

FY 2013
Inspector General
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

GENERAL INSTRUCTIONS	1
Sources of Questions and Guidance for the United States Government-Wide (USG-Wide) Federal Information Security Management Act (FISMA) Program.....	1
Expected Levels of Performance.....	2
Administration Priorities:.....	2
Key FISMA Metrics:	3
Baseline Questions:.....	3
Guidance for Responses.....	3
Flexibility in NIST Special Publication 800-53 Requirements.....	3
Empowering OIGs to Focus on Risk	5
1. CONTINUOUS MONITORING MANAGEMENT.....	7
Purpose and Use	7
2. CONFIGURATION MANAGEMENT.....	7
Purpose and Use	7
3. IDENTITY AND ACCESS MANAGEMENT.....	9
Purpose and Use	9
4. INCIDENT RESPONSE AND REPORTING.....	10
Purpose and Use	10
5. RISK MANAGEMENT.....	11
Purpose and Use	11
6. SECURITY TRAINING	13
Purpose and Use	13
7. PLAN OF ACTION & MILESTONES (POA&M)	14
Purpose and Use	14
8. REMOTE ACCESS MANAGEMENT.....	15
Purpose and Use	15
9. CONTINGENCY PLANNING	16
Purpose and Use	16
10. CONTRACTOR SYSTEMS	17
Purpose and Use	17

11. SECURITY CAPITAL PLANNING	18
Purpose and Use	18
Appendix A: Definitions	20
Scope of Definitions	20
Appendix B: Acronyms	28

GENERAL INSTRUCTIONS

Refer to the General Instructions section of the FY13 CIO Reporting Metrics, specifically the Definitions under each control area. All of these instructions apply to the OIG questions except the instructions for “Structure and Organization.”

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.

Expected Levels of Performance¹

Administration Priorities: The expected levels of performance for these 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. Minimum levels and targets have been set by OMB for the AP metrics for FY2013 (Table 1 shows the AP metrics and targets from the *FY13 Chief Information Officer FISMA Reporting Metrics*.)

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 .		
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, that 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 .	80%	95%
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 (TIC⁴) .	80%	95%

¹ The milestones established in this document are not intended to supersede deadlines set by Presidential Directives, OMB policy, or NIST standards. As necessary, DHS is working with agencies to establish milestones as part of agency corrective action plans.

² Continuous does not mean instantaneous. NIST SP 800-137 says that 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).

Administration Priority Area	Section	Performance Metric	Minimal Level for 2013	Target Level for 2013
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](#).”

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

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

Baseline Questions: These questions are being asked to 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.” These 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 of these questions have been established for all organizations to demonstrate improved security over time. New questions are introduced at the Base level unless otherwise directed by OMB.

Guidance for Responses

Based on requests for clarity on questions from the previous fiscal year, the following guidance rules have been incorporated and should be taken into consideration. The level of detail, provided in the narrative box in the OMB template for the security area sections, is at the IG’s discretion. There are no specific requirements for the type or amount of information needed. Where applicable, please indicate the organization’s progress in implementing recommendations to correct material weaknesses identified in prior OIG and GAO audit reports.

Flexibility in NIST Special Publication 800-53 Requirements

Federal agencies and OIGs are clearly required to follow Federal laws and mandatory standards such as the NIST Federal Information Processing Standards (FIPS). OMB also has authority to make other NIST guidelines mandatory.

In the context of FISMA, a number of questions were raised concerning the extent to which NIST SP 800-53, Revision 3, is to be followed. This section attempts to clarify that issue. NIST SP 800-53, Revision 3, is the basis for all of the following discussions.

This topic is partially clarified in NIST SP 800-53, Revision 3, itself: “FIPS are compulsory and binding for federal agencies,” and “FIPS 200 mandates the *use* of NIST SP 800-53, as amended.” (Emphasis added.)

However, there is flexibility in the application of the NIST SP 800-53 requirements:

While federal agencies are required to follow certain specific NIST Special Publications in accordance with OMB policy, *there is flexibility in how agencies apply the guidance*. Federal agencies should apply the security concepts and principles articulated in the NIST Special Publications in accordance with and in the context of the agency’s missions, business functions, and environment of operation. Consequently, the application of NIST guidance by federal agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of adequate security for federal information systems. (Emphasis added.) (NIST SP 800-53, Rev. 3, p. iv)

However, “it is the responsibility of organizations [D/As] to select the appropriate controls, to implement the controls correctly, and **to demonstrate the effectiveness** of the controls in satisfying their stated security requirements.” (Emphasis added) (NIST SP 800-53, Rev. 3, p. 3) In applying NIST SP 800-53, the following should be considered:

- NIST SP 800-53 is meant to serve as a model. There will be circumstances where it is not appropriate to apply each and every one of the controls from the relevant baselines in NIST SP 800-53. As noted by NIST, a screen saver control is generally required, but it probably should not be used on computers in certain real-time control systems. For example, a screen saver could restrict the availability of an FAA air traffic control center system to a degree where it could disrupt the mission of the system. Accordingly, it may not be advisable in this situation to use a screen saver.
- Thus agencies are afforded flexibility to selectively choose which aspects of NIST SP 800-53 are applied and to what degree, as long as there is a documented, conscious, and risk-based justification for the determination as well as approval by an appropriate organization official.
- There are alternative ways to meet the objective(s) stated in NIST SP 800-53 (without using the recommended controls stated) that may be more cost-effective and thus should be employed as an alternative way to achieve [adequate security](#) for federal information systems. If costs are reduced and [adequate security](#) achieved, then the alternative methods are encouraged and acceptable as long as there is a documented, conscious, and risk-based justification for the determination as well as approval by an appropriate organization official.

In short, NIST SP 800-53 is a guide for customizing effective and cost-efficient security measures. In the interest of achieving the best security, there is considerable flexibility in its application (including choosing not to implement controls from relevant baselines) as long as it is done in a documented, risk-based manner.

Empowering OIGs to Focus on Risk

A primary goal in issuing these FISMA questions is to further empower OIGs to focus on how Agencies are evaluating risk and prioritizing security issues. This is guided by the following language from NIST SP 800-53:

When assessing federal organization compliance with NIST Special Publications, Inspectors General, evaluators, auditors, and assessors, ***should consider the intent of the security concepts and principles articulated within the specific guidance document and how the agency applied the guidance in the context of its mission/business responsibilities, operational environment, and unique organizational conditions.*** (Emphasis added.) (NIST SP 800-53, Rev. 3, p. iv)

Below are some examples of items that may not be characterized as a high priority when applying an evaluation focusing on the risk-based nature of the environment:

- Agencies are generally expected to record changes to documentation in the document [change log](#). However, a lack of notation in the [change log](#) should not be considered a high priority if the organization demonstrates it made changes that benefit security and there is no evidence it produces inadequate security. However, organizations should be able to demonstrate that changes were approved by an appropriate organization official.
- While NIST SP 800-53 guidelines suggest agencies develop [configuration guidelines](#), it is generally not cost effective to eliminate all deviations or to require individual waivers for each deviation on each machine. Thus, the mere presence of such deviations should be presumed insignificant, unless the level of deviations stems from a greater weakness in the overall security environment. If the organization has a way to determine what level of compliance provides “adequate” security and meets that standard, then compliance has been achieved. In these cases, organizations must be able to demonstrate how it determined that the level of compliance in fact provided “adequate security”.
- While “annual” awareness training is required, circumstances may dictate that some personnel will not receive their training within exactly 12 months. While the non-compliance is relevant, as long as such deviations do not demonstrably create inadequate security, this situation should not be deemed as a priority. The organization must be able to demonstrate that such deviations are not significant.

OIGs are encouraged to use a type of risk analysis specified in NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, to evaluate findings and compare them to (1) existing organization priorities, (2) Administration Priorities, and (3) Key FISMA Metrics identified in the CIO metrics, to determine areas of weakness and highlight the significance of security issues. This is not to suggest that OIGs should conduct their own full risk analysis. Rather, it is expected that the organization’s own risk analysis be evaluated by the OIG to assess strategically how the organization applied NIST SP 800-39 guidance in the context of its mission, responsibilities, and environment.

Cautionary Note: The methods described above work best in organizations with a mature approach to risk-based assessment. Without that maturity, it can potentially lead to over- or under-expenditure on controls and less effective security.

1. CONTINUOUS MONITORING MANAGEMENT

Purpose and Use

- Even with a completely [hardened system](#), [exploitation](#) may still occur due to attacks like [zero-day vulnerabilities](#). However, continuous monitoring of approved, authorized hardware and software may force attackers to elevate their sophistication for successful attacks.
 - A robust continuous monitoring solution will be able to provide additional visibility for organizations to identify signs of compromise, though no single indicator may identify a definitive [incident](#).
- 1.1. Has the organization [established](#) an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
 - 1.1.1. Documented policies and procedures for continuous monitoring (NIST SP 800-53: CA-7). (AP)
 - 1.1.2. Documented strategy and plans for continuous monitoring (NIST SP 800-37 Rev. 1, Appendix G). (AP)
 - 1.1.3. Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST SP 800-53, 800-53A). (AP)
 - 1.1.4. Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as a common and consistent [POA&M](#) program that is updated with the frequency defined in the strategy and/or plans (NIST SP 800-53, 800-53A). (AP)
 - 1.2. Please provide any additional information on the effectiveness of the organization's Continuous Monitoring Management Program that was not noted in the questions above.

2. CONFIGURATION MANAGEMENT

Purpose and Use

- A key goal of configuration management is to make assets **harder to exploit** through better configuration.
- A key assumption is that configuration management covers the universe of assets to which other controls need to be applied (controls that are defined under asset management).
- 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
 - be implemented in a manner that promotes system accuracy and integrity over time
- 2.1. Has the organization [established](#) a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
- 2.1.1. Documented policies and procedures for configuration management. (Base)
 - 2.1.2. Defined standard [baseline configurations](#). (Base)
 - 2.1.3. Assessments of compliance with [baseline configurations](#). (Base)
 - 2.1.4. Process for timely (as specified in organization policy or standards) remediation of scan result deviations. (Base)
 - 2.1.5. For Windows-based components, [USGCB](#) secure configuration settings are fully implemented, and any deviations from [USGCB](#) baseline settings are fully documented. (Base)
 - 2.1.6. Documented proposed or actual changes to hardware and software configurations. (Base)
 - 2.1.7. Process for timely and secure installation of software patches. (Base)
 - 2.1.8. Software assessing (scanning) capabilities are fully implemented (NIST SP 800-53: RA-5, SI-2). (Base)
 - 2.1.9. Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards (NIST SP 800-53: CM-4, CM-6, RA-5, SI-2). (Base)
 - 2.1.10. [Patch management](#) process is fully developed, as specified in organization policy or standards (NIST SP 800-53: CM-3, SI-2). (Base)
- 2.2. Please provide any additional information on the effectiveness of the organization's Configuration Management Program that was not noted in the questions above.

3. 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 only given to the intended individuals and/or processes.⁵

3.1. Has the organization [established](#) an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and which identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes?

- 3.1.1. Documented policies and procedures for account and identity management (NIST SP 800-53: AC-1). (Base)
- 3.1.2. Identifies all users, including Federal employees, contractors, and others who access organization systems (NIST SP 800-53, AC-2). (Base)
- 3.1.3. Identifies when special access requirements (e.g., multi-factor authentication) are necessary. (Base)
- 3.1.4. If multi-factor authentication is in use, it is linked to the organization's PIV program where appropriate (NIST SP 800-53, IA-2). (KFM)
- 3.1.5. Organization has planned for implementation of PIV for logical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11). (AP)

⁵ 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 without subsequently using it to control access.

- 3.1.6. Organization has adequately planned for implementation of PIV for physical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11).
 - 3.1.7. Ensures that the users are granted access based on needs and separation-of-duties principles. (Base)
 - 3.1.8. Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users. (For example: IP phones, faxes, and printers are examples of devices attached to the network that are distinguishable from desktops, [laptops](#), or servers that have user accounts.) (Base)
 - 3.1.9. Identifies all user and [non-user accounts](#). (Refers to user accounts that are on a system. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes. They are not associated with a single user or a specific group of users.) (Base)
 - 3.1.10. Ensures that accounts are terminated or deactivated once access is no longer required. (Base)
 - 3.1.11. Identifies and controls use of shared accounts. (Base)
- 3.2. Please provide any additional information on the effectiveness of the organization's Identity and Access Management Program that was not noted in the questions above.

4. INCIDENT RESPONSE AND REPORTING

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.
 - This allows the organization to use this information about successful attacks and their impact to make informed, risk-based decisions about where it is most cost effective and essential to focus security resources.
 - Penetration testing allows organizations to test their network defenses and estimate the extent to which they are able to detect and respond to actual threats.
- 4.1. Has the organization [established](#) an [incident](#) response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

- 4.1.1. Documented policies and procedures for detecting, responding to, and reporting [incidents](#) (NIST SP 800-53: IR-1). (Base)
 - 4.1.2. Comprehensive analysis, validation, and documentation of [incidents](#). (KFM)
 - 4.1.3. When applicable, reports to US-CERT within [established](#) timeframes (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19). (KFM)
 - 4.1.4. When applicable, reports to law enforcement within [established](#) timeframes (SP 800-61). (KFM)
 - 4.1.5. Responds to and resolves [incidents](#) in a timely manner, as specified in organization policy or standards, to minimize further damage (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19). (KFM)
 - 4.1.6. Is capable of tracking and managing risks in a virtual/[cloud](#) environment, if applicable. (Base)
 - 4.1.7. Is capable of [correlating incidents](#). (Base)
 - 4.1.8. Has sufficient [incident](#) monitoring and detection coverage in accordance with government policies (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19). (Base)
- 4.2. Please provide any additional information on the effectiveness of the organization's Incident Management Program that was not noted in the questions above.

5. RISK MANAGEMENT

Purpose and Use

- One goal in issuing these FISMA questions is to further empower OIGs to focus on how organizations are evaluating risk and prioritizing security issues.
 - OIGs are encouraged to use a type of risk analysis as specified in NIST SP 800-39 to evaluate findings and compare them to (1) existing organization priorities and (2) Administration Priorities, and (3) Key FISMA Metrics identified in the CIO metrics, to determine areas of weakness and highlight the significance of security issues.
- 5.1. Has the organization [established](#) a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
- 5.1.1. Documented policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process. (Base)

- 5.1.2. Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1. (Base)
- 5.1.3. Addresses risk from a mission and business process perspective and is guided by the risk decisions from an organizational perspective, as described in NIST SP 800-37, Rev. 1. (Base)
- 5.1.4. Addresses risk from an information system perspective and is guided by the risk decisions from an organizational perspective and the mission and business perspective, as described in NIST SP 800-37, Rev. 1. (Base)
- 5.1.5. Has an up-to-date system inventory.(Base)
- 5.1.6. Categorizes information systems in accordance with government policies. (Base)
- 5.1.7. Selects an appropriately tailored set of [baseline security controls](#). (Base)
- 5.1.8. Implements the tailored set of [baseline security controls](#) and describes how the controls are employed within the information system and its environment of operation. (Base)
- 5.1.9. Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (Base)
- 5.1.10. Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable. (Base)
- 5.1.11. Ensures information security controls are monitored on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting [security impact analyses](#) of the associated changes, and reporting the security state of the system to designated organizational officials. (Base)
- 5.1.12. Information-system-specific risks (tactical), mission/business-specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization. (Base)
- 5.1.13. Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO). (Base)
- 5.1.14. Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information-system-related security risks. (Base)

- 5.1.15. [Security authorization package](#) contains system security plan, security assessment report, and [POA&M](#) in accordance with government policies (NIST SP 800-18, 800-37). (Base)
- 5.1.16. [Security authorization package](#) contains accreditation boundaries, defined in accordance with government policies, for organization information systems. (Base)
- 5.2. Please provide any additional information on the effectiveness of the organization's Risk Management Program that was not noted in the questions above.

6. SECURITY TRAINING

Purpose and Use

- Worldwide, some of the most effective attacks on cyber networks currently are directed at exploiting user behavior. These include [phishing attacks](#), social engineering to obtain passwords, and introduction of malware via removable media.
 - These threats are especially effective when directed at those with elevated network privileges and/or other elevated cyber responsibilities.
 - Training users (privileged and unprivileged) and those with access to other pertinent information and media is a necessary deterrent to these methods. Therefore, organizations are expected to use risk-based analysis to determine the correct amount, content, and frequency of update to achieve [adequate security](#) in the area of influencing these behaviors that affect cybersecurity.
 - DHS has determined that some metrics in this section are prioritized as Key FISMA Metrics.
 - Some questions in this section also contain baseline information to be used to assess future improvement in performance.
 - The metrics will be used to assess the extent to which organizations are providing adequate training to address these attacks and threats.⁶
- 6.1. Has the organization [established](#) a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
- 6.1.1. Documented policies and procedures for [security awareness training](#) (NIST SP 800-53: AT-1). (Base)
- 6.1.2. Documented policies and procedures for specialized training for users with significant information security responsibilities. (Base)
- 6.1.3. Security training content based on the organization and roles, as specified in organization policy or standards. (Base)

⁶ Even if the organization uses a DHS ISS-LOB, it remains the organization's responsibility to determine whether the content of the training is adequate to cover the threats being faced by that organization.

- 6.1.4. Identification and tracking of the status of [security awareness training](#) for all personnel (including employees, contractors, and other organization users) with access privileges that require [security awareness training](#). (KFM)
 - 6.1.5. Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training. (KFM)
 - 6.1.6. Training material for [security awareness training](#) contains appropriate content for the organization (NIST SP 800-50, 800-53). (Base)
- 6.2. Please provide any additional information on the effectiveness of the organization's Security Training Program that was not noted in the questions above.

7. PLAN OF ACTION & MILESTONES (POA&M)

Purpose and Use

- [POA&M](#) processes are important as part of the risk management process to track problems and decide which ones to address.
 - Effective POA&M processes also indicate an organization's efforts to address corrective actions with a standard and centralized approach.
- 7.1. Has the organization [established](#) a [POA&M](#) program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
- 7.1.1. Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation. (Base)
 - 7.1.2. Tracks, prioritizes, and remediates weaknesses. (Base)
 - 7.1.3. Ensures remediation plans are effective for correcting weaknesses. (Base)
 - 7.1.4. Establishes and adheres to milestone remediation dates. (Base)
 - 7.1.5. Ensures resources and ownership are provided for correcting weaknesses. (Base)
 - 7.1.6. [POA&Ms](#) include security weaknesses discovered during assessments of security controls and that require remediation (do not need to include security weakness due to a risk-based decision to not implement a security control) (OMB M-04-25). (Base)
 - 7.1.7. Costs associated with remediating weaknesses are identified (NIST SP 800-53, Rev. 3, Control PM-3; OMB M-04-25). (Base)

- 7.1.8. Program officials report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the [POA&M](#) activities at least quarterly (NIST SP 800-53, Rev. 3, Control CA-5; OMB M-04-25). (Base)
- 7.2. Please provide any additional information on the effectiveness of the organization's [POA&M](#) Program that was not noted in the questions above.

8. REMOTE ACCESS MANAGEMENT

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. Responses to the above questions will help Agencies deter, detect, and defend against unauthorized network connections/access to internal and external networks.
 - Remote connections allow users to access the network without gaining physical access to organization space and the computers hosted there. Moreover, the connections over the Internet provide opportunities for compromise of information in transit. Because these connections are beyond physical security controls, they need [compensating controls](#) to ensure that only properly identified and authenticated users gain access, and that the connections prevent [hijacking](#) by others.
- 8.1. Has the organization [established](#) a [remote access](#) program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
- 8.1.1. Documented policies and procedures for authorizing, monitoring, and controlling all methods of [remote access](#) (NIST SP 800-53: AC-1, AC-17). (Base)
- 8.1.2. Protects against unauthorized connections or subversion of authorized connections. (Base)
- 8.1.3. Users are uniquely identified and authenticated for all access (NIST SP 800-46, Section 4.2, Section 5.1). (Base)
- 8.1.4. Telecommuting policy is fully developed (NIST SP 800-46, Section 5.1). (Base)
- 8.1.5. If applicable, multi-factor authentication is required for [remote access](#) (NIST SP 800-46, Section 2.2, Section 3.3). (KFM)
- 8.1.6. Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms. (Base)

- 8.1.7. Defines and implements encryption requirements for information transmitted across public networks. (KFM)
 - 8.1.8. [Remote access](#) sessions, in accordance with OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required. (Base)
 - 8.1.9. Lost or stolen devices are disabled and appropriately reported (NIST SP 800-46, Section 4.3; US-CERT Incident Reporting Guidelines). (Base)
 - 8.1.10. [Remote access](#) rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4). (Base)
 - 8.1.11. Remote-access user agreements are adequate in accordance with government policies (NIST SP 800-46, Section 5.1; NIST SP 800-53, PS-6). (Base)
- 8.2. Please provide any additional information on the effectiveness of the organization's Remote Access Management that was not noted in the questions above.
- 8.3. How many unauthorized (rogue) connections were identified in FY13?

9. CONTINGENCY PLANNING

Purpose and Use

- Contingency planning deals with rarely occurring risks. As such, there is a temptation to ignore these risks.
 - The purpose of this section is to determine if the organization is giving adequate attention to the rare events that have the potential for significant consequences and promoting them to first-priority risks.
- 9.1. Has the organization [established](#) an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
- 9.1.1. Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST SP 800-53: CP-1). (Base)
 - 9.1.2. The organization has incorporated the results of its system's Business Impact Analysis (BIA) into the analysis and strategy development efforts for the organization's Continuity of Operations Plan (COOP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) (NIST SP 800-34). (Base)

- 9.1.3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures (NIST SP 800-34). (Base)
 - 9.1.4. Testing of system-specific contingency plans. (Base)
 - 9.1.5. The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34). (Base)
 - 9.1.6. Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)
 - 9.1.7. Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans. (Base)
 - 9.1.8. After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34). (Base)
 - 9.1.9. Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)
 - 9.1.10. Alternate processing sites are not subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).
 - 9.1.11. Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)
 - 9.1.12. Contingency planning that considers supply chain threats. (Base)
- 9.2. Please provide any additional information on the effectiveness of the organization's Contingency Planning Program that was not noted in the questions above.

10. CONTRACTOR SYSTEMS

Purpose and Use

- These questions are being asked because in the past some Federal Agencies tended to assume that they were not responsible for managing the risk of contractor systems.
 - The key question is "Are these contractor-operated systems being managed to ensure that they have [adequate security](#), and can the organization make an informed decision about whether or not to accept any residual risk?"
- 10.1. Has the organization [established](#) a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in the [cloud](#) external to the organization? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

- 10.1.1. Documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in a [public cloud](#). (Base)
 - 10.1.2. The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with Federal and organization guidelines (NIST SP 800-53: CA-2). (Base)
 - 10.1.3. A complete inventory of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in a [public cloud](#). (Base)
 - 10.1.4. The inventory identifies interfaces between these systems and organization-operated systems (NIST SP 800-53: PM-5). (Base)
 - 10.1.5. The organization requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates. (Base)
 - 10.1.6. The inventory of contractor systems is updated at least annually. (Base)
 - 10.1.7. Systems that are owned or operated by contractors or entities, including organization systems and services residing in a [public cloud](#), are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines. (Base)
- 10.2. Please provide any additional information on the effectiveness of the organization's Contractor Systems Program that was not noted in the questions above.

11. SECURITY CAPITAL PLANNING

Purpose and Use

- One key area of capital investment in the next few years will be investments in the tools and other infrastructure needed for adequate continuous monitoring. Fortunately, most of these tools also support (and are needed for) good network and system operations. Thus many of these tools may already be in place.
- This section might equally consider operational budgeting. Clearly, good security requires a wise investment of operational resources, not just capital.

11.1. Has the organization [established](#) a security capital planning and investment program for information security? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

- 11.1.1. Documented policies and procedures to address information security in the [capital planning and investment control \(CPIC\)](#) process. (Base)

- 11.1.2. Includes information security requirements as part of the capital planning and investment process. (Base)
 - 11.1.3. Establishes a discrete line item for information security in organizational programming and documentation (NIST SP 800-53: SA-2). (Base)
 - 11.1.4. Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST SP 800-53: PM-3). (Base)
 - 11.1.5. Ensures that information security resources are available for expenditure as planned. (Base)
- 11.2. Please provide any additional information on the effectiveness of the organization's Security Capital Planning Program that was not noted in the questions above.

Appendix A: Definitions

Scope of Definitions

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

adequate security

“Security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls” (OMB Circular A-130, Appendix III, definitions). Per OMB FISMA guidance (M-11-33, FAQ 15), the Agency head is responsible for determining the acceptable level of risk, with input from system owners, program officials, and CIOs.

applicable hardware assets

Those [hardware assets](#) counted in section 2.0 of the *FY13 Chief Information Officer FISMA Reporting Metrics* that have the software being configured and installed on the asset.

automated capability

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

automated capability to detect hardware assets

Automated detection of [hardware assets](#) is also known as “automated device discovery processes.”

Defined as any report of actual assets that can be generated by a computer, this includes:

- active scanners (might include a dedicated discovery scan or a vulnerability scan of an IP range)
- passive listeners
- agent-generated data
- switches and routers reporting connected devices
- scripts run 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 the device outside the designated range (foreign devices) at the levels of LAN, MAN, WAN, and so on. Preferably, traffic would not be routed to/from such foreign devices.

baseline configurations

As defined by NIST SP 800-53, the baseline configuration is a documented, up-to-date specification that provides information about the components of an information system (e.g., the standard software load

for a workstation, server, network component, or mobile device, including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture.

baseline security controls

The tailored set of minimum security controls defined in NIST SP 800-53 for a low-impact, moderate-impact, or high-impact information system in accordance with FIPS 200.

BlackBerry

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

capital planning and investment control (CPIC)

This guidance is based on the NIST SP 800-65, *Recommendations for Integrating Information Security into the Capital Planning and Investment Control Process*. As defined by the Clinger-Cohen Act and OMB Circular A-11, capital planning and investment control (CPIC) is a decision-making process for ensuring IT investments integrate strategic planning, budgeting, procurement, and the management of IT in support of Agency missions and business needs.

change log

A documented record of approved changes to a system, program, or document.

cloud computing resources

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

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics.⁷

- **On-demand self-service.** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- **Broad network access.** Capabilities are available over the network⁸ and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, [tablets](#), [laptops](#), and workstations).
- **Resource pooling.** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant⁹ model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level

⁷ All of these must be present to make the service a cloud service.

⁸ The network does not necessarily mean the Internet.

⁹ The reference to a multi-tenant model does not necessarily imply a public cloud. The multiple tenants could all be parts of a large organization, for example in a government-dedicated cloud.

of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

- **Rapid elasticity.** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- **Measured service.** Cloud systems automatically control and optimize resource use by leveraging a metering capability¹⁰ at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

compensating controls

Defined by NIST SP 800-53 as alternative safeguards and countermeasures that are employed to accomplish the intent of the original security controls that could not be effectively employed. Organizational decisions on the use of compensating controls are documented in the security plan and are not exceptions or waivers to the baseline controls.

configuration guidelines

Procedures that can be developed for the security program in general and for a particular information system that are consistent with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

correlating incidents

The process that the organization utilizes to correlate individual events or incidents to achieve an organization-wide perspective on incident awareness and response using automated support tools.

device discovery process

See the definition for "[automated capability to detect hardware assets](#)." This is an automated ability to discover devices connected to the network to produce a network topology and retrieve basic device information.

established

Consistent implementation of the defined policy and procedures.

exploitation

The unexpected use of an identified vulnerability of an information system to gain access, escalate privileges, or launch attacks.

hardened system

An information system in which stringent configuration settings have been applied utilizing a security guide, Security Technical Implementation Guide (STIG), or benchmark to meet operational requirements with the least amount of functionality.

¹⁰ "Typically this is done on a pay-per-use or charge-per-use basis" (NIST SP 800-145, p. 2).

hardware assets

Agencies 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. The last category, “other addressable devices on the network,” indicates the criterion for including other kinds of specialized devices not explicitly called out.

- non-portable computers¹¹
 - servers
 - workstations (desktops)
- portable computers
 - laptops
 - net-books
 - [tablets](#) (iPad, Kindle, other Android)
 - [mobile devices](#)
 - smartphones (iPhone, Android)
 - cell phones
 - [BlackBerry](#)
- networking devices¹²
 - routers
 - switches
 - gateways, bridges, Wireless Access Points (WAPs)
 - firewalls
 - intrusion detection/prevention systems
 - Network Address Translators (NAT devices)
 - hybrids of these types (like a NAT router)
 - load balancers
 - modems
- other communication devices
 - encryptors
 - decryptors
 - VPN endpoints¹³
 - medical devices that are part of a patient monitoring network
 - alarms and physical access control devices
 - PKI infrastructure¹⁴
- other input/output devices if they appear with their own address
 - network printers/plotters/copiers/multi-function devices (MFDs)
 - network fax portals

¹¹ Multi-purpose devices need only be counted once per device. Devices with multiple IP connections need only be counted once per device, not once per connection. This is an inventory of [hardware assets](#), not data.

¹² 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.

¹³ VPN endpoints generally mean the encryptors/decryptors at each end of the VPN tunnel.

¹⁴ PKI assets should be included in the network(s) on which it resides. Special methods may be needed to adequately check it for vulnerabilities, compliance, and so on, as described in subsequent sections, or if these are not done, it should be included among the assets not covered.

- network scanners
- network accessible storage devices
- VOIP phones
- other network I/O devices
- virtual machines that can be addressed¹⁵ as if they are a separate physical machine should be counted as separate assets,¹⁶ 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) and non-GFE assets are included if they meet the other criteria for inclusion listed here.¹⁷ Mobile devices that receive Federal e-mail are to be considered to be connected. Note: If non-GFE is allowed to connect, it is especially important that it be inventoried, authorized, and correctly configured prior to connection.¹⁸

Only devices connected to the network(s) of the organization should be reported, and only if they are addressable¹⁹ for network traffic (except USB connected devices, which are included). The reason we limit this to addressable devices is that from a network point of view, only addressable devices are attackable. For example, a monitor (not addressable, thus not included) can only be attacked through the addressable computer it is connected to. USB devices are added because they are a source of attacks.

hijacking

An attacker taking control of an information system through the [exploitation](#) of a vulnerability by using a network connection or physical access.

incident

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices (per NIST SP 800-61). While this definition is based on compliance, it is also appropriate to consider a broader definition of incident as being any event that compromises the

¹⁵ “Addressable” means by IP address or any other method to communicate to the network.

¹⁶ 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, generally do not create separate assets 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>).

¹⁷ If this non-GFE connects in a limited way such that it can only send and receive presentation-layer data from a virtual machine on the network, and this data has appropriate encryption (such as a Citrix connection), the non-GFE does not have to be counted.

¹⁸ If this non-GFE connects in a limited way such that it can only send and receive presentation layer-data from a virtual machine on the network, and this data has appropriate encryption (such as a Citrix connection), the non-GFE does not have to be counted.

¹⁹ “Addressable” means that communications can be routed to this asset, typically because it has an assigned IP address. Devices connecting via mechanisms like Citrix that limit the traffic allowed to pass do not need to be counted if justified by an adequate risk assessment, approved by the AO.

confidentiality, integrity, and availability of the organization’s information to an extent that has a noticeable negative impact on mission performance in support of the risk management hierarchy described in NIST SP 800-39.

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 be connected to a number of different networks. These often have wireless capability requiring special controls.

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 that presents credentials and performs functions under the management of the person (or group) that owns the account²⁰ 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.²¹

patch management

The methodology used by an Agency to manage flaw remediation and the installation of software updates on information systems.

Personal Identity Verification (PIV) card

A PIV card (credential) is a “Personal Identity Verification Card,” as defined in NIST FIPS 201. For the purposes of answering this question, we only count PIV 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.

phishing attack

A network user responding to a fraudulent message producing a negative impact on the confidentiality, integrity, and/or availability of the organization’s information.

Plan of Action and Milestones (POA&M)

Documents the vulnerabilities, associated corrective actions/remediation activities, and corrective action cost for each Agency security weakness.

²⁰ For example, this includes machine accounts and operating system built-in accounts. More generally, it includes “service” accounts.

²¹ 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.”

public cloud

A cloud computing model in which a service provider provides applications, storage, and other services to the general public.

remote access

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

security authorization package

According to NIST SP 800-53, a security authorization package consists of three principal documents: the security plan, the security assessment report, and the [POA&M](#).

security awareness training

Training provided to all information system users when network access is initially granted and as required after system changes, according to organizational requirements.

security impact analyses

An assessment of risk to understand the impact of the changes to an information system and determine if additional security controls are required.

smartphone

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

tablet computers

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

Trusted Internet Connection (TIC)

The purpose of the TIC Initiative, as outlined in OMB Memorandum M-08-05, is to optimize and standardize the security of individual external network connections currently in use by Federal Agencies, to include connections to the Internet.

United States Government Configuration Baseline (USGCB)

According to NIST, "The purpose of the United States Government Configuration Baseline (USGCB) initiative is to create security configuration baselines for Information Technology products widely deployed across the federal agencies. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate. The USGCB is a Federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain an effective configuration settings focusing primarily on security." (NIST, "The United States Government Configuration Baseline," <http://usgcb.nist.gov/>.)

visibility at the organization's enterprise level

The information about hardware assets can be viewed at the level of

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

zero-day vulnerabilities

Vulnerabilities in software that the developer may not be aware of and has not remediated before an attacker can develop and distribute vulnerability exploit code.

Appendix B: Acronyms

Acronym	Definition
AO	authorizing official
AP	Administration Priorities
Base	baseline questions
BIA	Business Impact Analysis
CAC	Common Access Cards
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CNCI	Comprehensive National Cybersecurity Initiative
CPIC	Capital Planning and Investment Control
CPU	central processing unit
CVE	Common Vulnerabilities and Exposures
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DMZ	demilitarized zone
FAQ	frequently asked questions
FAA	Federal Aviation Administration
FIPS	Federal Information Processing Standards
FNS	Federal Network Security
GAO	Government Accountability Office
GFE	Government-Furnished Equipment
HSPD	Homeland Security Presidential Directive
I/O	input/output
IP	Internet protocol
KFM	Key FISMA Metrics
LAN	Local Area Network
MAN	Metropolitan Area Network
MFD	multi-function device
MOU	Memorandum of Understanding
MTIPS	Managed Trusted Internet Protocol Services
NAT	Network Address Translators

Acronym	Definition
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NSA	National Security Agency
NVD	National Vulnerability Database
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIV	personal identity verification
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
TT&E	test, training, and exercise
TIC	Trusted 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
VOIP	voice over internet protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	Wireless Access Point