FY 2015

Inspector General

Federal Information Security Modernization Act Reporting Metrics V1.2

Prepared by:

U.S. Department of Homeland Security
Office of Cybersecurity and Communications
Federal Network Resilience

June 19, 2015

Document History

Version	Date	Comments	Author	Sec/Page
0.1	27 Oct 2014	Initial release of FY15 IG annual FISMA metrics	DHS FNR	All
1.1	8 Dec 2014	Incorporation of FAEC Change Requests	DHS FNR	All
1.2	19 June 2015	Added ISCM Maturity Model and Appendix A. Formatting changes throughout.	DHS FNR	All

Table of Contents

GENERAL INSTRUCTIONS 1
1. CONTINUOUS MONITORING MANAGEMENT 6
2. CONFIGURATION MANAGEMENT 11
3. IDENTITY AND ACCESS MANAGEMENT 13
4. INCIDENT RESPONSE AND REPORTING 15
5. RISK MANAGEMENT 17
6. SECURITY TRAINING 19
7. PLAN OF ACTION & MILESTONES (POA&M) 21
8. REMOTE ACCESS MANAGEMENT 22
9. CONTINGENCY PLANNING 24
10. CONTRACTOR SYSTEMS 26
Appendix A: IG ISCM Maturity Model for FY15 FISMA 27
Appendix B: Summary of FISMA CAP Goal Targets & Methodology 32
Appendix C: Definitions 33
Appendix D: Acronyms 41

Table of Tables

Table 1: IG ISCM Maturity Model Definitions 10
Table 2: IG ISCM Maturity Model for FY15 FISMA 31
Table 3: Summary of CAP Goal Target & Methodology 32

GENERAL INSTRUCTIONS

Refer to the General Instructions section of the FY15 CIO Annual Metrics. All of the guidance, definitions, requirements, and best practices from that document apply to the OIG metrics.

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:

    - Information Security Continuous Monitoring - Provide ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity: posture, hygiene, and operational readiness.
    - Identity Credential and Access Management - Implement a set of capabilities that ensure users must authenticate to information technology resources and have access to only those resources that are required for their job function.
    - Anti-phishing and Malware Defense - Implement technologies, processes and training that reduce the risk of malware introduced through email and malicious or compromised web sites.

2. Key FISMA Metrics (KFM): These questions are based on the FISMA regulation and can be found in the following Performance Areas:

    - Incident Response and Reporting
    - Remote Access Management
    - Security Training

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 PERFORMANCE[1]

Administration Priorities

The expected levels of performance for the AP FISMA metrics are based on review and input

[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.

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 United States government(USG)-wide application. The FY15 Q1 and Q2 CIO FISMA metrics were used to establish a baseline to generate a scoring methodology for the CAP goals (See Appendix B: Summary of FISMA CAP Goal Targets and Methodology).

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 2015.

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

For operational information systems, D/As are expected to be in compliance with NIST guidelines within one year of the publication date. D/As must become compliant with any new or updated

materials in revised NIST guidelines within one year of the revision. For information systems under development or for operational systems undergoing significant changes, D/As are expected to be in compliance with the NIST publications immediately upon deployment of the information system. Each D/A should consider its ability to meet this requirement when developing the Plan of Action and Milestones (POA&M).

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 4, is to be followed. This section attempts to clarify that issue. NIST SP 800-53, Revision 4, is the basis for all of the following discussions.

This topic is partially clarified in NIST SP 800-53, Revision 4, itself: "FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, is a mandatory federal standard developed by NIST in response to FISMA. To comply with the federal standard, organizations first determine the security category of their information system in accordance with FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, derive the information system impact level from the security category in accordance with FIPS 200, and then apply the appropriately tailored set of baseline security controls in NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*" (NIST SP 800-53, Rev. 4, p. vi).

However, there is flexibility in the application of the NIST SP 800-53 requirements: "Organizations have flexibility in applying the baseline security controls in accordance with the guidance provided in Special Publication 800-53. This allows organizations to tailor the relevant security control baseline so that it more closely aligns with their mission and business requirements and environments of operation" (NIST SP 800-53, Rev. 4, p. vi).

However, "Organizations have the responsibility to select the appropriate security controls, to implement the controls correctly, and to demonstrate the effectiveness of the controls in satisfying established security requirements" (NIST SP 800-53, Rev. 4, p. 4). 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:

> "The answers to these questions are not given in isolation but rather in the context of an effective risk management process for the organization that identifies, mitigates as deemed necessary, and monitors on an ongoing basis, risks arising from its information and information systems… The security controls defined in this publication and recommended for use by organizations to satisfy their information security requirements should be employed as part of a well-defined risk management process that supports organizational information security programs" (NIST SP 800-53, Rev. 4, p. 1).

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 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 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.
- OMB M-14-03 directs D/As to implement continuous monitoring of security controls as part of a phased approach through FY 2017.
- At the level of the Federal enterprise, the current metrics aim to provide situational awareness as to where agencies stand with implementing and operating continuous monitoring as it is envisioned by NIST SP 800-137, DHS Continuous Diagnostics and Mitigation (CDM), and the Information Security Continuous Monitoring (ISCM) Concept of Operations (ConOps).
- The Joint Continuous Monitoring Working Group (JCMWG) recommends that asset management is one of the first areas where continuous monitoring needs to be developed. Organizations must first know about devices and software (both authorized/managed and unauthorized/unmanaged) before they can manage the devices/software for configuration and vulnerabilities.
- A key goal of ISCM is to make hardware assets harder to exploit through hardware asset management, software asset management, secure configuration management, and vulnerability management.

Development of a Maturity Model to Guide OIG FISMA Reviews

The Information Technology Committee of the Council of Inspectors General on Integrity and Efficiency (CIGIE), in coordination with DHS, OMB, NIST, and other key stakeholders, has developed a maturity model to provide perspective on the overall status of information security within an agency, as well as across agencies. The purpose of the CIGIE maturity model is to (1) summarize the status of agencies' information security programs and their maturity on a 5-level scale, (2) provide transparency to agency CIOs, top management officials, and other interested readers of OIG FISMA reports about what has been accomplished and what still needs to be implemented to improve the information security program to the next maturity level, and (3) help ensure consistency across the OIGs in their annual FISMA reviews. Developing a maturity model is an enormous undertaking; to break this into manageable components, the CIGIE IT Committee started with a maturity model for just the information security continuous monitoring domain for 2015. The CIGIE, in coordination with DHS, OMB, NIST and other key stakeholders, plans to extend the maturity model to other security domains for OIGs to utilize in their 2016 FISMA reviews.

1.1. Utilizing the ISCM maturity model definitions, in conjunction with the attributes outlined in Appendix A, please assess the maturity of the organization's ISCM program along the domains of people, processes, and technology. Provide a maturity level for each of these domains as well as for the ISCM program overall.[2]

IG ISCM Maturity Model Definitions

Level	Definition
1 Ad-hoc	**ISCM program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.** • ISCM activities are performed without the establishment of comprehensive policies, procedures, and strategies developed consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. • ISCM stakeholders and their responsibilities have not been defined and communicated across the organization. • ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. • The organization lacks personnel with adequate skills and knowledge to effectively perform ISCM activities. • The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. • The organization has not identified and defined the ISCM technologies needed in one or more of the following automation areas and relies on manual/procedural methods in instances where automation would be more effective: patch management, license management, information management, software assurance, vulnerability management, event management, malware detection, asset management, configuration management, network management, and incident management. • ISCM activities are not integrated with respect to organizational risk tolerance, the threat environment, and business/mission requirements. • There is no defined process for collecting and considering lessons learned to improve ISCM processes. • The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions.

[2] To reach a particular level of maturity, organizations should meet all of the attributes outlined in Appendix A for that respective level. For instance, to reach a *Level 2* for the *people* domain, an organization should meet attributes 1.2.1 to 1.2.4. Similarly, to reach *Level 2* for the ISCM program overall, organizations should meet attributes 1.2.1 to 1.2.10. When determining the overall maturity level, the lowest common denominator approach shall apply. For instance, if an organization is at *Level 1* for the *people* domain but at Level 3 for both the *processes* and *technology* domains, the overall maturity of the organization's ISCM program would be *Level 1*.

Level	Definition
2 Defined	**The organization has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. However, ISCM policies, procedures, and strategies are not consistently implemented organization-wide.** • ISCM activities are defined and formalized through the establishment of comprehensive ISCM policies, procedures, and strategies developed consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. • ISCM stakeholders and their responsibilities have been defined and communicated across the organization, but stakeholders may not have adequate resources (people, processes, tools) to consistently implement ISCM activities. • ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. • The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization. • The organization has identified and fully defined the ISCM technologies it plans to utilize in the ISCM automation areas. Automated tools are implemented to support some ISCM activities but the tools may not be interoperable. In addition, the organization continues to rely on manual/procedural methods in instances where automation would be more effective. • The organization has defined how ISCM activities will be integrated with respect to organizational risk tolerance, the threat environment, and business/mission requirements. However, the organization does not consistently integrate its ISCM and risk management activities. • The organization has defined its process for collecting and considering lessons learned to make improvements to its ISCM program. Lessons learned are captured but are not shared at an organizational level to make timely improvements. • ISCM information is not always shared with individuals with significant security responsibilities in a timely manner with which to make risk-based decisions.

Level	Definition
3 Consistently Implemented	**In addition to the formalization and definition of its ISCM program (Level 2), the organization consistently implements its ISCM program across the agency. However, qualitative and quantitative measures and data on the effectiveness of the ISCM program across the organization are not captured and utilized to make risk-based decisions consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.** • The ISCM program is consistently implemented across the organization, in accordance with the organization's ISCM policies, procedures, and strategies and NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO CONOPS. • ISCM stakeholders have adequate resources (people, processes, technologies) to effectively accomplish their duties. • The rigor, intensity, scope, and results of ISCM activities are comparable and predictable across the organization. • The organization has standardized and consistently implemented its defined technologies in all of the ISCM automation areas. ISCM tools are interoperable, to the extent practicable. • ISCM activities are fully integrated with organizational risk tolerance, the threat environment, and business/mission requirements. • The organization is consistently capturing and sharing lessons learned on the effectiveness of ISCM processes and activities. Lessons learned serve as a key input to making regular updates to ISCM processes. • ISCM information is shared with individuals with significant security responsibilities in a consistent and timely manner with which to make risk-based decisions and support ongoing system authorizations.
4 Managed and Measurable	**In addition to being consistently implemented (Level 3), ISCM activities are repeatable and metrics are used to measure and manage the implementation of the ISCM program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations.** • Qualitative and quantitative measures on the effectiveness of the ISCM program are collected across the organization and used to assess the ISCM program and make necessary changes. • Data supporting ISCM metrics is obtained accurately, consistently, and in a reproducible format, in accordance with the organization's ISCM policies, procedures, and strategies and NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO CONOPS. • ISCM data is analyzed consistently and collected and presented using standard calculations, comparisons, and presentations. • ISCM metrics are reported to organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities, including situational awareness and risk response. • ISCM metrics provide persistent situational awareness to stakeholders across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations, the organization's infrastructure, and security domains. • ISCM is used to maintain ongoing authorizations of information systems and the environments in which those systems operate, including common controls and keep required system information and data (i.e., System Security Plan Risk Assessment Report, Security Assessment Report, and POA&M) up to date on an ongoing basis

Level	Definition
5 Optimized	**In addition to being managed and measurable (Level 4), the organization's ISCM program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape.** • Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner. • The ISCM program is integrated with strategic planning, enterprise architecture and capital planning and investment control processes. • The ISCM program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact.

Table 1: IG ISCM Maturity Model Definitions

1.2. Please provide any additional information on the effectiveness of the organization's Information Security Continuous Monitoring Management Program that was not noted in the maturity model 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 findings. (Base)

2.1.5. For Windows-based components, USGCB secure configuration settings are fully implemented (when available), and any deviations from USGCB baseline settings are fully documented. (Base)

2.1.6. Documented proposed or actual changes to hardware and software baseline configurations. (Base)

2.1.7. Implemented software assessing (scanning) capabilities (NIST SP 800-53: RA-5, SI-2). (Base)

2.1.8. 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)

2.1.9. Patch management process is fully developed, as specified in organization policy or standards, including timely and secure installation of software patches (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.

2.3. Does the organization have an enterprise deviation[3] handling process and is it integrated with an automated scanning capability.[4] (Base)

2.3.1. Is there a process for mitigating the risk introduced by those deviations? A deviation is an authorized departure from an approved configuration. As such it is not remediated but may require compensating controls to be implemented. (Base)

[3] Deviation from agency-defined baseline configuration in metric 2.1.2
[4] Scanning capability from 2.1.8

3. IDENTITY AND ACCESS MANAGEMENT

Purpose and Use

- 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]
- For more information regarding PIV eligibility, please see the OPM's Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12 here.

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 (HSPD 12, NIST SP 800-53, AC-2). (Base)

3.1.3. 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)

3.1.4. Organization has 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).

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

[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. Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, servers) from those without user accounts (e.g. IP phones, faxes, printers) (Base)

3.1.7. Ensures that accounts are terminated or deactivated once access is no longer required according to organizational policy. (Base)

3.1.8. 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 and the agency Inspector General within established timeframes.[6] (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 correlating incidents. (Base)

[6] Several levels of law enforcement are available to investigate incidents: for example, within the United States, Federal investigatory agencies (e.g., the Federal Bureau of Investigation [FBI] and the U.S. Secret Service), district attorney offices, state law enforcement, and local (e.g., county) law enforcement. Law enforcement agencies in other countries may also be involved, such as for attacks launched from or directed at locations outside the US. In addition, agencies have an Office of Inspector General (OIG) for investigation of violation of the law within each agency The incident response team should become acquainted with its various law enforcement representatives before an incident occurs to discuss conditions under which incidents should be reported to them, how the reporting should be performed, what evidence should be collected, and how it should be collected. (NIST SP 800-61 2.3.4.2)

4.1.7. 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. 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)

5.1.2. 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)

5.1.3. 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)

5.1.4. Has an up-to-date system inventory. (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 and describes how the controls are employed within the information system and its environment of operation. (Base)

5.1.7. Implements the approved set of tailored baseline security controls specified in metric 5.1.6. (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. Information-system-specific risks (tactical), mission/business-specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization. (Base)

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

5.1.12. 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)

5.1.13. Security authorization package contains system security plan, security assessment report, POA&M, accreditation boundaries in accordance with government policies for organization information systems (NIST SP 800-18, 800-37). (Base)

5.1.14. The organization has an accurate and complete inventory of their cloud systems, including identification of FedRAMP approval status.

5.1.15. For cloud systems, the organization can identify the security controls, procedures, policies, contracts, and service level agreements (SLA) in place to track the performance of the Cloud Service Provider (CSP) and manage the risks of Federal program and personal data stored on cloud systems.

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.[7]

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)

6.1.4. 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)

[7] 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.

6.1.5. 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 and provides adequate justification for missed 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 in terms of dollars (NIST SP 800-53: 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: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. Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms. (Base)

8.1.6. Defines and implements encryption requirements for information transmitted across public networks. (KFM)

8.1.7. 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)

8.1.8. Lost or stolen devices are disabled and appropriately reported (NIST SP 800-46, Section 4.3; US-CERT Incident Reporting Guidelines). (Base)

8.1.9. Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4). (Base)

8.1.10. 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. Does the organization have a policy to detect and remove unauthorized (rogue) connections?

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 and Business Process Analysis into the appropriate analysis and strategy development efforts for the organization's Continuity of Operations Plan, Business Continuity Plan, and Disaster Recovery Plan. (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. Alternate processing sites are not subject to the same risks as primary sites. Organization contingency planning program identifies alternate processing sites for systems that require them (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)

9.1.10. Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)

9.1.11. 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 for organization systems and services residing in a 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 other government agencies), including organization systems and services residing in a public, hybrid, or private cloud (Base)

10.1.2. The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and compliant with FISMA requirements, OMB policy, and applicable NIST 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 other government agencies), including organization systems and services residing in public, hybrid, or private 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)

10.2. Please provide any additional information on the effectiveness of the organization's Contractor Systems Program that was not noted in the questions above.

Appendix A: IG ISCM Maturity Model for FY15 FISMA

ISCM Program Maturity Level	Definition	People	Processes	Technology
Level 1 Ad-hoc	**1.1** ISCM program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. .	**1.1.1** ISCM stakeholders and their responsibilities have not been fully defined and communicated across the organization. **1.1.2** The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. Key personnel do not possess knowledge, skills, and abilities to successfully implement an effective ISCM program. **1.1.3** The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions. **1.1.4** The organization has not defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements.	**1.1.5** ISCM processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. **1.1.6** ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. **1.1.7** The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. **1.1.8** The organization has not defined its processes for collecting and considering lessons learned to improve ISCM processes.	**1.1.9** The organization has not identified and defined the ISCM technologies needed in one or more of the following automation areas and relies on manual/procedural methods in instances where automation would be more effective**.** Use of ISCM technologies in the following areas is ad-hoc. -Patch management -License management -Information management -Software assurance -Vulnerability management -Event management -Malware detection -Asset management -Configuration management -Network management -Incident management **1.1.10** The organization has not defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software.

ISCM Program Maturity Level	Definition	People	Processes	Technology
Level 2 Defined	**1.2** The organization has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. However, ISCM policies, procedures, and strategies are not consistently implemented organization-wide.	**1.2.1** ISCM stakeholders and their responsibilities have been defined and communicated across the organization. However, stakeholders may not have adequate resources (people, processes, and technology) to effectively implement ISCM activities. **1.2.2** The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. In addition, the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective ISCM program. **1.2.3** The organization has defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions. However, ISCM information is not always shared with individuals with significant security responsibilities in a timely manner with which to make risk-based decisions. **1.2.4** The organization has defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements**.** However, ISCM activities are not consistently integrated with the organization's risk management program.	**1.2.5** ISCM processes have been fully defined for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. However, these processes are inconsistently implemented across the organization. **1.2.6** ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. **1.2.7** The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization. **1.2.8** The organization has a defined process for capturing lessons learned on the effectiveness of its ISCM program and making necessary improvements. However, lessons learned are not consistently shared across the organization and used to make timely improvements to the ISCM program.	**1.2.9** The organization has identified and fully defined the ISCM technologies it plans to utilize in the following automation areas. In addition, the organization has developed a plan for implementing ISCM technologies in these areas: patch management, license management, information management, software assurance, vulnerability management, event management, malware detection, asset management, configuration management, network management, and incident management. However, the organization has not fully implemented technology is these automation areas and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while automated tools are implemented to support some ISCM activities, the tools may not be interoperable. **1.2.10** The organization has defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. However, the organization does not consistently implement the technologies that will enable it to manage an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software.

ISCM Program Maturity Level	Definition	People	Processes	Technology
Level 3 Consistently Implemented	**1.3** In addition to the formalization and definition of its ISCM program (Level 2), the organization consistently implements its ISCM program across the agency. However, qualitative and quantitative measures and data on the effectiveness of the ISCM program across the organization are not captured and utilized to make risk-based decisions, consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.	**1.3.1** ISCM stakeholders and their responsibilities have been identified and communicated across the organization, and stakeholders have adequate resources (people, processes, and technology) to effectively implement ISCM activities. **1.3.2** The organization has fully implemented its plans to close any gapes in skills, knowledge, and resources required to successfully implement an ISCM program. Personnel possess the required knowledge, skills, and abilities to effectively implement the organization's ISCM program. **1.3.3** ISCM information is shared with individuals with significant security responsibilities in a consistent and timely manner with which to make risk-based decisions and support ongoing system authorizations. **1.3.4** ISCM activities are fully integrated with organizational risk tolerance, the threat environment, and business/mission requirements.	**1.3.5** ISCM processes are consistently performed across the organization in the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. **1.3.6** The rigor, intensity, scope, and results of ISCM activities are comparable and predictable across the organization. **1.3.7** The organization is consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting. ISCM measures provide information on the effectiveness of ISCM processes and activities. **1.3.8** The organization is consistently capturing and sharing lessons learned on the effectiveness of ISCM processes and activities. Lessons learned serve as a key input to making regular updates to ISCM processes.	**1.3.9** The organization has consistently implemented its defined technologies in all of the following ISCM automation areas. ISCM tools are interoperable to the extent practicable. -Patch management -License management -Information management -Software assurance -Vulnerability management -Event management -Malware detection -Asset management -Configuration management -Network management -Incident management **1.3.10** The organization can produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software.

ISCM Program Maturity Level	Definition	People	Processes	Technology
Level 4 Managed & Measurable	**1.4** In addition to being consistently implemented (Level 3), ISCM activities are repeatable and metrics are used to measure and manage the implementation of the ISCM program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations.	**1.4.1** The organization's staff is consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of the organization's ISCM program. **1.4.2** Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the ISCM program. **1.4.3** Staff are assigned responsibilities for developing and monitoring ISCM metrics, as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the ISCM program.	**1.4.4** The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing ISCM. **1.4.5** Data supporting ISCM metrics are obtained accurately, consistently, and in a reproducible format. **1.4.6** The organization is able to integrate metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations and security domains. **1.4.7** The organization uses its ISCM metrics for determining risk response actions including risk acceptance, avoidance/rejection, or transfer. **1.4.8** ISCM metrics are reported to the organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities. **1.4.9** ISCM is used to maintain ongoing authorizations of information systems and the environments in which those systems operate, including common controls and keep required system information and data (i.e., System Security Plan Risk Assessment Report, Security Assessment Report, and POA&M) up to date on an ongoing basis.	**1.4.10** The organization uses technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing ISCM. **1.4.11** The organization's ISCM performance measures include data on the implementation of its ISCM program for all sections of the network from the implementation of technologies that provide standard calculations, comparisons, and presentations. **1.4.12** The organization utilizes a SIEM tool to collect, maintain, monitor, and analyze IT security information, achieve situational awareness, and manage risk.

ISCM Program Maturity Level	Definition	People	Processes	Technology
Level 5 Optimized	**1.5** In addition to being managed and measurable (Level 4), the organization's ISCM program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape.	**1.5.1** The organization's assigned personnel collectively possess a high skill level to perform and update ISCM activities on a near real-time basis to make any changes needed to address ISCM results based on organization risk tolerance, the threat environment, and business/mission requirements.	**1.5.2** The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity and practices. **1.5.3** On a near real-time basis, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner. **1.5.4** The ISCM program is fully integrated with strategic planning, enterprise architecture and capital planning and investment control processes, and other mission/business areas, as appropriate. **1.5.5** The ISCM program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact.	**1.5.6** The organization has institutionalized the implementation of advanced cybersecurity technologies in near real-time. **1.5.7** The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its ISCM program.

Table 2: IG ISCM Maturity Model for FY15 FISMA

Appendix B: Summary of FISMA CAP Goal Targets & Methodology

Appendix B provides a summary of the FISMA CAP Goal Metric Targets and methodology for Information Security Continuous Monitoring (ISCM), Strong Authentication (ICAM), and Anti-Phishing and Malware Defense.

Summary of FISMA CAP Goal Targets & Methodology			
Capability	**Target %**	**FY15 Annual FISMA CIO Metrics**	**Agency Calculation**
Information Security Continuous Monitoring (ISCM)			
Hardware Asset Management	≥ 95%	2.2, 2.3	Both results must be greater than or equal to target
Software Asset Management	≥ 95%	2.6, 2.7	Both results must be greater than or equal to target
Vulnerability and Weakness Management	≥ 95%	2.11	Result must be greater than or equal to target
Secure Configuration Management	≥ 95%	2.10.6	Result must be greater than or equal to target
Identity and Credential Access Management (ICAM)			
Unprivileged Network Users	≥ 85%	3.1.1	Result must be greater than or equal to target
Privileged Network Users	> 85%	3.2.1	Result must be greater than target
Anti-Phishing and Malware Defense			
Anti-Phishing Defense	≥ 90%	4.2, 4.5, 4.6, 4.7, 4.9, 4.13, 8.2.1	Top 5 results must be greater than or equal to target
Malware Defense	≥ 90%	4.3, 4.4, 4.8, 4.11, 6.1.4	Top 3 results must be greater than or equal to target
Blended Defense	≥ 90%	4.1, 4.10, 4.12, 4.14	Top 2 results must be greater than or equal to target

Table 3: Summary of CAP Goal Target & Methodology

Appendix C: 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 Appendix C of the *FY15 CIO Annual FISMA 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.

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.[8]

- **On-demand self-service.** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- **Broad network access.** Capabilities are available over the network[9] and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

[8] All of these must be present to make the service a cloud service.
[9] The network does not necessarily mean the Internet.

- **Resource pooling.** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant[10] model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
- **Rapid elasticity.** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- **Measured service.** Cloud systems automatically control and optimize resource use by leveraging a metering capability[11] 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.

[10] 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.

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

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.

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.

- endpoints[12]
  - servers
  - workstations (desktops)
  - laptops
  - net-books
- mobile devices
  - Blackberry
  - iPhone
  - Android
  - Tablets
- networking devices[13]
  - routers
  - switches
  - gateways, bridges, wireless access points
  - firewalls
  - intrusion detection/prevention systems
  - Network Address Translators (NAT devices)
  - hybrids of these types (e.g. NAT router)
  - load balancers
  - modems

[12] 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.
[13] This list is not meant to be exhaustive, as there are many types of networking devices. If they are connected, they are to be included.

- other communication devices
  - encryptors
  - decryptors
  - VPN
  - alarms and physical access control devices
  - PKI infrastructure[14]
- other input/output devices if they appear with their own address
  - network printers/plotters/copiers/multi-function devices (IP addressable)
  - network fax portals
  - network scanners
  - network accessible storage devices
  - VOIP phones
  - other network input/output devices
- virtual machines that can be addressed[15] 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
- other devices 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]

Hijacking
An attacker taking control of an information system through the exploitation of a vulnerability by using a network connection or physical access.

[14] PKI assets should be counted as constituent assets on networks in which they reside.
[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.

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 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 device
A portable computer device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possess local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and e-readers.

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 account[19] 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.[20]

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

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

[20] 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."

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 two-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.

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 D: 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
D/A	U.S. Government Department or Agency
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
ISCM	Information Security Continuous Monitoring
KFM	Key FISMA Metrics
LAN	Local Area Network
MAN	Metropolitan Area Network
MFD	Multi-function Device
MOU	Memorandum of Understanding

Acronym	Definition
MTIPS	Managed Trusted Internet Protocol Services
NIST	National Institute of Standards and Technology
NAT	Network Address Translators
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