (Organizations should consult with DHS/FNR on the appropriateness of the definition of lower levels of the organization, if in doubt.)

[35] "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.

3. CONFIGURATION MANAGEMENT

Purpose and Use:

- A key goal of improved configuration management is to make assets harder to exploit.
- 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).
- The configuration management capability needs to
  - be complete—cover enough of the software base to significantly increase the effort required for a successful attack
  - operate in near-real-time (less than 72 hours)—able to find and fix configuration deviations faster than they can be exploited
  - be accurate—have a low enough rate of false positives to avoid unnecessary effort and have a low enough rate of false negatives to avoid unknown weaknesses

3.1. For each operating system vendor, product, version, and patch-level[36] combination referenced in 2.5, report the following:

3.1.1. Has an adequately secure configuration baseline been defined?[37] (KFM)

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

3.1.3. What percentage of the applicable hardware assets (per question 2.1) of each kind of operating system software in 3.1 have an automated capability to identify deviations from the approved configuration baselines identified in 3.1.1 and to provide visibility at the organization's enterprise level? (AP)

3.1.4. What is the frequency of deviation identification (answer in days, per General Instructions)? (Base)

3.2. For each of the enterprise-wide COTS general-purpose applications referenced in question 2.6., report the following:

3.2.1. Has an adequately secure configuration baseline been defined?[38] (KFM)

[36] Knowing version and patch-level is critical to knowing the CVEs these operating systems have, and defining secure configuration baselines and what machines should use those baselines.

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

[38] 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.

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

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

3.2.4. How frequently is the identification of deviations conducted? (Base)

3.3. What percentage of network boundary devices are assessed by an automated capability to ensure that they are adequately configured as intended, such as to adequately protect security? (Base)

Future Metrics and Definitions

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.	As soon as FY2014
• 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 FY2015

Table 7 – Expected Areas of Future Expansion for Configuration Management

Each of these expanded areas would require organizations to know the following:

1. desired configuration checks for common[39] operating systems and applications to provide adequate security
2. actual automated configuration data[40] to match desired configurations
3. unauthorized configurations list (i.e., the difference between *a* and *b*)
4. ability to correct configurations in near-real-time (less than 72 hours) to an acceptable level[41]

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

[40] 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.

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

Definitions for FY2013 Configuration Management Section

applicable hardware assets

Those hardware assets counted in section 2.0 that 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 to retrieve data
- any other reliable and valid method
- some combination of the above

organization approved deviation[42]

This shall be interpreted to include deviations approved for

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

Such deviations should generally be supported by a risk-based analysis,[43] which justifies any increased risk of the deviation based on business needs. The deviation may be approved at any organizational level in accordance with organizational policies and procedures. The approval should come from the system owner and the designated authorizing authority.

[42] 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, CIS, etc.).

[43] 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

Purpose and Use

- Unpatched vulnerabilities are a major attack vector.
- A key goal of vulnerability management is to make assets harder to exploit through mitigation or remediation of vulnerabilities identified in NIST's National Vulnerability Database.
- A key assumption is that vulnerability management covers the universe of applicable assets (defined under asset management). The SCAP standard can support this process.
- The vulnerability management capability needs to be
  - complete—covering enough of the software base to significantly increase the effort required for a successful attack
  - timely—able to find and fix vulnerabilities faster than they can be exploited
  - accurate—has a low enough rate of false positives, to avoid unnecessary effort, and false negatives, to avoid unknown weaknesses

4.1. What percentage of network boundary devices are assessed by an automated capability to ensure that they continue to be adequately free of vulnerabilities? (Base)

4.2. What percentage of hardware assets identified in section 2.1 are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization's enterprise level? (AP)[44]

4.2.1. What percentage of hardware assets identified in 2.1 that were evaluated using tools to assess the security of the systems and that generated output are compliant with each of the following?

4.2.1.1. Common Vulnerabilities and Exposures (CVE) (Base)

4.2.1.2. Common Vulnerability Scoring System (CVSS) (Base)

4.2.1.3. Open Vulnerability and Assessment Language (OVAL) (Base)

4.3. For what percentage of information systems does the organization do the following (see Table 8)?[45] (Base)

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

[45] The presence of this question about identifying weaknesses in non-COTS software does not require any organization to use the tools described in section 4.1, as long as some effective method is used to adequately find and remove common weaknesses like register overflow and SQL injection and prevent common attack patterns from compromising software.

		For systems in development and/or maintenance:		For systems in production:	
		Use methods described in Table 9 to identify and fix instances of common weaknesses, prior to placing that version of the code into production.	Can the organization 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 the organization find SCAP compliant tools and good SCAP content?
Impact Level	High				
	Moderate				
	Low				

Table 8 – Responses to Question 4.3

Identify Universe Enumeration	Find Instances Tools and Languages	Assess Importance
• 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.	—

Table 9 – Methods to Identify and Fix Instances of Common Weaknesses

See guidance that 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.

Future Metrics and Definitions

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 timely manner to provide adequate security. • Evaluate software weakness and vulnerabilities through software assurance metrics.	As soon as FY2014
• 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 FY2015

Table 10 – Expected Areas of Future Expansion for Vulnerability and Weakness Management

Each of these sections would require organizations to know potential vulnerabilities from NVD for installed[46] operating systems and applications, weaknesses from CWE and CAPEC analysis to provide adequate security, and actual vulnerability/weakness data[47] to reduce vulnerabilities and weaknesses in near-real-time (less than 72 hours) to an acceptable level.[48]

Definitions for FY2013 Vulnerability and Weakness Management Section

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

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

[47] Because of limits to the ability to conduct automated checks, this may 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 when they are not necessary.

[48] An acceptable level does not mean zero vulnerability, but rather that the worst vulnerabilities are fixed in near-real-time and that the remainder represents an acceptable risk, as determined by the organization's risk-based analysis.

5. IDENTITY AND ACCESS MANAGEMENT

Purpose and Use

- HSPD-12/PIV is an Administration Priority.
- OMB has 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 given only to the intended individuals and/or processes.[49]
- The Identity and Access Management capability needs to be
  - complete—covering all accounts
  - timely—able to find and remove stale or compromised accounts faster than they can be exploited
  - accurate—has a low enough rate of false positives, to avoid unnecessary effort, and false negatives, to avoid unknown weaknesses

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

[49] This is done by establishing a process to assign attributes to a digital identity and by connecting an individual to that identity; but this would be pointless if it were not subsequently used to control access.

5.2. What percentage of people with an *unprivileged* network account can log onto the network in each of the following ways? See Table 11.

Metric	Percentage[50]	Comments
5.2.1. Allowed to log on with user ID and password. (Base)		Measures the percentage of people who are allowed to use user ID and password as their normal mode of authentication. • Percentage should measure people because a person may have multiple accounts. • For a person with more than one unprivileged network account, the person should be counted in the percentage if the person is permitted to use user ID and password to log onto any account.
5.2.2. Allowed, but not required, to log on with a non-PIV form of two-factor authentication. (Base)		Measures the percentage of people whose accounts have been enabled to allow logon using a non-PIV form of two-factor authentication. • Percentage may include an account that allows both non-PIV, two-factor authentication and an alternative authentication mechanism (such as user ID and password). • Percentage should measure people because a person may have multiple accounts. • For a person with more than one unprivileged network account, the person should be counted in the percentage if the person is permitted to use a non-PIV form of two-factor authentication to log onto any account.
5.2.3. Allowed, but not required, to log on with a two-factor PIV card. (Base)		Measures the percentage of people whose accounts have been enabled to allow logon using a two-factor PIV card. • Percentage may include an account that allows both PIV and an alternative authentication mechanism (such as user ID and password). • Percentage should measure people because a person may have multiple accounts. • For a person with more than one unprivileged network account, the person should be counted in the percentage if the person is permitted to use a two-factor PIV card to log onto any account.

[50] Each row should be assessed independently; the percentages are not expected to sum to 100%.

Metric	Percentage[50]	Comments
5.2.4. Required to log on with a non-PIV form of two-factor authentication. (Base)		Measures the percentage of people who are required to log on using a non-PIV form of two-factor authentication as the normal mode of authentication. • Percentage should measure people because a person may have multiple accounts. • For a person with more than one unprivileged network account, the person should be counted in the percentage only if the person is required to use two-factor authentication for all accounts.[51]
5.2.5. Required to log on with a two-factor PIV card. (AP)		Measures the percentage of people who are required to log on using a two-factor PIV card as the normal mode of authentication. Question 5.2.5 is inclusive of anyone counted in 5.2.6. • Percentage should include people currently using temporary credentials if the person's normal mode of authentication is PIV-enforced. • Percentage should measure people because a person may have multiple accounts. • For a person with more than one unprivileged network account, the person should be counted in the percentage only if the person is required to use a two-factor PIV card to authenticate to all accounts.
5.2.6. Required to conduct PIV authentication at the user-account level. (KFM)[52]		Measures the percentage of people for whom only the PIV card can be used to log onto the person's account. • Percentage should measure people because a person may have multiple accounts. • For a person with more than one unprivileged network account, the person should be counted in the percentage only if two-factor PIV card authentication is enforced at the user-account level for all accounts.

Table 11 – Responses to Questions 5.2.1–5.2.6

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

[51] Organizations are expected to transition all network access to two-factor PIV card authentication; therefore, this metric should not be construed as requiring implementation of alternative non-PIV forms of two-factor authentication. During the transition to two-factor PIV card authentication, this metric is expected to include people who are required to use PIV card authentication on some accounts and non-PIV two-factor authentication on other accounts who have not yet been transitioned or cannot be transitioned to PIV card authentication due to the technical limitations of the implementation.

[52] This metric is operating-system specific and is intended to assess a specific implementation method. It may not apply to all operating system platforms.

5.4. What percentage of people with a *privileged* network account can log onto the network in each of the following ways? See Table 12.

Metric	Percentage[53]	Comments
5.4.1. Allowed to log on with user ID and password. (Base)		Measures the percentage of people who are allowed to use user ID and password as their normal mode of authentication. • Percentage should measure people because a person may have multiple accounts. • For a person with more than one privileged network account, the person should be counted in the percentage if the person is permitted to use user ID and password to log onto any account.
5.4.2. Allowed, but not required, to log on with a non-PIV form of two-factor authentication. (Base)		Measures the percentage of people whose accounts have been enabled to allow logon using a non-PIV form of two-factor authentication. • Percentage may include an account that allows both non-PIV two-factor authentication and an alternative authentication mechanism (such as user ID and password). • Percentage should measure people because a person may have multiple accounts. • For a person with more than one privileged network account, the person should be counted in the percentage if the person is permitted to use a non-PIV form of two-factor authentication to log onto any account.
5.4.3. Allowed, but not required, to log on with a two-factor PIV card. (Base)		Measures the percentage of people whose accounts have been enabled to allow logon using a two-factor PIV card. • Percentage may include an account that allows both PIV and an alternative authentication mechanism (such as user ID and password). • Percentage should measure people because a person may have multiple accounts. • For a person with more than one privileged network account, the person should be counted in the percentage if the person is permitted to use a two-factor PIV card to log onto any account.

[53] Each row should be assessed independently; the percentages are not expected to sum to 100%.

Metric	Percentage[53]	Comments
5.4.4. Required to log on with a non-PIV form of two-factor authentication. (Base)		Measures the percentage of people who are required to log on using a non-PIV form of two-factor authentication as the normal mode of authentication. • Percentage should measure people because a person may have multiple accounts. • For a person with more than one privileged network account, the person should be counted in the percentage only if the person is required to use two-factor authentication for all accounts.[54]
5.4.5. Required to log on with a two-factor PIV card. (AP)		Measures the percentage of people who are required to log on using a two-factor PIV card as the normal mode of authentication. Question 5.4.5 is inclusive of anyone counted in 5.4.6. • Percentage should include people currently using temporary credentials if the person's normal mode of authentication is PIV-enforced. • Percentage should measure people because a person may have multiple accounts. • For a person with more than one privileged network account, the person should be counted in the percentage only if the person is required to use a two-factor PIV card to authenticate to all accounts.
5.4.6. Required to conduct PIV authentication at the user-account level. (KFM)[55]		Measures the percentage of people for whom only the PIV card can be used to log onto the person's account. • Percentage should measure people because a person may have multiple accounts. • For a person with more than one privileged network account, the person should be counted in the percentage only if two-factor PIV card authentication is enforced at the user-account level for all accounts.

Table 12 – Responses to Questions 5.4.1–5.4.6

[54] Organizations are expected to transition all network access to two-factor PIV card authentication; therefore, this metric should not be construed as requiring implementation of alternative non-PIV forms of two-factor authentication. During the transition to two-factor PIV card authentication, this metric is expected to include people who are required to use PIV card authentication on some accounts and non-PIV two-factor authentication on other accounts who have not yet been transitioned or cannot be transitioned to PIV card authentication due to the technical limitations of the implementation.

[55] This metric is operating-system specific and is intended for a specific implementation. It may not be applicable to all operating system platforms. Organizations are not required or expected to adopt the authentication method described in the metric, organizations that record 0% in this column will not be penalized.

5.5. What is the estimated number of organization internal systems?[56] (Base)

5.6. What percentage of the organizations internal systems are configured for authentication in each of the following ways? See Table 13.

Metric	Percentage	Comments
5.6.1. Allows user ID and password. (Base)		Measures the percentage of the organizations systems that are configured to allow users to use user ID and password for authentication. If a system allows any user(s) to use user ID and password as the normal mode of access, then it would be included in the metric.
5.6.2. Allows, but does not enforce, non-PIV, two-factor authentication for users. (Base)		Measures the percentage of the organizations systems that are configured to allow users to use a non-PIV form of two-factor authentication. A system should be counted in the metric if it allows any user to use a non-PIV form of two-factor authentication as the normal mode of access.
5.6.3. Allows, but does not enforce, two-factor PIV card authentication for users. (Base)		Measures the percentage of the organizations systems that are configured to allow users to use a two-factor PIV card for authentication. A system should be counted in the metric if it allows any user to use a two-factor PIV card as the normal mode of access.
5.6.4. Enforces non-PIV, two-factor authentication for all users. (Base)		Measures the percentage of the organizations systems that are configured to require use of a non-PIV form of two-factor authentication.
5.6.5. Enforces two-factor PIV card for all users. (Base)		Measures the percentage of the organizations systems that are configured to require use of a two-factor PIV card for authentication. A system should be counted only if it is configured to enforce two-factor PIV card authentication for all users.

Table 13 – Responses to Questions 5.6.1–5.6.5

5.7. Does the organization have a policy in place that requires the review of privileged network users' privileges? (If the answer is no, then skip questions 5.7.1 through 5.7.2.)

5.7.1. What percentage of privileged network users[57] had their privileges reviewed this year for the following?

[56] Internal systems include those that are accessed by internal organization users, defined for the purpose of this question as Federal employees, contractors, and affiliates, covered under the scope of HSPD-12.

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

5.7.1.1. Privileges on that account reconciled with work requirements. (Base)

5.7.1.2. Adequate separation of duties considering aggregated privileges on all accounts for the same person (user). (Base)

5.7.2. What percentage of privileged network users had their privileges adjusted or terminated after being reviewed this year? (Base)

5.8. What percentage of the organizations systems that have intergovernmental users enforce two-factor PIV card authentication for all users? (Organizations with no intergovernmental systems may respond with N/A.) (Base)

5.9. Does your organization's Federal Identity, Credential, and Access Management (FICAM) implementation plan include an enterprise Identity and Access Management approach[58] that system owners can leverage to adopt PIV enablement? (Base)

Future Metrics and Definitions

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 FY2014
• Add network account asset inventory parallel to the hardware asset inventory.	As soon as FY2015

Table 14 – Expected Areas of Future Expansion for Identity and Access Management

Each of these expanded areas would require D/As to

1. know the desired state of the identity and access protections to provide adequate security,[59]
2. know the actual state of the identity and access protections,
3. identify and prioritize the differences between *a* and *b*, and
4. correct differences in a prioritized manner and in near-real-time (less than 72 hours), to an acceptable level.[60]

[58] Per the FICAM Roadmap and Implementation Guidance, Version 2.0, an enterprise logical access management approach may be achieved using one or more systems.

[59] See definitions for the Identity and Access Management section.

[60] 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 FY2013 Identity and Access Management Section

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 account

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

network accounts with elevated privileges

A network account that provides access to powers and data within the system/application that are significantly greater than those available to the majority of accounts. Also known as "privileged network user accounts." Such greater powers include, but are not limited to, the ability to

- view/copy/modify/delete sensitive system meta-information[61] and/or network resources
- change the access rights to network resources

At a low level of privilege, the 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 because the account has more privileges.

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, because they are non-user accounts, and local workstation administrators, because they are not network accounts.

network accounts without elevated privileges

Any network account that is not a network account with elevated privileges. Also known as "unprivileged network accounts."

non-user account

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

[61] 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, who have broad rights to view/copy/modify/delete the transactions of multiple other users.

management of the person (or group) that owns the account[62] 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.[63]

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 (for example; an RSA key 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 count only 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.[64]

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

An account that is intended to be controlled directly by a particular person to perform work. The person presents their credential to gain access. User accounts include temporary, guest, and generic student accounts.

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, so this is considered to be one-factor authentication.

[62] For example, this includes machine accounts and operating system built-in accounts. More generally, it includes "service" accounts.
[63] 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.
[64] http://www.yourwindow.to/information-security/gl_privilegeduser.htm

6. DATA PROTECTION

Purpose and Use

- Mobile devices and unencrypted email are primary sources 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 organization's networks. The use of encryption of data at rest or in motion is vital to protect that data's confidentiality and integrity.

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

6.1. What is the estimated number of hardware assets from 2.1 in each of the following mobile asset types, and how many are encrypted? Answer in Table 15. (KFM)

Mobile Asset 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 encryption of data on the device.**[65]
Laptop computers and netbooks		
Tablet-type computers		
BlackBerries and other smartphones		
Other cellular devices		
USB-connected devices (e.g., flash drives and removable hard drives)		
Other mobile hardware assets (describe types in comments field)		

Table 15 – Responses to Question 6.1

6.2. What percentage of the organization's email traffic is on systems that implement FIPS 140-2[66] compliant encryption technologies, such as S/MIME, PGP, OpenPGP, or PKI, when sending messages to government organizations? (KFM)

6.2.1. What percentage of inter-organization email traffic is on systems that implement FIPS 140-2 compliant encryption technologies, such as S/MIME, PGP, OpenPGP, or PKI, when sending messages to the public? (KFM)

[65] The numbers in column *b* cannot be larger than the numbers in column *a*.

[66] Per FIPS 201, this means both digital signing and digital encryption.

6.3. Which one of the following best describes the organization's PKI Certificate Authority? Respond with the letter of that option. (Base) The organization

a. self-manages a legacy PKI certificate authority (which is not a Federal Shared Service Provider)
b. is a Federal Shared PKI Service Provider
c. receives PKI support from a Federal or commercial Shared Service Provider, but is responsible for some portion of the PKI service
d. Has another source of PKI Certificate Authority

Future Metrics and Definitions

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 16 – Expected Areas of Future Expansion for Data Protection

Definitions for FY2013 Data Protection Section

encryption
All user data is 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, count it as adequately encrypted.

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

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

estimated total number[67]
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 year-to-year progress 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 from year to year because of the inability to count these assets, then this should be indicated in the comments.

flash drives
A solid-state drive (SSD), sometimes called a solid-state disk or electronic disk. An SSD 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 may be plugged directly into devices like smartphones. In either case, flash drives 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 small, lightweight, and inexpensive laptop computer. Netbooks typically lack an internal CD/DVD drive, legacy ports, an ISA bus, or sometimes any internal expansion bus at all.

PGP and OpenPGP
A data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. Pretty Good Privacy (PGP) is often used for signing, encrypting, and decrypting texts, emails, 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 email or other transport protocols.

[67] 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.

public key infrastructure (PKI)
A 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 that are usually connected to the computer through USB ports, reside externally to the computer, and allow easy removal and connection to other computers. This category could also include similar drives connected directly to the network that 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, and 3851. S/MIME functionality is built into the majority of modern email software and interoperates between them.

tablet computers
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 and mouse. Tablets often use an onscreen virtual keyboard, a passive stylus pen, or a digital pen.

7. BOUNDARY PROTECTION

Purpose and Use

- A key goal of boundary protection is to make assets harder for outsiders to exploit by keeping outsiders outside the network perimeter.
- Trusted Internet Connection (TIC) is an Administration Priority, and the Federal Continuous Monitoring Working Group (CMWG) has recommended that it is among the areas where continuous monitoring needs to be developed.
- Boundary email protection is needed to reduce the number of phishing attacks, which currently represent a high-risk threat.
- Monitoring for unapproved wireless networks that can bypass boundary security devices must be included.
- A key assumption is that boundary protection is centrally managed by an organization and covers all hardware assets (defined under Asset Management).
- A key threat is creation of unapproved holes in the boundary, making it critical to establish uniform, standardized, and tested processes for exceptions and to audit frequently for unauthorized changes.
- A capable boundary protection program
    - covers all avenues of access to/from the network
    - is able to find and fix attacks and intrusions faster than they can be completed
    - has a low enough rate of false positives to avoid unnecessary effort and has a low enough rate of false negatives to avoid unknown weaknesses

Instruction: Question 7.1 applies only to Federal Civilian TIC Access Providers (TICAPs). If the reporting organization is not (a) a Federal civilian organization and/or (b) not a TIC access provider, answer N/A to these questions.

7.1. What percentage of the required TIC 2.0 Capabilities are implemented? (AP)

Instruction: Questions 7.2–7.3 apply only to Federal civilian organizations. If the reporting organization is not a Federal civilian organization, answer N/A to these questions.

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

7.3. What percentage of external network/application interconnections to/from the organization's networks passes through a TIC/MTIPS? (KFM)

Instruction: The remaining questions apply to all reporting organizations.

7.4. What percentage of organization email systems implement sender verification (anti-spoofing) technologies when sending messages? (KFM)

7.5. What percentage of organization email systems use sender verification (anti-spoofing) technologies to detect possibly forged messages from outside the network? (Base)

7.6. What is the estimated percentage of incoming email traffic (measured in messages) whose links or attachments are executed or opened in an in-line sandbox or virtual environment to ascertain whether or not they are malicious, and quarantined as appropriate, before they can be opened by the recipient? (Note: If you consider this to be infeasible, please explain why in the comments.) (KFM)

7.7. With what frequency does the organization conduct scheduled scans for unauthorized wireless access points (WAP) connected to an organizational network? Scans of different areas may count as different scans. A scan does not need to cover a particular percentage of the organization to be counted. (Base)

7.7.1. What percentage of hardware assets in 2.1 are in facilities where scheduled WAP scans are conducted? (Base)

7.7.2. How many WAPs were found? (Base)

7.8. With what frequency does the organization conduct planned, unannounced scans for unauthorized WAPs? Scans of different areas may count as different scans. A scan does not need to cover a substantial portion of the organization or assets to be counted. (Base)

7.8.1. What percentage of hardware assets in 2.1 are in facilities where planned, unannounced WAP scans are conducted?

7.8.2. How many WAPs were found? (Base)

7.9. How many devices in 2.1, with DLP/DRM (Digital Loss Protection/Digital Rights Management), does the organization have at the gateway to capture outbound data leakage (e.g., PII)? (Base)

7.10. Is the organization’s internet service (whether obtained through a TICAP or other means) configured to manage filters, excess capacity, bandwidth, or provide other redundancies to limit the effects of information-flooding types of denial-of-service attacks on the organization’s internal networks and internet services. Such configuration may include agreements with external network operators to reduce the susceptibility to these types of attacks and respond to them. (Base)

Future Metrics and Definitions

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 DLP/DRM at the gateway for content inspection	As soon as FY2014
• Timeliness of monitoring and response • Adequate coverage of monitoring and response for all assets, as applicable	As soon as FY2015

Table 17 – Expected Areas of Future Expansion for Boundary Protection

Each of these expanded areas would require D/As to

1. know the desired state of the boundary protections to provide adequate security,
2. know the actual state of the boundary protections,
3. identify and prioritize the differences between *a* and *b*, and
4. correct differences in a prioritized manner and in near-real-time (less than 72 hours), to an acceptable level.[68]

Definitions for FY2013 Boundary Protection Section

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 creates significant risk.

email systems
Organizational software such as Outlook Exchange or Gmail that provides email accounts that enable people to exchange digital messages.

[68] An acceptable level does not mean zero differences, but rather that the differences that would have the greatest negative impact are addressed in near-real-time and that the remainder represents an acceptable risk, as determined by the organization's risk-based analysis.

network boundary devices
Devices that are part of the cyber perimeter.

scheduled scans
Scans (or other automated capabilities) in which the person managing the devices to be scanned knows when to expect the scan, allowing the person to prepare for it.

sender verification (anti-spoofing) technologies
These include

- Domain Keys Identified Mail (DKIM)
- Sender Policy Framework (SPF)
- digital signing of email using PKI
- other technologies able to prevent spoofing (described in the comments)

TIC 2.0 capabilities
A body of 60 critical capabilities that were collaboratively developed to improve upon the baseline security requirements in TIC Reference Architecture V2.0. These are available on OMB's MAX Portal.

TIC/MTIPS (trusted internet connections/managed trusted internet protocol services)
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, so they provide a more accurate view of the hardware assets.

virtual environment
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

Purpose and Use:

- Given real-world reports, 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 have been successful.
- Organizations can 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.

8.1. How many of the organization's hardware assets from 2.1 are on networks on which controlled network penetration testing was performed in the reporting period?[69] (KFM)

8.1.1. What percentage of applicable events was detected by NOC/SOC during the penetration test? (KFM)

8.1.2. What percentage of applicable events was detected by NOC/SOC during the other scans or tests? (Base)

8.1.3. What was the mean time to detection of applicable events? (KFM)

[69] Section 8.1 applies 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.

Future Metrics and Definitions

Expected Areas of Future Expansion for Incident Management

Area of Expansion	Target for Future Inclusion
• Increase levels of detection in shorter periods of time. • Increase percentage of incidents "tipped"[70] via o DHS-US-CERT/Einstein o internal threat analysis o intelligence threat analysis o public threat analysis o other threat analysis • Percentage of events/incidents that are detected by organization SOC versus reported by system-level users/administrators o Identify the number of SOC-detected events/incidents that are malicious logic. • The number of events/incidents related to known vulnerabilities	As soon as FY2014
• Metrics related to effective and timely remediation of such applicable events	As soon as FY2015

Table 18 – Expected Areas of Future Expansion for Incident Management

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

Definitions for FY2013 Incident Management Section

applicable events

During a penetration test, events that would be expected to be detected. Detecting these events would demonstrate an adequate level of security[71] on the network.

controlled penetration testing

Penetration testing may be sponsored by the organization or by lower levels of the organization and conducted on a controlled portion of the networks or systems. The purpose of this test is to determine (a) available means of attack and (b) whether the network defenders (typically the NOC/SOC) detect the attack. Ideally a controlled penetration test would be known to managers but unannounced to front-line operators.

[70] Detection of a signature or other symptom that indicates a possible incident.

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

event
In penetration testing, an incident-like action created by the penetration test team. Technically, events not incidents because they were approved by the AO (or other appropriate authority) as part of the test plan. They 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).

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

network penetration testing
Penetration testing performed on the organization's network.

penetration testing
A testing methodology in which assessors attempt to circumvent or defeat the security features of an information system or network. Generally, the assessors work under specific guidelines that prevent the test from compromising mission performance.

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.

9. TRAINING AND EDUCATION

Purpose and Use

- Some of the most effective current attacks on cyber networks world-wide exploit 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. 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 behaviors, which affect cybersecurity.
- The metrics will be used to assess the extent to which organizations are providing adequate training to address these attacks and threats.[72]

The introduction of the OPM EHRI[73] data elements for cybersecurity personnel will aid in the identification of those professionals available to broaden the pool of skilled and educated workers capable of supporting a cyber-secure nation.[74]

Note: In Section 5, you were asked to provide the number of unprivileged and privileged network users. Section 9 assumes that these users represent the universe of all users for the organization who thus need training. If this is not the case, please explain in the comment section to question 9.1.

9.1. What percentage of the organization's network users have been given and successfully completed cybersecurity awareness training in FY2012 (at least annually)? (KFM)

9.1.1. What is the estimated percentage of new users who satisfactorily completed security awareness training before being granted network access, or completed security awareness training within an organizationally defined time limit that provides adequate security after being granted access? (KFM)

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

[72] 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 it faces.

[73] http://www.opm.gov/egov/e-gov/EHRI/

[74] The National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework is available at www.nist.gov/nice/framework.

9.2.1. What was the average frequency in days of content provisions? See General Instructions. (Base)

9.2.2. What percentage of this additional content that addresses emerging threats were not previously covered[75] in the annual training? (Base)

9.2.3. What is the total number of organization-sponsored exercises (focusing on emerging threats such as phishing) designed to increase cybersecurity awareness and/or measure the effectiveness of cybersecurity awareness training in molding behavior? (Base)

9.2.4. What percentage of exercises in 9.2.3 suffered no problems or suffered problems that were addressed through appropriate training within three months? (Base)

9.3. How many of the organizations network users and other staff[76] have significant security responsibilities? (Base)

9.3.1. What is the organization's standard for the longest acceptable amount of time between security training events for the personnel counted in question 9.3? (KFM)

9.3.2. How many of the personnel counted in question 9.3 have taken security training within the organizational standard defined in 9.3.1? (Base)

[75] If training is conducted periodically throughout the year, then "not previously covered" means what percentage of the content was added or strengthened during the year.

[76] "Other staff" means non-network users who may still have a significant impact on security. This group might include senior executives who do not use the network themselves but affect factors such as budget, staffing, and priorities. The size of this group is expected to be small.

Future Metrics and Definitions

Expected Areas of Future Expansion for Training and Education

Area of Expansion	Target for Future Inclusion
• *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 Federally defined common roles. Organizations have adapted the National Cybersecurity Workforce Framework to provide clear guidance on organization-specific cybersecurity functions that fit this category and the common behaviors that should be addressed in training.	As soon as FY2014
In addition to the goals for 2014: • *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 federally defined common roles and organization-specific cybersecurity functions. The organization has some mechanism to test the effectiveness of some role-based training through exercises and/or other means.	As soon as FY2015

Table 19 – Expected Areas of Future Expansion for Training and Education

Successful performance in this area would require the organization to

1. know the total inventory of persons needing training and the content of training needed based on each person's role,
2. know the actual training provided and the user's performance result (usually test results),
3. know the difference between *a* and *b*, and
4. have a process to address the differences by providing training or removing access rights and responsibilities.

Definitions for FY2013 Training and Education Section

emerging threat exercises

These exercises include (a) simulated threats where the user is not aware that the event is an exercise (user-blind exercise) and (b) practice exercises where the user knows that the event is an exercise (non-blind exercise, much like an announced fire drill). Often, blind exercises are more effective if the person's behavior is not recorded but if 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

given and successfully completed cybersecurity awareness training

For situations that are likely[77] to confront unprivileged network users, the user has received training that gives them the ability to

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

Successful completion means (at a minimum) that the user has passed a test on the content. Preferably, it means that the user's behavior and judgment is measurably 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.

network user

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.

national cybersecurity workforce framework

Cybersecurity professionals, regardless of job title, in their daily actions perform certain functions. These functions have been distilled into specialty areas noted in the National Cybersecurity Workforce Framework (www.nist.gov/nice/framework). Organizations are tasked by OPM to update the OPM EHRI data warehouse with the appropriate codes for Federal cybersecurity personnel.

significant security responsibilities

Also known as "special cybersecurity roles and responsibilities," a network user's role and/or responsibility for which cybersecurity awareness training, by itself, fails to describe all the behaviors the user needs to adequately protect cybersecurity. Those with significant security responsibilities include all users who have one or more privileged network user account and all other users who have managerial or operational responsibilities that allow them to increase or decrease cybersecurity.

[77] "Likely" is used here to indicate that organizations should use risk-based analysis to decide what behaviors should be covered in this awareness 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 organizational experience, threats, and countermeasures.

significant security responsibility training

Training that gives privileged network users, and others whose role materially and substantially affect cybersecurity, the ability to

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

Significant security responsibility training covers situations beyond those covered in cybersecurity awareness training. Note that such training may be provided as (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.

10. REMOTE ACCESS

Purpose and Use

- 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.
- Remote connections allow users to access the network without gaining physical access to organization's facility and the computers hosted there. However, 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.

This section applies to remote access solutions that protect access to the organization's desktop LAN/WAN resources and services. Remote access excludes externally facing applications (e.g., OWA). For application access, please see question 5.6.

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

10.2. For remote access, what percentage of people can log onto the organization's desktop LAN/WAN resources or services in each of the following ways? See Table 20.

Metric	Percentage[78]	Comments
10.2.1. Allowed to log on with user ID and password. (Base)		Measures the percentage of people who are allowed to use user ID and password as their normal mode of authentication for remote access. • Percentage should measure people because a person may have multiple accounts. • People with more than one account should be counted in the percentage if they are permitted to use user ID and password to log onto any account.

[78] Each row should be assessed independently; the percentages are not expected to sum to 100%.

Metric	Percentage[78]	Comments
10.2.2. Allowed, but not required, to log on with a non-PIV form of two-factor authentication. (Base)		Measures the percentage of people who are allowed to log on using a non-PIV form of two-factor authentication for remote access. • Percentage may include an account that allows both non-PIV two-factor authentication and an alternative authentication mechanism (such as user ID and password). • Percentage should measure people because a person may have multiple accounts. • People with more than one account should be counted in the percentage if they are permitted to use a non-PIV form of two-factor authentication to log onto any account.
10.2.3. Allowed, but not required, to log on with a two-factor PIV card. (Base)		Measures the percentage of people who are allowed to log on using a two-factor PIV card for remote access. • Percentage may include an account that allows both PIV and an alternative authentication mechanism (such as user ID and password). • Percentage should measure people because a person may have multiple accounts. • People with more than one account should be counted in the percentage if they are permitted to use a two-factor PIV card to log onto any account.
10.2.4. Required to log on with a non-PIV form of two-factor authentication. (Base)		Measures the percentage of people who are required to log on using a non-PIV form of two-factor authentication as the normal mode of authentication for remote access. • Percentage should measure people because a person may have multiple accounts. • People with more than one account should be counted in the percentage only if they are required to use two-factor authentication for all accounts.[79]

[79] Organizations are expected to transition all network access to two-factor PIV card authentication; therefore, this metric should not be construed as requiring implementation of alternative non-PIV forms of two-factor authentication. During the transition to two-factor PIV card authentication, this metric is expected to include people who are required to use PIV card authentication on some accounts and non-PIV two-factor authentication on other accounts that have not yet been transitioned or cannot be transitioned to PIV card authentication due to the technical limitations of the implementation.

Metric	Percentage[78]	Comments
10.2.5. Required to log on with a two-factor PIV card. (AP)		Measures the percentage of people who are required to log on using a two-factor PIV card as the normal mode of authentication for remote access. Question 10.2.5 is inclusive of anyone counted in 10.2.6. • Percentage should include people currently using temporary credentials if the person's normal mode of authentication is PIV-enforced. • Percentage should measure people because a person may have multiple accounts. • People with more than one account should be counted in the percentage only if they are required to use a two-factor PIV card to authenticate to all accounts.
10.2.6. Required to conduct PIV authentication at the user-account level. (KFM)[80]		Measures the percentage of people for whom only the PIV card can be used to log onto the person's account for remote access. • Percentage should measure people because a person may have multiple accounts. • People with more than one account should be counted in the percentage only if two-factor PIV card authentication is enforced at the user-account level for all their accounts.

Table 20 – Responses to Questions 10.2.1–10.2.6

10.3. What is the estimated percentage of remote access connections that have each of the following properties?

10.3.1. Utilizes FIPS 140-2-validated cryptographic modules. (KFM)

10.3.2. Prohibits split tunneling and/or dual-connected remote hosts where the laptop has two active connections. (KFM)

10.3.3. Configured in accordance with OMB M-07-16 to time-out after 30 minutes of inactivity (or less) and require re-authentication to reestablish session. (KFM)

10.3.4. Scans for malware upon connection. (KFM)

[80] This metric is operating-system specific and is intended to assess a specific implementation method. It may not apply to all operating system platforms.

10.4. How many of the organizations systems are internet-accessible and are accessed by the organizations users?[81] This excludes systems accessed through the remote access solutions covered in 10.1 and 10.2. (Base)

10.5. What percentage of organizations systems that are internet-accessible and are accessed by the D/A's users are configured for authentication in each of the following ways? See Table 21.

Metric	Percentage	Comments
10.5.1. Allows user ID and password. (Base)		Measures the percentage of internet-accessible organization systems that are configured to allow users to use user ID and password for authentication. Systems that allow any user(s) to use user ID and password as the normal mode of access should be counted.
10.5.2. Allows, but does not enforce, non-PIV two-factor authentication for users. (Base)		Measures the percentage of internet-accessible organization systems that are configured to allow users to use a non-PIV form of two-factor authentication. Systems that allow any user(s) to use a non-PIV form of two-factor authentication as the normal mode of access should be counted.
10.5.3. Allows, but does not enforce, two-factor PIV card for users. (Base)		Measures the percentage of internet-accessible organization systems that are configured to allow users to use a two-factor PIV card for authentication. Systems that allow any user(s) to use a two-factor PIV card as the normal mode of access should be counted.
10.5.4. Enforces non-PIV two-factor authentication for all users. (Base)		Measures the percentage of internet-accessible organization systems that are configured to require users to use a non-PIV form of two-factor authentication.
10.5.5. Enforces two-factor PIV card for all users. (Base)		Measures the percentage of internet-accessible organization systems that are configured to require users to use a two-factor PIV card for authentication. Only systems configured to enforce two-factor PIV card authentication for all users should be counted.

Table 21 – Responses to Questions 10.5.1–10.5.5

[81] Defined for the purpose of this question as the organizations Federal employees, contractors, and affiliates covered under the scope of HSPD-12.

Future Metrics and Definitions Expected Areas of Future Expansion for Remote Access

Area of Expansion	Target for Future Inclusion
• Controls to protect against weaknesses in non-GFE devices that may be allowed to connect to the network (i.e., BYOD) • Controls to protect against weaknesses in an increasing number of mobile and wireless devices • Protection of email servers from being used as relay hosts	As soon as FY2014

Table 22 – Expected Areas of Future Expansion for Remote Access

Successful performance in this area would require the organization to know all of the following:

1. the total inventory of remote connection methods and their desired security posture
2. the actual remote connection methods and their actual security posture
3. the difference between *a* and *b*
4. ability to address the differences by removing unauthorized access methods and correcting defects in the remote access method

Definitions for FY2013 Remote Access Section

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 situation where the host is connected to more than one network. The connections may be wired or wireless. One 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 organization should know the number of connections with sufficient accuracy to be able to measure progress from year to year. Thus, 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 is a Federal Information Processing Standard that specifies the security requirements satisfied by a cryptographic module utilized within a system. While many vendors claim their cryptographic modules are FIPS 140-2 compliant, only those currently validated as compliant can be reliably counted in this report. (Validation is provided through independent laboratories via the

Cryptographic Module Validation Process managed by NIST. See http://csrc.nist.gov/groups/STM/cmvp/index.html for more information on this process and a listing of validated cryptographic modules.)

full access to the organization's normal desktop LAN/WAN resources or services
Connections that provide many or most of the features of a full desktop. Do 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 for mail or calendaring connections)
- tablets unless these connections provide access to many or most desktop features.   Such connections are excluded, for the time being, because they pose less risk and/or the organization has less control over these resources.

relay host
A server that acts as a relay, accepting and agreeing to try to deliver a message that is not destined for a domain that the main server hosts.

remote access
The ability for an organization's users to access its non-public computing resources from locations external to the organization's facilities.

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

split tunneling
A method that 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

Purpose and Use

- 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, D/As 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 used to assess organizations' progress toward meeting these Federal level mandates.
- DHS/FNR 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/FNR also uses those tools to verify organizations' 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 that the owning organization does not update.

11.1. How many public-facing domain names[82] (second-level, e.g., www.dhs.gov) does the organization own? (Exclude domain names which host only FIPS-199 low-impact information on ISPs.) (KFM)

11.1.1. How many DNS names from 11.1 are signed using DNSSEC? (KFM)

11.1.2. What percentage of the second-level DNS names from 11.1 and their sub-domains are signed? (KFM)

11.2. What percentage of public-facing servers[83] use IPv6 (e.g., web servers, email servers, DNS servers, etc.)? (Exclude low-impact networks, cloud servers, and ISP resources unless they require IPv6 to perform their business function.) (KFM)

[82] The terms DNS names and domain names are synonymous.

[83] While the mandate refers to "servers and services," IPv6 addresses apply to hardware assets, not services. To avoid double counting, this question refers to the servers only, both physical and virtual. The servers included should host public-facing services.

Future Metrics and Definitions

Expected Areas of Future Expansion for Network Security Protocols

Area of Expansion	Target for Future Inclusion
• 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 that operate correctly only in IPv4 address spaces	As soon as FY2014
• No additional DNSSEC requirement • 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 D/As will also continue running IPv4 into the foreseeable future	As soon as FY2015

Table 23 – Expected Areas of Future Expansion for Network Security Protocols

Definitions for FY2013 Network Security Protocols

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, which can fool a cache into accepting false DNS data. Various man-in-the-middle attacks are also possible. The (DNSSEC) is not designed to end these attacks, but to make them detectable by the end user.

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 a computer based on its host name. For example, in “host-A.csrc.nist.gov,” “host-A” is a specific computer on the network.

second-level domain name
Variable-length name 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 include “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, and so on, for example, “csrc.nist.gov.” Sub-domain names include all domain names below the top level.

top-level domain name
A name used to indicate a country or region or the type of organization using a name. For example, “.gov,” and “.mil,” are common top-level domains reserved for Federal U.S. organizations.

Appendix A: Computing the Administration Priority Metrics

This appendix describes how the FY13 quarterly and annual FISMA metrics as reported to CyberScope are computed to derive a government-wide average for each capability area of the Administration's priorities. The government-wide averages are computed from the FISMA submissions of the 24 Chief Financial Officers (CFO) Act agencies. Beyond FY12, as the metrics are refined, more complex algorithms or weighting may become part of the calculations.

Overall CAP Score—The overall Cross Agency Priority (CAP) score is currently weighted as the average of the three Continuous Monitoring scores plus the two TIC scores plus the PIV score. All capabilities are considered equally important. Future overall CAP scores may reflect a different weighting because an individual capability might increase in priority.

Continuous Monitoring—The continuous monitoring score is the average of the following three components of continuous monitoring:

> **Asset Management**—Organizations are asked for the total number of organization information technology hardware assets. They are then asked how many of these organization assets have an automated process to provide enterprise-level visibility into asset inventory information. The responses from the 24 CFO Act agencies are totaled for hardware assets (*a*) and assets under the automated asset process (*b*). Dividing the total number of hardware assets with automated asset inventory information by the total number of hardware assets (*b*/*a*) gives a government-wide percentage of automated asset management.
>
> **Configuration Management**—Organizations are asked for the number of assets for which an automated process provides enterprise-level visibility into system configuration information to identify deviations from approved configuration baselines. The responses for the 24 CFO Act agencies are totaled for assets with an automated configuration process (*c*). Dividing the total number of hardware assets with automated configuration information by the total number of hardware assets (*c*/*a*) gives a government-wide percentage of automated configuration management.
>
> **Vulnerability Management**—Organizations are asked for the number of assets for which an automated process provides enterprise-level visibility into NIST National Vulnerability Database vulnerabilities (CVEs). The responses for the 24 CFO Act agencies are totaled for assets with an automated vulnerability process (*d*). Dividing the total number of hardware assets with automated vulnerability information by the total number of hardware assets (*d*/*a*) gives a government-wide percentage of automated vulnerability management.

PIV—The FY13 CAP percentage for PIV-required authentication is obtained by dividing the total number of unprivileged, privileged, and remote access people who are required to log onto the network using two-factor PIV cards by the total number of unprivileged, privileged, and remote access people who are allowed to log onto the network.

To determine the number of people with an unprivileged network account who are required to use PIV, multiply the percentage in 5.2.5 by the total in 5.1.

> *5.2.5. [What percentage of people with an unprivileged network account] are required to log on with a two-factor PIV card? (AP)*
>
> *5.1. How many people have unprivileged network accounts? (Exclude privileged network accounts and non-user accounts.) (Base)*

To determine the number of people with a privileged network account who are required to use PIV, multiply the percentage in 5.4.5 by the total in 5.3.

> *5.4.5. [What percentage of people with a privileged network account] are required to log on with a two-factor PIV card? (AP)*
>
> *5.3. How many people have privileged network accounts? (Exclude unprivileged network accounts and non-user accounts.)(Base)*

To determine the number of people with a remote logon to a network account who are required to use PIV, multiply the percentage in 10.2.5 by the total in 10.1.

> *10.2.5. [For remote access, what percentage of people] are required to log on with a two-factor PIV card? (AP)*
>
> *10.1. How many people log onto the D/A's remote access solution(s) to obtain access to the organization's desktop LAN/WAN resources or services? (Base)*

To determine the total number of people who are required to log on using two-factor PIV cards, sum the results of the three calculations above.

The sum of 5.1 plus 5.3 plus 10.1 equals the number of people with either an interactive or remote network logon account.

The calculation of the FY13 CAP percentage for PIV-required authentication is as follows:

<u>TIC capabilities</u>—Organizations report quarterly on the percentage of the required TIC 1.0 capabilities that are implemented. These self-reported numbers are then used to compute a government average for the large CFO Act agencies. The percentages for the CFO Act agencies are totaled and divided by 23 (DOD is exempted from reporting). *[We are currently checking to see if these numbers align with the CCV assessment numbers from the Cybersecurity Assessment group.]*

<u>TIC consolidation</u>—Organizations report quarterly on the percentage of external network traffic passing through a TIC/MTIPS. These self-reported numbers are then used to compute a government average for the large CFO Act agencies. The percentages for the CFO Act agencies are totaled and divided by 23 (DOD is exempted from reporting). *[We are currently checking to see if these numbers align with the CCV assessment numbers from the Cybersecurity Assessment group.]*

<u>Recap</u>

Automated Asset Management =

____

Automated Configuration Management =

____

Automated Vulnerability Management =

____

PIV =

____

TIC capabilities =

____

TIC consolidation=

____

Appendix B: Acronyms

AO	Authorizing Official
AP	Administration Priorities
APT	Advanced Persistent Threat
ATO	Authorization to Operate
BASE	Baseline Questions
BYOD	Bring Your Own Device
CA	Certificate Authority and/or Certification Authority
CAC	Common Access Cards
CAPEC	Common Attack Pattern Enumeration and Classification
CCB	Configuration Control Board
CCE	Common Configuration Enumeration
CIO	Chief Information Officer
CIS	Center for Internet Security
CM	Continuous Monitoring
CMWG	Continuous Monitoring Working Group
COCO	Contractor Owned Contractor Operated
COTS	Commercial Off The Shelf
CPE	Common Product Enumeration.
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CWSS	Common Weakness Scoring System
D/A	Department/Agency
DBA	Database Administrator
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DKIM	Domain Keys Identified Mail
DLP	Digital Loss Protection

DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	Domain Name System Security Extension
DRM	Digital Rights Management
FAQ	Frequently Asked Questions
FDCC/USGCB	Federal Desktop Core Configuration / United States Government Configuration Baseline
FedRAMP	Federal Risk and Authorization Management Program
FICAM	Federal Identity Credential and Access Management
FIPS	Federal Information Processing Standards
FNS	Federal Network Security
FPKPA	Federal Public Key Infrastructure Policy Authority
GFE	Government Furnished Equipment
GOCO	Government Owned Contractor Operated
GOGO	Government Owned Government Operated
GOTS	Government Off the Shelf
HSPD	Homeland Security Presidential Directive
HW	Hardware
I/O	Input/Output
IP	Internet Protocol
ISP	Internet Service Provider
KFM	Key FISMA Metrics
LAN	Local Area Network
MAC	Media Access Control
MAC	Media Access Card
MAN	Metropolitan Area Network
MFD	Multi Function Device
MTIPS	Managed Trusted Internet Protocol Services
NAC	Network Access Controls
NAT	Network Address Translators
NIST	National Institute of Standards and Technology

NIST SP	National Institute of Standards and Technology Special Publication
NOC	Network Operations Center
NSA	National Security Agency
NVD	National Vulnerability Database
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPM EHRI	Office of Personnel Management Enterprise Human Resources Integration
OS	Operating System
OVAL	Open Vulnerability and Assessment Language
OWA	Outlook Web Access
PGP	Pretty Good Privacy
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RA	Registration Authority
S/MIMI	Secure/Multipurpose Internet Mail Extensions
SAR	Security Awareness Reports
SBU	Sensitive but Unclassified
SCAP	Secure Content Automation Program
SOC	Secure Operations Center
SPF	Sender Policy Framework
SQL	Structured Query Language
SSD	Solid-state drive
SSL	Secure Sockets Layer
SW	Software
TIC	Trust Internet Connections
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
USG	United States Government
USGCB	United States Government Configuration Baseline

VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	Wireless Access Point

Appendix C: Mapping to NIST Controls

FY13 Metric	NIST Guidance	NIST Control (FIPS 200 Specs)
1.1. For each of the FIPS 199 systems' categorized impact levels (H = High, M = Moderate, L = Low) in this question, what is the total number of information systems by organization (i.e., Bureau or Sub-Department Operating Element)? (Organizations with fewer than 5,000 users may report as one unit.)	NIST 800-53	CM-8, RA-2, PM-5
1.1.1. Organization-Operated Systems	NIST 800-53	CM-8,PM-5
1.1.2. Contractor-Operated Systems	NIST 800-53	CM-8, RA-2, PM-5
1.1.3. Systems (from 1.1.1 and 1.1.2) with Security ATO	NIST 800-53, NIST 800-37	CM-8, RA-2, PM-5
2.1. What is the total number of the organization's hardware assets connected to the organization's unclassified network(s)?	NIST 800-53	CM-8,PM-5
2.2. What percentage of assets in 2.1 have an automated capability (scans/device discovery processes) to provide enterprise-level visibility into asset inventory information for all hardware assets?	NIST 800-53	CM-8 enhancement 2
2.2.1. How often are these automated capabilities (scans/device discovery processes) conducted on all assets connected to the organization's full network(s)? Report the lowest frequency of automated device 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.	NIST 800-53	CM-8 enhancement 3
2.3. For how many assets in 2.1 does the organization have an automated capability to determine both whether the asset is authorized and to whom management has been assigned?	NIST 800-53	CM-8 enhancement 3 and 4
2.4. For how many assets in 2.1 does the organization have an automated capability to compare assets from 2.2 and 2.3 in order to identify and remove (manually or through NAC, etc.) the unauthorized devices?	NIST 800-53	CM-8 enhancement 3
2.4.1. For the assets in 2.4, how much time does it actually take to assign an asset for management (authorize)?	NIST 800-53	CM-8 enhancement 3
2.4.2. For the assets in 2.4, how much time does it actually take to remove unauthorized devices, once discovered, with 95% confidence? Report the shortest period in which the removal process is typically completed for all applicable networks. The roll-up of this information is typically the longest time for removal based on all the organization networks, assuming all portions of the organization are using	NIST 800-53	CM-6 enhancement 2

consistent processes. 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 duration, use the comments to explain why, and whether you think this is or is not a valuable metric.		
2.4.3. On how many assets in 2.1 has the organization implemented an automated capability to detect and mitigate unauthorized routes, including routes across air-gapped networks?	NIST 800-53	SC-7 controls (8, 9, 10, 11, 13, 14, 15)
2.5. Can the organization track the installed operating system's vendor, product, version, and patch-level combination(s) in use on the assets in 2.1? If yes, report the number of patch-level combinations. We assume one operating system per device. In the comments, report the number of devices that can boot with multiple operating systems. Note that virtual machines should be counted as assets.	NIST 800-53	CM-2
2.6. 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.) installed on the assets in 2.1? If yes, report the number of general-purpose applications.	NIST 800-53	CM-2 enhancement 5
2.7. For what percentage of applicable assets in 2.1 has the organization implemented an automated capability to detect and block unauthorized software from executing, or for what percentage does no such software exist for the device type? This may include software whitelisting tools that identify executable software by a digital fingerprint and selectively block these. It might also include sandboxing of mobile code to determine before execution whether to allow it to run, where static files do not allow whitelisting. In general, any method included should be able to block zero-day and APT threats.	NIST 800-53	CM-7 Control Enhancement 2
3.1. For each operating system vendor, product, version, and patch-level combination referenced in 2.5, report the following:	NIST 800-53 NIST 800-70	
3.1.1. Has an adequately secure configuration baseline been defined?	NIST 800-53	CM-2
3.1.2. How many hardware assets (which are covered by this baseline, if it exists) have this software?	NIST 800-53	CM-2
3.1.3. What percentage of the applicable hardware assets (per question 2.1) of each kind of operating system software in 3.1 have an automated capability to identify deviations from the approved configuration baselines identified in 3.1.1 and to	NIST 800-53	CM-2 enhancement 2, CM-6 control enhancement 1

provide visibility at the organization's enterprise level?		
3.1.4. What is the frequency of deviation identification (answer in days, per General Instructions)?	NIST 800-53	CM-2 enhancement 1
3.2. For each of the enterprise-wide COTS general-purpose applications referenced in question 2.6., report the following:	NIST 800-53	
3.2.1. Has an adequately secure configuration baseline been defined?	NIST 800-53	CM-2
3.2.2. How many hardware assets (which are covered by this baseline, if it exists) have this software?	NIST 800-53	CM-2
3.2.3. What percentage of the applicable hardware assets, with each kind of software in 3.2, have an automated capability to identify configuration deviations from the approved defined baselines and provide visibility at the organization's enterprise level?	NIST 800-53	CM-2
3.2.4. How frequently is the identification of deviations conducted?	NIST 800-53	CM-3, CM-6
3.3. What percentage of network boundary devices are assessed by an automated capability to ensure that they are adequately configured as intended, such as to adequately protect security?	NIST 800-53	CM-6 enhancement 1
4.1. What percentage of network boundary devices are assessed by an automated capability to ensure that they continue to be adequately free of vulnerabilities?	NIST 800-53	RA-5 enhancement 2
4.2. What percentage of hardware assets identified in section 2.1 are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization's enterprise level?	NIST 800-53	SI-7
4.2.1. What percentage of hardware assets identified in 2.1 that were evaluated using tools to assess the security of the systems and that generated output are compliant with each of the following?	NIST 800-53	RA-5
4.2.1.1. Common Vulnerabilities and Exposures (CVE)	NIST 800-40	RA-5
4.2.1.2. Common Vulnerability Scoring System (CVSS)	NIST 800-40	RA-5
4.2.1.3. Open Vulnerability and Assessment Language (OVAL)	NIST 800-40	RA-5
4.3. For what percentage of information systems does the organization do the following?		
Use methods described in Table 9 to identify and fix instances of common weaknesses, prior to placing that version of the code into production.	NIST 800-53	SA-4
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).	NIST 800-53	CM-2, RA-5
5.1. How many people have unprivileged network accounts?	NIST 800-	IA-2

(Exclude privileged network accounts and non-user accounts.)	53,	
5.2. What percentage of people with an unprivileged network account can log onto the network in each of the following ways?	NIST 800-53	IA-2
5.2.1. Allowed to log on with user ID and password.	NIST 800-53	IA-2
5.2.2. Allowed, but not required, to log on with a non-PIV form of two-factor authentication.	NIST 800-53	IA-2 enhancement 2 and 7
5.2.3. Allowed, but not required, to log on with a two-factor PIV card.	NIST 800-53	IA-2 enhancement 2 and 7
5.2.4. Required to log on with a non-PIV form of two-factor authentication.	NIST 800-53	IA-2 enhancement 2 and 7
5.2.5. Required to log on with a two-factor PIV card.	NIST 800-53	IA-2 enhancement 2 and 7
5.2.6. Required to conduct PIV authentication at the user-account level.	NIST 800-53	IA-2 enhancement 2 and 7
5.3. How many people have privileged network accounts? (Exclude unprivileged network accounts and non-user accounts.)	NIST 800-53	IA-2 enhancements 3 and 6
5.4. What percentage of people with a privileged network account can log onto the network in each of the following ways?	NIST 800-53	IA-2
5.4.1. Allowed to log on with user ID and password.	NIST 800-53	IA-2
5.4.2. Allowed, but not required, to log on with a non-PIV form of two-factor authentication.	NIST 800-53	IA-2 enhancements 1 and 6
5.4.3. Allowed, but not required, to log on with a two-factor PIV card.	NIST 800-53	IA-2 enhancements 1 and 6
5.4.4. Required to log on with a non-PIV form of two-factor authentication.	NIST 800-53	IA-2 enhancements 1 and 6
5.4.5. Required to log on with a two-factor PIV card.	NIST 800-53	IA-2 enhancements 1 and 6
5.4.6. Required to conduct PIV authentication at the user-account level.	NIST 800-53	IA-2 enhancements 1 and 6
5.5. What is the estimated number of organization internal systems?	NIST 800-53	IA-2
5.6. What percentage of the organizations internal systems are configured for authentication in each of the following ways?	NIST 800-53	IA-2
5.6.1. Allows user ID and password.	NIST 800-53	IA-2
5.6.2. Allows, but does not enforce, non-PIV, two-factor authentication for users.	NIST 800-53	IA-2 enhancement 2 and 7
5.6.3. Allows, but does not enforce, two-factor PIV card authentication for users.	NIST 800-53	IA-2 enhancement 2 and 7
5.6.4. Enforces non-PIV, two-factor authentication for all users.	NIST 800-53	IA-2 enhancement 2 and 7

5.6.5. Enforces two-factor PIV card for all users.	NIST 800-53	IA-2 enhancement 2 and 7
5.7. Does the organization have a policy in place that requires the review of privileged network users' privileges?	NIST 800-53	IA-2
5.7.1. What percentage of privileged network users had their privileges reviewed this year for the following?	NIST 800-53	IA-2
5.7.1.1 Privileges on that account reconciled with work requirements.	NIST 800-53	IA-2
5.7.1.2. Adequate separation of duties considering aggregated privileges on all accounts for the same person (user).	NIST 800-53	IA-2
5.7.2. What percentage of privileged network users had their privileges adjusted or terminated after being reviewed this year?	NIST 800-53	IA-2
5.8. What percentage of the organizations systems that have intergovernmental users enforce two-factor PIV card authentication for all users? (Organizations with no intergovernmental systems may respond with N/A.)	NIST 800-53	IA-5 (11)
5.9. Does your organization's Federal Identity, Credential, and Access Management (FICAM) implementation plan include an enterprise Identity and Access Management approach that system owners can leverage to adopt PIV enablement?	NIST 800-53	IA-2
6.1. What is the estimated number of hardware assets from 2.1 in each of the following mobile asset types, and how many are encrypted?	NIST 800-53	AC-3
6.2. What percentage of the organization's email traffic is on systems that implement FIPS 140-2 compliant encryption technologies, such as S/MIME, PGP, OpenPGP, or PKI, when sending messages to government organizations?	NIST 800-53	AC-3
6.2.1 What percentage of inter-organization email traffic is on systems that implement FIPS 140-2 compliant encryption technologies, such as S/MIME, PGP, OpenPGP, or PKI, when sending messages to the public?	NIST 800-54	AC-3
6.3. Which one of the following best describes the organization's PKI Certificate Authority? Respond with the letter of that option. The organization	NIST 800-53, NIST 800-63	SC-17
7.1. What percentage of the required TIC 2.0 Capabilities are implemented?	NIST 800-53	SC-7, enhancement 3
7.2. What percentage of external network traffic to/from the organization's networks passes through a TIC/MTIPS?	NIST 800-53	SC-7
7.3. What percentage of external network/application interconnections to/from the organization's networks passes through a TIC/MTIPS?	NIST 800-53	SC-7
7.4. What percentage of organization email systems implement sender verification (anti-spoofing) technologies	NIST 800-53	AU-10

when sending messages?		
7.5. What percentage of organization email systems use sender verification (anti-spoofing) technologies to detect possibly forged messages from outside the network?	NIST 800-53	AU-10
7.6. What is the estimated percentage of incoming email traffic (measured in messages) whose links or attachments are executed or opened in an in-line sandbox or virtual environment to ascertain whether or not they are malicious, and quarantined as appropriate, before they can be opened by the recipient? (Note: If you consider this to be infeasible, please explain why in the comments.)	NIST 800-53	SI-3
7.7. With what frequency does the organization conduct scheduled scans for unauthorized wireless access points (WAP) connected to an organizational network? Scans of different areas may count as different scans. A scan does not need to cover a particular percentage of the organization to be counted.	NIST 800-53	AC-18 enhancement 2
7.7.1. What percentage of hardware assets in 2.1 are in facilities where scheduled WAP scans are conducted?	NIST 800-53	AC-18
7.7.2. How many WAPs were found?	NIST 800-53	AC-18
7.8. With what frequency does the organization conduct planned, unannounced scans for unauthorized WAPs? Scans of different areas may count as different scans. A scan does not need to cover a substantial portion of the organization or assets to be counted.	NIST 800-53	AC-18
7.8.1. What percentage of hardware assets in 2.1 are in facilities where planned, unannounced WAP scans are conducted?	NIST 800-53	AC-18
7.8.2. How many WAPs were found?	NIST 800-53	AC-18
7.9. How many devices in 2.1, with DLP/DRM (Digital Loss Protection/Digital Rights Management), does the organization have at the gateway to capture outbound data leakage (e.g., PII)?	NIST 800-122, NIST 800-53	SI-4
7.10. Is the organization's internet service (whether obtained through a TICAP or other means) configured to manage filters, excess capacity, bandwidth, or provide other redundancies to limit the effects of information-flooding types of denial-of-service attacks on the organization's internal networks and internet services. Such configuration may include agreements with external network operators to reduce the susceptibility to these types of attacks and respond to them.	NIST 800-53	SC-5, SC-7
8.1. How many of the organization's hardware assets from 2.1 are on networks on which controlled network penetration testing was performed in the reporting period?	NIST 800-53	IR-3, IR-2 enhancement 1, CA-2 enhancement 2, CA-7 enhancement 2, RA-5 enhancement 9,

8.1.1. What percentage of applicable events was detected by NOC/SOC during the penetration test?	NIST 800-53	IR-3, IR-2 enhancement 1, CA-2 enhancement 2, CA-7 enhancement 2, RA-5 enhancement 9,
8.1.2. What percentage of applicable events was detected by NOC/SOC during the other scans or tests?	NIST 800-53	IR-3, IR-2 enhancement 1, CA-2 enhancement 2, CA-7 enhancement 2, RA-5 enhancement 9,
8.1.3. What was the mean time to detection of applicable events?	NIST 800-53	IR-3, IR-2 enhancement 1, CA-2 enhancement 2, CA-7 enhancement 2, RA-5 enhancement 9,
9.1. What percentage of the organization's network users have been given and successfully completed cybersecurity awareness training in FY2012 (at least annually)?	NIST 800-53	AT-2
9.1.1. What is the estimated percentage of new users who satisfactorily completed security awareness training before being granted network access, or completed security awareness training within an organizationally defined time limit that provides adequate security after being granted access?	NIST 800-53	AT-2
9.2. To what extent were users given cybersecurity awareness training content more frequently than annually? (Content could include a single question or tip of the day.)	NIST 800-53	AT-2 enhancement 1
9.2.1. What was the average frequency in days of content provisions? See General Instructions.	NIST 800-53	AT-2 enhancement 1
9.2.2. What percentage of this additional content that addresses emerging threats were not previously covered in the annual training?	NIST 800-53	AT-2 enhancement 1
9.2.3. What is the total number of organization-sponsored exercises (focusing on emerging threats such as phishing) designed to increase cybersecurity awareness and/or measure the effectiveness of cybersecurity awareness training in molding behavior?	NIST 800-53	AT-2 enhancement 1
9.2.4. What percentage of exercises in 9.2.3 suffered no problems or suffered problems that were addressed through appropriate training within three months?	NIST 800-53	AT-2 enhancement 1
9.3. How many of the organizations network users and other staff have significant security responsibilities?	NIST 800-53	AT-3, SA-3
9.3.1. What is the organization's standard for the longest acceptable amount of time between security training events for the personnel counted in question 9.3?	NIST 800-53	AT-3
9.3.2. How many of the personnel counted in question 9.3 have taken security training within the organizational standard defined in 9.3.1?	NIST 800-53	AT-3

10.1. How many people log onto the organization’s remote access solution(s) to obtain access to the organization’s desktop LAN/WAN resources or services?	NIST 800-53, NIST 800-63	AC-17
10.2. For remote access, what percentage of people can log onto the organization’s desktop LAN/WAN resources or services in each of the following ways?	NIST 800-53, NIST 800-64	IA-2
10.2.1. Allowed to log on with user ID and password.	NIST 800-53, NIST 800-63	IA-2
10.2.2. Allowed, but not required, to log on with a non-PIV form of two-factor authentication.	NIST 800-53, NIST 800-64	IA-2
10.2.3. Allowed, but not required, to log on with a two-factor PIV card.	NIST 800-53, NIST 800-65	IA-2
10.2.4. Required to log on with a non-PIV form of two-factor authentication.	NIST 800-53, NIST 800-65	IA-2
10.2.5. Required to log on with a two-factor PIV card.	NIST 800-53, NIST 800-65	IA-2
10.2.6. Required to conduct PIV authentication at the user-account level.	NIST 800-53, NIST 800-65	IA-2
10.3. What is the estimated percentage of remote access connections that have each of the following properties?	NIST 800-53	AC-17
10.3.1. Utilizes FIPS 140-2-validated cryptographic modules.	NIST 800-53	AC-17, AC-3
10.3.2. Prohibits split tunneling and/or dual-connected remote hosts where the laptop has two active connections.	NIST 800-53	AC-11, AC-17
10.3.3. Configured in accordance with OMB M-07-16 to time-out after 30 minutes of inactivity (or less) and require re-authentication to reestablish session.	NIST 800-53	AC-11, AC-17, CM-2
10.3.4. Scans for malware upon connection.	NIST 800-53	AC-4, enhancement 15, AC-17, SI-3
10.4. How many of the organizations systems are internet-accessible and are accessed by the organizations users? This excludes systems accessed through the remote access solutions covered in 10.1 and 10.2.	NIST 800-53	AC-17
10.5. What percentage of organizations systems that are internet-accessible and are accessed by the D/A’s users are configured for authentication in each of the following ways?	NIST 800-53	AC-17, IA-2
10.5.1. Allows user ID and password.	NIST 800-53	AC-17, IA-2
10.5.2. Allows, but does not enforce, non-PIV two-factor authentication for users.	NIST 800-53	AC-17, IA-2

10.5.3. Allows, but does not enforce, two-factor PIV card for users.	NIST 800-53	AC-17, IA-2
10.5.4. Enforces non-PIV two-factor authentication for all users.	NIST 800-53	AC-17, IA-2
10.5.5. Enforces two- factor PIV card for all users.	NIST 800-53	AC-17, IA-2
11.1. How many public-facing domain names (second-level, e.g., www.dhs.gov) does the organization own? (Exclude domain names which host only FIPS-199 low-impact information on ISPs.)	NIST 800-53	SC-20
11.1.1. How many DNS names from 11.1 are signed using DNSSEC?	NIST 800-53	SC-20
11.1.2 What percentage of the second-level DNS names from 11.1 and their sub-domains are signed?	NIST 800-53	SC-20
11.2. What percentage of public-facing servers use IPv6 (e.g., web servers, email servers, DNS servers, etc.)? (Exclude low-impact networks, cloud servers, and ISP resources unless they require IPv6 to perform their business function.)	NIST 800-53	SC-20

Table 24 – Mapping of FISMA Metrics to NIST Guidance and Controls