UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF
INSPECTOR GENERAL

August 11, 2016

The Honorable Vanessa Allen Sutherland
Chairperson and Chief Executive Officer
U.S. Chemical Safety and Hazard Investigation Board
1750 Pennsylvania Avenue, NW, Suite 910
Washington, D.C. 20006

Dear Ms. Sutherland:

The Office of Inspector General (OIG) for the U.S. Environmental Protection Agency plans to begin fieldwork for an audit of the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) compliance with the Federal Information Security Modernization Act of 2014 (FISMA). This project is mandated under FISMA.

The purpose of this letter is to confirm our mutual understanding of the objective and scope of the audit, as well as responsibilities of the CSB and the OIG during the project. The OIG plans to conduct its work at CSB headquarters in Washington, D.C. The project will be conducted using applicable generally accepted government auditing standards. The anticipated benefit of this project is to help CSB improve its business practices and accountability.

The audit objective is to assess the CSB's compliance with FISMA for fiscal year 2016. Specifically, the OIG will:

- Follow up on the status of prior-year audit recommendations.

- Document and selectively test CSB security practices related to performance measures, as outlined in the FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics V1.1, dated July 29, 2016.

We will contact you to arrange a mutually agreeable time to discuss the audit scope and objective. We would also be particularly interested in any areas of concern that you may have. We will answer any of your questions about the project process, reporting procedures, methods used to gather and analyze data, and what we should expect of each other during the course of the project.

During the audit, we will provide updates on a regular basis by email and/or during meetings with CSB staff. To ensure the success and timely completion of this project, please provide the OIG with the information listed on the "Request for Information" enclosure by August 30, 2016.

We respectfully note that the OIG is authorized by the Inspector General Act of 1978 (5 U.S.C. App 3) to have timely access to personnel and all materials necessary to complete its objectives. We will request your resolution if an agency employee or contractor refuses to provide requested records to the OIG, or otherwise fails to cooperate with the OIG. We may report unresolved access matters to the appropriate CSB officials and include the incident in the Semiannual Report to Congress.

If you or your staff have any questions, please contact me at (202) 566-0893 or brevard.rudy@epa.gov; or Charles M. Dade, Project Manager, at (202) 566-2575 or dade.chuck@epa.gov

Sincerely,

Rudolph M. Brevard

Rudolph M. Brevard, Director
Information Resources Management Audits

Enclosures
1. Request for Information
2. Copy of the FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics V1.1, dated July 29, 2016

cc: Kristen Kulinowski, Ph.D., Board Member, CSB
Manuel Ehrlich, Board Member, CSB
Rick Engler, Board Member, CSB
Anna Brown, Director of Administration and Audit Liaison, CSB
Allen Smith, Deputy Director of Administration, CSB
Hillary Cohen, Communications Manager, CSB
Charlie Bryant, Chief Information Officer, CSB
Ron LaRoche, Deputy Chief Information Officer, CSB
Nic Grzegozewski, Agency Follow-Up Coordinator
Frank Benenati, Associate Administrator for Public Affairs
Melissa Harrison, Press Secretary, Office of Public Affairs
Arthur A. Elkins Jr., Inspector General
Charles Sheehan, Deputy Inspector General
Alan Larsen, Counsel to the Inspector General
Kevin Christensen, Assistant Inspector General for Audit
Carolyn Copper, Assistant Inspector General for Program Evaluation
Patrick Sullivan, Assistant Inspector General for Investigations
Edward Shields, Acting Assistant Inspector General for Management
Richard Eyermann, Deputy Assistant Inspector General for Audit
Jennifer Kaplan, Deputy Assistant Inspector General for Congressional and Public Affairs
Jeffrey Lagda, Congressional and Media Liaison, Office of Inspector General

Enclosure 1

Request for Information

Information Requested for the Fiscal Year 2016 CSB Audit for Compliance With the Federal Information Security Modernization Act of 2014

Please provide the following information in electronic format as soon as possible, but no later than August 30, 2016:

1. The CSB's self-assessment for the Risk Management, Contractor System, Configuration Management, Identity and Access Management, Security and Privacy Training, Incident Response Program Maturity Model (for Levels 1 and 2), and Contingency Planning.

2. For questions answered with "Yes," in the self-assessment, please provide supporting documentation. For questions answered with "No" in the self-assessment, please include comments explaining the response.

3. Provide an updated corrective action plan for all open information security audit recommendations outlined in chapters 2 and 3 of OIG Report 16-P-0035, dated November 5, 2015. If corrective actions have been completed, please provide supporting documentation.

4. For the Information Security Continuous Monitoring (ISCM) section, please verify whether responses from the FY 2015 FISMA for this area are still applicable for FY 2016. If the responses are still applicable, please let us know whether any significant changes occurred. If there have been any significant changes in the ISCM area, please provide an updated response and an explanation of what has changed.

Enclosure 2

FY 2016

Inspector General

Federal Information Security Modernization Act of 2014 Reporting Metrics

V1.1

July 29, 2016

Document History

Version	Date	Comments	Sec/Page
1.0	19 June 2016	Aligned questions with CIO FISMA metrics.	All
1.1	29 July 2016	Updated scoring methodology.	All

Contents

GENERAL INSTRUCTIONS

Overview and Purpose

The Federal Information Security Modernization Act of 2014 (FISMA) requires the Inspectors General (IG) to conduct an annual independent evaluation to determine the effectiveness of the information security program and practices of their respective agency. These evaluations (a) test the effectiveness of information security policies, procedures, and practices of a subset of agency information systems, and (b) assess the effectiveness of an agency's information security policies, procedures, and practices. Accordingly, this document captures the fiscal year (FY) 2016 IG metrics and guidance for evaluating the effectiveness of agencies' information security programs and practices in accordance with FISMA.

Reporting Deadline

The due date for each agency's IG to submit its annual assessment to the Office of Management and Budget (OMB) through CyberScope is **Thursday, November 10, 2016**.

Methodology

OMB, the Department of Homeland Security (DHS), and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed the FY 2016 IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officer (CIO) Council. As with the FY 2016 CIO FISMA Reporting Metrics, the IG metrics are organized around the five information security functions outlined in the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks, as highlighted in **Table 1**.

Table 1. Aligning the Cybersecurity Framework Security Functions to the FY 2016 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2016 IG FISMA Metric Domains
Identify	Risk Management and Contractor Systems
Protect	Configuration Management, Identity and Access Management, and Security and Privacy Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

OMB, DHS, and CIGIE established a joint working group to develop the FY 2016 IG FISMA Reporting Metrics. The working group consolidated and reformatted the FY 2015 IG FISMA Reporting Metrics to facilitate greater consistency and comparability across IG FISMA

evaluations. The working group also added metrics to gauge agencies' progress in implementing the Administration's Cybersecurity Cross Agency Priority Goal as well as cybersecurity best practices and actions in support of the 30-Day Cybersecurity Sprint, the Cybersecurity Strategy and Implementation Plan, and the Cybersecurity Framework.

In addition to these key performance areas, the IG FISMA metrics assess the effectiveness of an agency's information security program. The IG FISMA metrics leverage NIST *Special Publication 800-53, Rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations,"* which defines security control effectiveness as the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing/mediating established security policies. To determine the effectiveness of an agency's information security program in a specific function area, IGs should consider additional attributes and best practices based on the unique missions and risks identified by their respective agencies. Accordingly, each function area includes metrics and additional questions to ascertain the level of testing performed by IGs, other attributes IGs may have considered to determine effectiveness, and the extent to which each agency's program is effective given the risks it faces.

Maturity Models for Information Security Continuous Monitoring and Incident Response

The purpose of the CIGIE maturity models 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 IG FISMA reports regarding what has been accomplished and what still needs to be implemented to improve the information security program, and (3) help ensure consistency across the IGs in their annual FISMA reviews. Within the maturity model context, agencies should perform a risk assessment and identify the optimal maturity level that achieves cost-effective security based on their missions and risks faced. All things being equal, Level 4, *Managed and Measurable*, represents an effective information security program.

In 2015, the CIGIE, in coordination with DHS, OMB, NIST, and other key stakeholders, undertook an effort to develop a maturity model to provide perspective on the overall status of ISCM within a given agency, as well as across agencies. Developing a maturity model is an enormous undertaking, and the CIGIE determined the process would be best served by breaking it into manageable components. In 2015, a maturity model was developed for the Information Security Continuous Monitoring domain, a key focus area for the Administration.

The FY 2016 IG FISMA Reporting Metrics continue the effort begun in 2015 with the development of an Incident Response maturity model, another area viewed as critical given the increasing threats to agency networks, systems, and data. The CIGIE, in coordination with DHS, OMB, and other key stakeholders, plans to extend the maturity model to other security domains for IGs to utilize in their FY 2017 FISMA reviews. In the meantime, however, metrics for those domains without an established maturity model are mapped to Maturity Model Indicators. These indicators will act as a stepping-stone, allowing IGs to reach preliminary conclusions similar to those achievable with a fully developed model.

Scoring

Agencies are allotted points for each Cybersecurity Framework Function area based on their achievement of various levels of maturity. For each Framework Function, a total of 20 points is possible. The point allotment for each level of maturity is provided in **Table 2**.

Table 2. Level of Maturity Point Allotment

Maturity Level	Scoring Description	Scoring Distribution
Level 1: Ad-hoc	Has not met all metrics designated "Defined"	3 points
Level 2: Defined	Met all metrics designated "Defined"	4 points
Level 3: Consistently Implemented	Met all metrics designated "Consistently Implemented"	6 points
Level 4: Managed and Measureable	For Identify, Protect, and Recover functions: Met half or greater of the metrics designated "Managed and Measureable" For Detect and Respond Maturity Models: Met all metrics in the Managed and Measurable section	5 points
Level 5: Optimized	For Identify, Protect, and Recover functions: Met all metrics designated "Managed and Measureable" For Detect and Respond Maturity Models: Met all metrics in the Optimized section	2 points

Due to the different models being used in the FY 2016 IG FISMA assessment, questions are distributed differently based on whether the function area utilizes a full maturity model (Detect and Respond) or maturity model indicators (Identify, Protect, and Recover). For those function areas that utilize a full maturity model, there are questions associated with each level. For those function areas that rely on maturity model indicators, however, the scoring distribution focuses on the *Defined*, *Consistently Implemented*, and *Managed and Measurable* maturity levels. Regardless of the model utilized, IGs must provide narrative responses in the comments field for any metrics rated as not met. IGs may also provide optional responses for any metrics rated as met. Agencies with programs that score at or above the Managed and Measureable for a NIST Framework Function have “effective” programs within that area in accordance effectiveness definition in NIST SP 800-53, Rev. 4, discussed above. The total FY 2016 IG FISMA reporting metrics score will be the total of an agency’s scores in all of the Framework functions.

FY 2016 IG FISMA Metric Domains

1.0 Identify

Maturity Model Indicator	Risk Management (Identify)
Defined	1.1 Has the organization established a risk management program that includes comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?
Defined	1.1.1 Identifies and maintains an up-to-date system inventory, including organization- and contractor-operated systems, hosting environments, and systems residing in the public, hybrid, or private cloud. (2016 CIO FISMA Metrics, 1.1; NIST Cybersecurity Framework (CF) ID.AM.1, NIST 800-53: PM-5)
Consistently Implemented	1.1.2 Develops a risk management function that is demonstrated through the development, implementation, and maintenance of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1. (NIST SP 800-39)
Consistently Implemented	1.1.3 Incorporates mission and business process-related risks into risk-based decisions at the organizational perspective, as described in NIST SP 800-37, Rev. 1. (NIST SP 800-39)
Consistently Implemented	1.1.4 Conducts information system level risk assessments that integrate risk decisions from the organizational and mission/business process perspectives and take into account threats, vulnerabilities, likelihood, impact, and risks from external parties and common control providers. (NIST SP 800-37, Rev. 1, NIST SP 800-39, NIST SP 800-53: RA-3)
Managed and Measurable	1.1.5 Provides timely communication of specific risks at the information system, mission/business, and organization-level to appropriate levels of the organization.
Consistently Implemented	1.1.6 Performs comprehensive assessments to categorize information systems in accordance with Federal standards and applicable guidance. (FIPS 199, FIPS 200, FISMA, Cybersecurity Sprint, OMB M-16-04, President's Management Council (PMC) cybersecurity assessments)
Defined	1.1.7 Selects an appropriately tailored set of baseline security controls based on mission/business requirements and policies and develops procedures to employ controls within the information system and its environment of operation.
Consistently Implemented	1.1.8 Implements the tailored set of baseline security controls as described in 1.1.7.
Managed and Measurable	1.1.9 Identifies and manages risks with system interconnections, including through authorizing system interconnections, documenting interface characteristics and security requirements, and maintaining interconnection security agreements. (NIST SP 800-53: CA-3)
Consistently Implemented	1.1.10 Continuously assesses the security controls, including hybrid and shared 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.
Managed and Measurable	1.1.11 Maintains ongoing information system authorizations 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 (OMB M-14-03, NIST Supplemental Guidance on Ongoing Authorization).
Managed and Measureable	1.1.12 Security authorization package contains system security plan, security assessment report, and POA&M that are prepared and maintained in accordance with government policies. (SP 800-18, SP 800-37)
Consistently Implemented	1.1.13 POA&Ms are maintained and reviewed to ensure they are effective for correcting security weaknesses.
Managed and Measured	1.1.14 Centrally tracks, maintains, and independently reviews/validates POA&M activities at least quarterly. (NIST SP 800-53 :CA-5; OMB M-04-25)

Maturity Model Indicator	Risk Management (Identify)
Managed and Measurable	1.1.15 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.
Consistently Implemented	1.1.16 Implemented an insider threat detection and prevention program, including the development of comprehensive policies, procedures, guidance, and governance structures, in accordance with Executive Order 13587 and the National Insider Threat Policy. (PMC; NIST SP 800-53: PM-12)
	1.1.17 Provide any additional information on the effectiveness (positive or negative) of the organization's Risk Management program that was not noted in the questions above. Based on all testing performed, is the Risk Management program effective?

Maturity Model Indicator	Contractor Systems (Identify)
Defined	1.2 Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including other government agencies, managed hosting environments, and systems and services residing in a cloud external to the organization that is inclusive of policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?
Consistently Implemented	1.2.1 Establishes and implements a process to ensure that contracts/statements of work/solicitations for systems and services, include appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information. (FAR Case 2007-004, Common Security Configurations, FAR Sections 24.104, 39.101, 39.105, 39.106, 52.239-1; PMC, 2016 CIO Metrics 1.8, NIST 800-53, SA-4 FedRAMP standard contract clauses; Cloud Computing Contract Best Practices)
Consistently Implemented	1.2.2 Specifies within appropriate agreements how information security performance is measured, reported, and monitored on contractor- or other entity-operated systems. (CIO and CAO Council Best Practices Guide for Acquiring IT as a Service, NIST SP 800-35)
Consistently Implemented	1.2.3 Obtains sufficient assurance that the security controls of systems operated on the organization’s behalf by contractors or other entities and services provided on the organization’s behalf meet FISMA requirements, OMB policy, and applicable NIST guidelines. (NIST SP 800-53: CA-2, SA-9)
	1.2.4 Provide any additional information on the effectiveness (positive or negative) of the organization's Contractor Systems Program that was not noted in the questions above. Based on all testing performed, is the Contractor Systems Program effective?

2.0 Protect

Maturity Model Indicator	Configuration Management (Protect)
Defined	2.1. Has the organization established a configuration management program that is inclusive of comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?
Defined	2.1.1 Develops and maintains an up-to-date inventory of the hardware assets (i.e., endpoints, mobile assets, network devices, input/output assets, and SMART/NEST devices) connected to the organization's network with the detailed information necessary for tracking and reporting. (NIST CF ID.AM-1; 2016 CIO FISMA Metrics 1.5, 3.17; NIST 800-53: CM-8)
Defined	2.1.2 Develops and maintains an up-to-date inventory of software platforms and applications used within the organization and with the detailed information necessary for tracking and reporting. (NIST 800-53: CM-8, NIST CF ID.AM-2)
Consistently Implemented	2.1.3 Implements baseline configurations for IT systems that are developed and maintained in accordance with documented procedures. (NIST SP 800-53: CM-2; NIST CF PR.IP-1)
Consistently Implemented	2.1.4 Implements and maintains standard security settings (also referred to as security configuration checklists or hardening guides) for IT systems in accordance with documented procedures. (NIST SP 800-53: CM-6; CIO 2016 FISMA Metrics, 2.3)
Managed and Measurable	2.1.5 Assesses configuration change control processes, including processes to manage configuration deviations across the enterprise that are implemented and maintained. (NIST SP 800-53: CM-3, NIST CF PR.IP-3)
Managed and Measurable	2.1.6 Identifies and documents deviations from configuration settings. Acceptable deviations are approved with business justification and risk acceptance. Where appropriate, automated means that enforce and redeploy configuration settings to systems at regularly scheduled intervals are deployed, while evidence of deviations is also maintained. (NIST SP 800-53: CM-6, Center for Internet Security Controls (CIS) 3.7)
Managed and Measurable	2.1.7 Implemented SCAP certified software assessing (scanning) capabilities against all systems on the network to assess both code-based and configuration-based vulnerabilities in accordance with risk management decisions. (NIST SP 800-53: RA-5, SI- 2; CIO 2016 FISMA Metrics 2.2, CIS 4.1)
Consistently Implemented	2.1.8 Remediates configuration-related vulnerabilities, including scan findings, in a timely manner as specified in organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2)
Managed and Measurable	2.1.9 Develops and implements a patch management process in accordance with organization policy or standards, including timely and secure installation of software patches. (NIST SP 800-53: CM-3, SI-2, OMB M-16-04, DHS Binding Operational Directive 15-01)
	2.1.10 Provide any additional information on the effectiveness (positive or negative) of the organization's Configuration Management Program that was not noted in the questions above. Based on all testing performed, is the Configuration Management Program effective?

Maturity Model Indicator	Identity and Access Management (Protect)
Defined	2.2 Has the organization established an identity and access management program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?
Consistently Implemented	2.2.1 Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements, participate in required training prior to being granted access, and recertify access agreements on a predetermined interval. (NIST 800-53: PL-4, PS-6)
Consistently Implemented	2.2.2 Ensures that all users are only granted access based on least privilege and separation-of-duties principles.
Consistently Implemented	2.2.3 Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, servers) from those without user accounts (e.g. networking devices, such as load balancers and intrusion detection/prevention systems, and other input/output devices such as faxes and IP phones).
Consistently Implemented	2.2.4 Implements 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)
Consistently Implemented	2.2.5 Implements PIV or a NIST Level of Assurance (LOA) 4 credential for logical access by all privileged users (system, network, database administrators, and others responsible for system/application control, monitoring, or administration functions). (Cybersecurity Sprint, OMB M-16-04, PMC, 2016 CIO FISMA Metrics 2.5.1)
Consistently Implemented	2.2.6 Enforces PIV or a NIST LOA 4 credential for logical access for at least 85% of non-privileged users. (Cybersecurity Sprint, OMB M-16-04, PMC, 2016 CIO FISMA Metrics 2.4.1)
Managed and Measurable	2.2.7 Tracks and controls the use of administrative privileges and ensures that these privileges are periodically reviewed and adjusted in accordance with organizationally defined timeframes. (2016 CIO FISMA Metrics 2.9, 2.10; OMB M-16-04, CIS 5.2)
Managed and Measurable	2.2.8 Ensures that accounts are terminated or deactivated once access is no longer required or after a period of inactivity, according to organizational policy.
Consistently Implemented	2.2.9 Identifies, limits, and controls the use of shared accounts. (NIST SP 800-53: AC-2)
Consistently Implemented	2.2.10 All users are uniquely identified and authenticated for remote access using Strong Authentication (multi-factor), including PIV. (NIST SP 800-46, Section 4.2, Section 5.1, NIST SP 800-63)
Consistently Implemented	2.2.11 Protects against and detects unauthorized remote access connections or subversion of authorized remote access connections, including through remote scanning of host devices. (CIS 12.7, 12.8, FY 2016 CIO FISMA metrics 2.17.3, 2.17.4, 3.11, 3.11.1)
Managed and Measurable	2.2.12 Remote access sessions are timed-out after 30 minutes of inactivity, requiring user re-authentication, consistent with OMB M-07-16, .
Consistently Implemented	2.2.13 Enforces a limit of consecutive invalid remote access logon attempts and automatically locks the account or delays the next logon prompt. (NIST 800-53: AC-7)
Consistently Implemented	2.2.14 Implements a risk-based approach to ensure that all agency public websites and services are accessible through a secure connection through the use and enforcement of https and strict transport security. (OMB M-15-13)
	2.2.15 Provide any additional information on the effectiveness (positive or negative) of the organization's Identity and Access Management Program that was not noted in the questions above. Based on all testing performed is the Identity and Access Management Program effective?

Maturity Model Indicator	Security and Privacy Training (Protect)
Defined	2.3 Has the organization established a security and privacy awareness and training program, including comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?
Consistently Implemented	2.3.1 Develops training material for security and privacy awareness training containing appropriate content for the organization, including anti-phishing, malware defense, social engineering, and insider threat topics. (NIST SP 800-50, 800-53: AR-5, OMB M-15-01, 2016 CIO Metrics, PMC, National Insider Threat Policy (NITP))
Consistently Implemented	2.3.2 Evaluates the skills of individuals with significant security and privacy responsibilities and provides additional security and privacy training content or implements human capital strategies to close identified gaps. (NIST SP 800-50)
Consistently Implemented	2.3.3 Identifies and tracks status of security and privacy awareness training for all information system users (including employees, contractors, and other organization users) requiring security awareness training with appropriate internal processes to detect and correct deficiencies. (NIST 800-53: AT-2)
Consistently Implemented	2.3.4 Identifies and tracks status of specialized security and privacy training for all personnel (including employees, contractors, and other organization users) with significant information security and privacy responsibilities requiring specialized training.
Managed and Measureable	2.3.5 Measures the effectiveness of its security and privacy awareness and training programs, including through social engineering and phishing exercises. (PMC, 2016 CIO FISMA Metrics 2.19, NIST SP 800-50, NIST SP 800-55)
	2.3.6 Provide any additional information on the effectiveness (positive or negative) of the organization's Security and Privacy Training Program that was not noted in the questions above. Based on all testing performed is the Security and Privacy Training Program effective?

3.0 Detect

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	**2.1** 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. .	**2.1.1** 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. **2.1.2** 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 **2.1.3** 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. **2.1.4** 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.	**2.1.5** 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. **2.1.6** ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. **2.1.7** 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. **2.1.8** 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.	**2.1.9** 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. **2.1.10** 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	**3.1**. 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.	**3.1.1** 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. **3.1.2** 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. **3.1.3** 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. **3.1.4** ISCM activities are fully integrated with organizational risk tolerance, the threat environment, and business/mission requirements.	**3.1.5** 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. **3.1.6** The rigor, intensity, scope, and results of ISCM activities are comparable and predictable across the organization. **3.1.7** 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. **3.1.8** 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. **3.1.9** The rigor, intensity, scope, and results of incident response activities (i.e. preparation, detection, analysis, containment, eradication, and recovery, reporting and post incident) are comparable and predictable across the organization.	**3.1.10** 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. **3.1.11** 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 and Measurable	**4.1** 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. .	**4.1.1** 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. **4.1.2** Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the ISCM program. **4.1.3** 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.	**4.1.4** 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. **4.1.5** Data supporting ISCM metrics are obtained accurately, consistently, and in a reproducible format. **4.1.6** 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. **4.1.7** The organization uses its ISCM metrics for determining risk response actions including risk acceptance, avoidance/rejection, or transfer. **4.1.8** ISCM metrics are reported to the organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities. **4.1.9** 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	**4.1.10** 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. **4.1.11** 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. **4.1.12** 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	**5.1** 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.	**5.1.1** 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.	**5.1.2** The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity and practices. **5.1.3** 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. **5.1.4** 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. **5.1.5** The ISCM program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact.	**5.1.6** The organization has institutionalized the implementation of advanced cybersecurity technologies in near real-time. **5.1.7** The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its ISCM program.

4.0 Respond

Incident Response Program Maturity Level	Definition	People	Processes	Technology
Level 1 Ad-hoc	**1.1** Incident response program is not formalized and incident response 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 FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines). .	**1.1.1** Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have not been fully defined and communicated across the organization, including the designation of a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities. **1.1.2** The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response program. Key personnel do not possess the knowledge, skills, and abilities to successfully implement an effective incident response program. **1.1.3** The organization has not defined a common threat vector taxonomy and defined how incident response information will be shared with individuals with significant security responsibilities and other stakeholders, and used to make timely, risk-based decisions. **1.1.4** The organization has not defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate.	**1.1.5** Incident response processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting to internal and external stakeholders using standard data elements and impact classifications within timeframes established by US-CERT. **1.1.6** The organization has not fully defined how it will collaborate with DHS and other parties, as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents. **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 incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk. **1.1.8** The organization has not defined its processes for collecting and considering lessons learned and incident data to improve security controls and incident response processes.	**1.1.9** The organization has not identified and defined the incident response technologies needed in one or more of the following areas and relies on manual/procedural methods in instances where automation would be more effective**.** Use of incident response technologies in the following areas is ad-hoc. - Web application protections, such as web application firewalls Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools -Aggregation and analysis, such as security information and event management (SIEM) products -Malware detection, such as anti-virus and antispam software technologies - Information management, such as data loss prevention -File integrity and endpoint and server security tools **1.1.10** The organization has not defined how it will meet the defined Trusted Internet Connection (TIC) security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. **1.1.11** The organization has not defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving the organization's networks. **1.1.12** The organization has not defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems.

Incident Response Program Maturity Level	Definition	People	Processes	Technology
Level 2 Defined	**2.1** The organizational has formalized its incident response program through the development of comprehensive incident response policies, plans, and procedures consistent with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines). However, incident response policies, plans, and procedures are not consistently implemented organization-wide. .	**2.1.1** Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have been fully defined and communicated across the organization, including the designation of a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities. However, stakeholders may not have adequate resources (people, processes, and technology) to effectively implement incident response activities. Further, the organization has not verified roles and responsibilities as part of incident response testing. **2.1.2** The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response 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 incident response program.	**2.1.5** Incident response processes have been fully defined for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting using standard data elements and impact classifications within timeframes established by US-CERT. However, these processes are inconsistently implemented across the organization. **2.1.6** The organization has fully defined, but not consistently implemented, its processes to collaborate with DHS and other parties as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents. **2.1.7** The organization has identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization. **2.1.8** The organization has defined its processes for collecting and considering lessons learned and incident data to improve security controls and incident response processes. However, lessons learned are not consistently captured and shared across the organization and used to make timely improvements to security controls and the incident response program.	**2.1.9** The organization has identified and fully defined the incident response technologies it plans to utilize in the following areas. - Web application protections, such as web application firewalls Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools -Aggregation and analysis, such as security information and event management (SIEM) products. However, the organization has not ensured that security and event data are aggregated and correlated from all relevant sources and sensors. -Malware detection such as Anti-virus and antispam software technologies - Information management such as data loss prevention - File integrity and endpoint and server security tools However, the organization has not fully implemented technologies in these areas and continues to rely on manual/procedural methods in instances where automation would be more effective**.** In addition, while tools are implemented to support some incident response activities, the tools are not interoperable to the extent practicable, do not cover all components of the organization's network, and/or have not been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, plans, and procedures.

Incident Response Program Maturity Level	Definition	People	Processes	Technology
		2.1.3 The organization has defined a common threat vector taxonomy and defined how incident response information will be shared with individuals with significant security responsibilities and other stakeholders, and used to make timely, risk-based decisions. However, the organization does not consistently utilize its threat vector taxonomy and incident response information is not always shared with individuals with significant security responsibilities and other stakeholders in a timely manner. **2.1.4** The organization has defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. However, incident response activities are not consistently integrated with these areas.		**2.1.10** The organization has defined how it will meet the defined TIC security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. However, the organization has not ensured that the TIC 2.0 provider and agency managed capabilities are consistently implemented. **2.1.11** The organization has defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving its networks. **2.1.12** The organization has defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems. However, the organization has not established, and does not consistently maintain, a comprehensive baseline of network operations and expected data flows for users and systems.

Incident Response Program Maturity Level	Definition	People	Processes	Technology
Level 3 Consistently Implemented	**3.1**. In addition to the formalization and definition of its incident response program (Level 2), the organization consistently implements its incident response program across the agency, in accordance with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines). However, data supporting metrics on the effectiveness of the incident response program across the organization are not verified, analyzed, and correlated.	**3.1.1** Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have been fully defined, communicated, and consistently implemented across the organization (Level 2). Further, the organization has verified roles and responsibilities of incident response stakeholders as part of incident response testing. **3.1.2** The organization has fully implemented its plans to close any gaps in the skills, knowledge, and resources needed to effectively implement its incident response program. Incident response teams are periodically trained to ensure that knowledge, skills, and abilities are maintained. **3.1.3** The organization consistently utilizes its defined threat vector taxonomy and shares information with individuals with significant security responsibilities and other stakeholders in a timely fashion to support risk-based decision making. **3.1.4** Incident response activities are integrated with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate.	**3.1.5** Incident response processes are consistently implemented across the organization for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting using standard data elements and impact classifications within timeframes established by US-CERT. **3.1.6** The organization has ensured that processes to collaborate with DHS and other parties as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents are implemented consistently across the organization. **3.1.7** The organization is consistently capturing qualitative and quantitative performance metrics on the performance of its incident response program. However, the organization has not ensured that the data supporting the metrics was obtained accurately and in a reproducible format or that the data is analyzed and correlated in ways that are effective for risk management. **3.1.8** The organization is consistently collecting and capturing lessons learned and incident data on the effectiveness of its incident response program and activities. However, lessons learned may not be shared across the organization in a timely manner and used to make timely improvements to the incident response program and security measures.	**3.1.10** The organization has consistently implemented its defined incident response technologies in the following areas. - Web application protections, such as web application firewalls Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools -Aggregation and analysis, such as security information and event management (SIEM) products. The organization ensures that security and event data are aggregated and correlated from all relevant sources and sensors. -Malware detection such as Anti-virus and antispam software technologies - Information management such as data loss prevention - File integrity and endpoint and server security tools In addition, the tools are interoperable to the extent practicable, cover all components of the organization's network, and have been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, procedures, and plans. **3.1.11** The organization has consistently implemented defined TIC security controls and implemented actions to ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. **3.1.12** The organization is utilizing DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving their networks.

Incident Response Program Maturity Level	Definition	People	Processes	Technology
			3.1.9 The rigor, intensity, scope, and results of incident response activities (i.e. preparation, detection, analysis, containment, eradication, and recovery, reporting and post incident) are comparable and predictable across the organization.	**3.1.13** The organization has fully implemented technologies to develop and maintain a baseline of network operations and expected data flows for users and systems.

Incident Response Program Maturity Level	Definition	People	Processes	Technology
Level 4 Managed and Measurable	**4.1** In addition to being consistently implemented (Level 3), incident response activities are repeatable and metrics are used to measure and manage the implementation of the incident response program, achieve situational awareness, and control ongoing risk. In addition, the incident response program adapts to new requirements and government-wide priorities. .	**4.1.1** Incident response stakeholders are consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and are collecting, analyzing, and reporting data on the effectiveness of the organization's incident response program. **4.1.2** Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the incident response program. **4.1.3** Incident response stakeholders are assigned responsibilities for developing and monitoring incident response 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 incident response program.	**4.1.4** 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 incident response. **4.1.5** Data supporting incident response measures and metrics are obtained accurately, consistently, and in a reproducible format. **4.1.6** Incident response data, measures, and metrics are analyzed, collected, and presented using standard calculations, comparisons, and presentations **4.1.7** Incident response metrics are reported to organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities.	**4.1.8** 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 incident response activities. **4.1.9** The organization's incident response performance measures include data on the implementation of its incident response program for all sections of the network.

Incident Response Program Maturity Level	Definition	People	Processes	Technology
Level 5 Optimized	**5.1** In addition to being managed and measurable (Level 4), the organization's incident response 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	**5.1.1** The organization's assigned personnel collectively possess a high skill level to perform and update incident response activities on a near real-time basis to make any changes needed to address incident response results based on organization risk tolerance, the threat environment, and business/mission requirements.	**5.1.2** The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity practices. **5.1.3** On a near real-time basis, the organization actively adapts its incident response program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a near real-time manner. **5.1.4** The incident response program is fully integrated with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. **5.1.5** The incident response program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact.	**5.1.6** The organization has institutionalized the implementation of advanced incident response technologies in near real-time. **5.1.7** The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its incident response program **5.1.8** The organization uses simulation based technologies to continuously determine the impact of potential security incidents to its IT assets and adjusts incident response processes and security measures accordingly.

5.0 Recover

Maturity Model Indicator	Contingency Planning (Recover)
Defined	5.1 Has the organization established an enterprise-wide business continuity/disaster recovery program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?
Consistently Implemented	5.1.1 Develops and facilitates recovery testing, training, and exercise (TT&E) programs. (FCD1, NIST SP 800-34, NIST SP 800-53)
Consistently Implemented	5.1.2 Incorporates the system's Business Impact Analysis and Business Process Analysis into analysis and strategy toward development of the organization's Continuity of Operations Plan, Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP). (NIST SP 800-34)
Consistently Implemented	5.1.3 Develops and maintains documented recovery strategies, plans, and procedures at the division, component, and IT infrastructure levels. (NIST SP 800-34)
Consistently Implemented	5.1.4 BCP and DRP are in place and ready to be executed upon if necessary. (FCD1, NIST SP 800-34, 2016 CIO FISMA Metrics 5.3, PMC)
Managed and Measureable	5.1.5 Tests BCP and DRP for effectiveness and updates plans as necessary. (2016 CIO FISMA Metrics, 5.4)
Consistently Implemented	5.1.6 Tests system-specific contingency plans, in accordance with organizationally defined timeframes, to determine the effectiveness of the plans as well as readiness to execute the plans if necessary. (NIST SP 800-53: CP-4)
Managed and Measureable	5.1.7 Develops after-action reports that address issues identified during contingency/disaster recovery exercises in order to improve contingency/disaster recovery processes. (FCD1, NIST SP 800-34)
Consistently Implemented	5.1.8 Determines alternate processing and storage sites based upon risk assessments which ensure the potential disruption of the organization's ability to initiate and sustain operations is minimized, and are not subject to the same physical and/or cybersecurity risks as the primary sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-6, CP-7)
Managed and Measurable	5.1.9 Conducts backups of information at the user- and system-levels and protects the confidentiality, integrity, and availability of backup information at storage sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-9, NIST CF, PR.IP-4, NARA guidance on information systems security records)
Defined	5.1.10 Contingency planning that considers supply chain threats.
	5.1.11 Provide any additional information on the effectiveness (positive or negative) of the organization's Contingency Planning Program that was not noted in the questions above. Based on all testing performed is the Contingency Planning Program effective?