FY 2012

Inspector General

Federal Information Security Management Act

Reporting Metrics

Prepared by:

US Department of Homeland Security

National Cyber Security Division

Federal Network Security

March 6, 2012

GENERAL INSTRUCTIONS

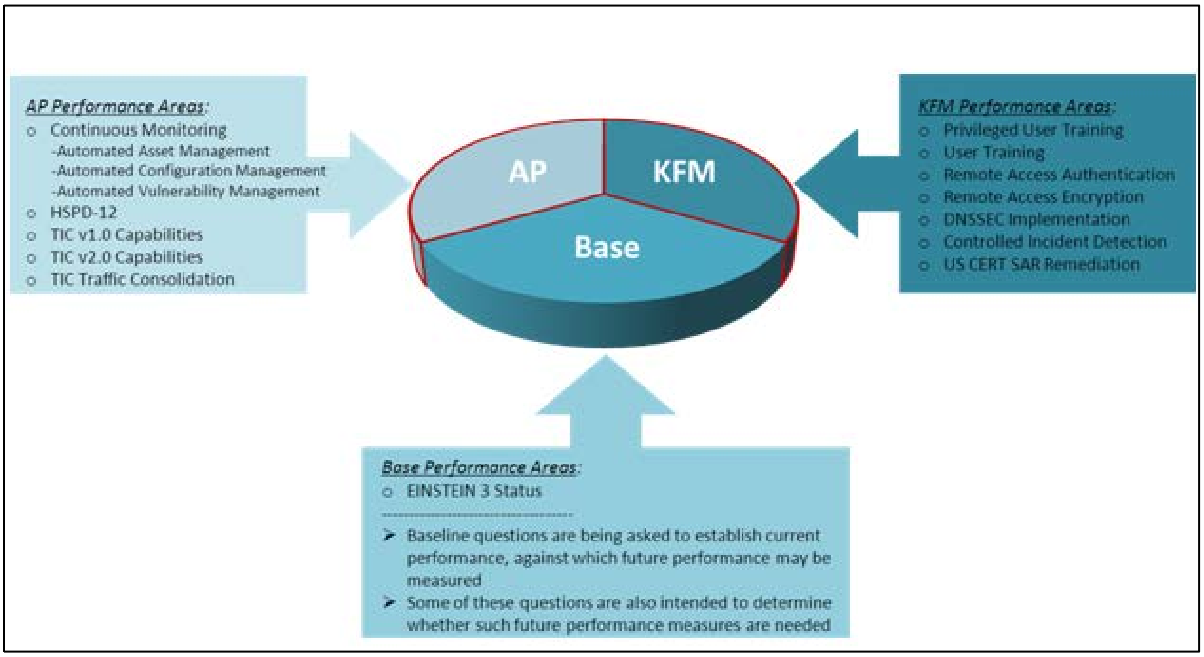
Refer to the General Instructions section of the FY12 CIO Reporting Metrics specifically, the Definitions under each control area. All of these instructions apply to the OIG questions except the instructions for "Structure and Organization".

The FY12 IG metrics are aligned with the FY 12 CIO Reporting Metrics in terms of identifying each individual question as an Administration Priority (AP), a Key FISMA Metric (KFM), or a Baseline Question (Base); Definitions and Purpose and Use Statements are also included for additional clarity. In future fiscal years, the OIG Metrics will be mapped with the CIO Reporting Metrics control areas as described in FISM 12-02.

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

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

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



AP Performance Areas:

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

KFM Performance Areas:

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

Base Performance Areas:

- EINSTEIN 3 Status

➢ Baseline questions are being asked to establish current performance, against which future performance may be measured

➢ Some of these questions are also intended to determine whether such future performance measures are needed

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

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

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

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 Special Publication 800-53 is to be followed. This section attempts to clarify that issue.

This topic is partially clarified in NIST SP 800-53 rev3 itself:

- "FIPS are compulsory and binding for federal agencies."
- "FIPS 200 mandates the ***<u>use</u>*** of Special Publication 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.) (800-53, rev3, 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 800-53, Rev 3, p. 3] In applying NIST SP 800-53, the following should be considered:

- NIST Special Publication 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 Special Publication 800-53. , As noted by NIST, a screen saver control is generally required, but 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 Special Publication 800-53 is applied and to what degree, as long as there is a documented, conscious and risk-based justification for the determination, and approval by an appropriate Organization official.
- There are alternative ways to meet the objective(s) stated in 800-53 (without using the recommended controls stated in 800-53 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 longs as there is a documented, conscious and risk-based justification for the determination, and approval by an appropriate Organization official.

In short, the NIST Special Publication 800-53 is a guide for customizing effective and cost-efficient security measures. In the interests of achieving the best security, there is considerable flexibility in the 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

One 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 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.) (800-53, rev3, p. iv)

Below are some examples of items that may not be characterized as a 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, if the Organization can demonstrate that it made appropriate changes, even though not logged in the change log (or if sub-document changes are not logged in a master document), the lack of notation in the change log should not be considered a high priority, unless there is evidence that it produces inadequate security. However, D/As should be able to demonstrate that changes were approved by an appropriate Organization official.
- While NIST 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 overall level of deviations threatens adequate security. If the Organization has a way to determine what level of compliance provides “adequate” security, and adequately meets that standard, then compliance has been achieved. In these cases, D/As 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 D/A must be able to demonstrate that such deviations are not significant.

OIGs are encouraged to use a type of risk analysis as specified in NIST 800-39 to evaluate findings and compare those to (1) existing Organization priorities, and (2) Administration priorities and 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 how the Organization applied 800-39 guidance in the context of it 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.

1. CONTINUOUS MONITORING MANAGEMENT

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? If yes, 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 800-53: CA-7). (AP)

1.1.2. Documented strategy and plans for continuous monitoring (NIST 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 800-53, NIST 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 POA&M additions and updates with the frequency defined in the strategy and/or plans (NIST 800-53, NIST 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.

Purpose and Use

These questions are being asked for the following reasons:

- The federal Continuous Monitoring Working Group (CMWG) has determined that continuous monitoring (CM) of configurations is one of the first areas where CM capabilities need to be developed. This applies to both operating systems, and widely used applications.
- Even with a completely hardened system, exploitation may still occur due to zero day vulnerabilities. However, this forces attackers to elevate their sophistication for successful attacks.
- Rather, a robust continuous monitoring solution will be able to provide additional visibility for organizations to identify signs of compromise, though no single indicator may identify a definitive incident.

2. CONFIGURATION MANAGEMENT

2.1. Has the Organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, 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. Standard baseline configurations defined. (Base)

2.1.3. Assessing for 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, FDCC/USGCB secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings 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 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 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 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.

Purpose and Use

These questions are being asked for the following reasons:

- A key goal of configuration management is to make assets harder to exploit through better configuration.
- A key assumption is that configuration management covers the universe of assets to which other controls need to be applied (controls that are defined under asset management).
- To have a capable configuration management program, the configuration management capability needs to be:
  - Relatively complete, covering enough of the software base to significantly increase the effort required for a successful attack.
  - Relatively timely, being able to find and fix configuration deviations faster than they can be exploited.

3. IDENTITY AND ACCESS MANAGEMENT

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 identifies users and network devices? If yes, 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 800-53: AC-1). (Base)

3.1.2. Identifies all users, including federal employees, contractors, and others who access Organization systems (NIST 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 800-53, IA-2).(KFM)

3.1.5. Organization has adequately 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)

3.1.6. Ensures that the users are granted access based on needs and separation of duties principles. (Base)

3.1.7. Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users. (For example: IP phones, faxes, printers are examples of devices attached to the network that are distinguishable from desktops, laptops or servers that have user accounts) (Base)

3.1.8. Identifies all User and Non-User Accounts (refers to user accounts that are on a system. Examples of non-user accounts are accounts such as an IP that is set up for printing. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes that are not associated with a single user or a specific group of users) (Base)

3.1.9. Ensures that accounts are terminated or deactivated once access is no longer required. (Base)

3.1.10. 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.

Purpose and Use

These questions are being asked for the following reasons:

- OMB and DHS have determined that Federal Identity Management (HSPD-12) is among the areas where additional controls need to be developed. See also OMB M-04-04 for web based systems.
- Strong information system authentication requires multiple factors to securely authenticate a user. Secure authentication requires something you have, something you are, and something you know. A single-factor authentication mechanism, such as a username and password, is insufficient to block even basic attackers.
- The USG will first move to a two factor authentication using PIV cards, though a stronger authentication solution would include all three factors.

- Enhanced identity management solutions also support the adoption of additional non-security benefits, such as Single Sign On, more useable systems, and enhanced identity capabilities for legal and non-repudiation needs.
- A key goal of identity and access management is to make sure that access rights are only given to the intended individuals and/or processes.[4]
- To have a capable identity management program, this capability needs to be:
  - Relatively complete, covering all accounts.
  - Relatively timely, being able to find and remove stale or compromised accounts faster than they can be exploited.

4. INCIDENT RESPONSE AND REPORTING

4.1. Has the Organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, 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 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 800-53, 800-61, and OMB M-07-16, M-06-19). (KFM)

4.1.4. When applicable, reports to law enforcement within established timeframes (SP 800-86). (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 800-53, 800-61, and 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. There is sufficient incident monitoring and detection coverage in accordance with government policies (NIST 800-53, 800-61, and 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.

Purpose and Use

These questions are being asked for the following reasons:

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

- Given real world realities, it is reasonable to expect that some attacks will succeed. Organizations need to be able to detect those attacks. Ideally, Organizations would defend against those attacks in real time, but at a minimum, Organizations are expected to determine the kinds of attacks that are most successful.
- This allows the Organization to use this information about successful attacks and their impact to make informed risk-based decisions about where it is most cost-effective and essential to focus security resources.

5. RISK MANAGEMENT

5.1. Has the Organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

5.1.1. Documented and centrally accessible 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 800-37, Rev.1(Base)

5.1.3. Addresses risk from a mission and business process perspective and is guided by the risk decisions at the organizational perspective, as described in NIST 800-37, Rev.1. (Base)

5.1.4. Addresses risk from an information system perspective and is guided by the risk decisions at the organizational perspective and the mission and business perspective, as described in NIST 800-37, Rev. 1. (Base)

5.1.5. Categorizes information systems in accordance with government policies. (Base)

5.1.6. Selects an appropriately tailored set of baseline security controls. (Base)

5.1.7. 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)

5.1.8. 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)

5.1.9. 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)

5.1.10. 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)

5.1.11. Information system specific risks (tactical), mission/business specific risks and organizational level (strategic) risks are communicated to appropriate levels of the organization. (Base)

5.1.12. Senior Officials are briefed on threat activity on a regular basis by appropriate personnel. (e.g., CISO). (Base)

5.1.13. 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)

5.1.14. Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies. (SP 800-18, SP 800-37) (Base)

5.1.15. Security authorization package contains Accreditation boundaries for Organization information systems defined in accordance with government policies. (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.

Purpose and Use:

These questions are being asked for the following reasons:

- One goal in issuing these FISMA questions is to further empower OIGs to focus on how Agencies are evaluating risk and prioritizing security issues.
- OIGs are encouraged to use a type of risk analysis as specified in NIST 800-39 to evaluate findings and compare those to (1) existing Organization priorities, and (2) Administration priorities and key FISMA metrics identified in the CIO metrics, to determine areas of weakness and highlight the significance of security issues.

6. SECURITY TRAINING

6.1. Has the Organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, 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 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)

6.1.4. 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 does not contain appropriate content for the Organization (SP 800-50, SP 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.

Purpose and Use

These questions are being asked for the following reasons:

- Some of the most effective attacks on cyber-networks, world-wide currently are directed at exploiting user behavior. These include phishing attacks, social engineering to obtain passwords, and introduction of malware via removable media.
- These threats are especially effective when directed at those with elevated network privileges and/or other elevated cyber responsibilities.
- 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.

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

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? If yes, 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 requiring 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 are provided for correcting weaknesses. (Base)

7.1.6. POA&Ms include security weaknesses discovered during assessments of security controls and requiring 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 and OMB M-04-25). (Base)

7.1.8. Program officials and contractors 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, and 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.

Purpose and Use

These questions are being asked for the following reasons:

- POA&M processes are important as part of the risk management process to track problems and to decide which ones to address.

8. REMOTE ACCESS MANAGEMENT

8.1. Has the Organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, 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 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 800-46, Section 4.2, Section 5.1). (Base)

8.1.4. Telecommuting policy is fully developed (NIST 800-46, Section 5.1). (Base)

8.1.5. If applicable, multi-factor authentication is required for remote access (NIST 800-46, Section 2.2, Section 3.3). (KFM)

8.1.6. Authentication mechanisms meet NIST Special Publication 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 to OMB M-07-16, are timed-out after 30 minutes of inactivity after which re-authentication are required. (Base)

8.1.9. Lost or stolen devices are disabled and appropriately reported (NIST 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 800-53, PL-4). (Base)

8.1.11. Remote access user agreements are adequate in accordance with government policies (NIST 800-46, Section 5.1, NIST 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.

Purpose and Use

These questions are being asked for the following reasons:

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

9. CONTINGENCY PLANNING

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? If yes, 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 800-53: CP-1). (Base)

9.1.2. The Organization has performed an overall Business Impact Analysis (BIA) (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 business continuity and disaster recovery plans are in place and can be implemented when necessary (FCD1, NIST SP 800-34). (Base)

9.1.6. Development and fully implementable of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST 800-53). (Base)

9.1.7. Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans 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 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 consider 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.

Purpose and Use

These questions are being asked for the following reasons:

- Contingency planning deals with risks which occur rarely. 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 which have such significant consequences that they become first-priority risks.

10. CONTRACTOR SYSTEMS

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? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program includes 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 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. (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 public cloud. (Base)

10.1.4. The inventory identifies interfaces between these systems and Organization-operated systems (NIST 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 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.

Purpose and Use

These questions are being asked for the following reasons:

- 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 DAA make an informed decision about whether or not to accept any residual risk?"

11. SECURITY CAPITAL PLANNING

11.1. Has the Organization established a security capital planning and investment program for information security? If yes, 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 800-53: SA-2). (Base)

11.1.4. Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST 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.

Purpose and Use

These questions are being asked for the following reasons:

- 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 ones.