Memorandum from the Office of the Inspector General

December 21, 2017

Scott D. Self, SP 3A-C

REQUEST FOR MANAGEMENT DECISION – AUDIT 2017-15489 – FEDERAL INFORMATION SECURITY MODERNIZATION ACT

Attached is the subject final report for your review and management decision. You are responsible for determining the necessary actions to take in response to our findings. Please advise us of your management decision within 60 days from the date of this report.

If you have any questions or wish to discuss our findings, please contact Scott A. Marler, Director (Acting), Information Technology Audits, at (865) 633-7352. We appreciate the courtesy and cooperation received from your staff during the audit.

David P. Wheeler

David P. Wheeler
Assistant Inspector General
(Audits and Evaluations)
ET 3C-K

SAM:BSC
Attachment
cc (Attachment):
TVA Board of Directors
Robert P. Arnold, MP 2C-C
Andrea S. Brackett, WT 5D-K
Janet J. Brewer, WT 7C-K
Josh T. Brewer, LP 2G-C
Clay Deloach, Jr., SP 3L-C
Robertson D. Dickens, WT 9C-K
Jeremy P. Fisher, MR 6D-C
Asa S. Hayes, MR BK-C
David M. Johnson, SP 2B-C
William D. Johnson, WT 7B-K
Dwain K. Lanier, MR 6D-C
Melissa A. Livesey, WT 5B-K
Justin C. Maierhofer, WT 7B-K
Jill M. Matthews, ET 4C-K
Philip D. Propes, MP 2C-C
Laura L. Snyder, MP 5G-C
John M. Thomas III, MR 6D-C
OIG File No. 2017-15489

Office of the Inspector General

Audit Report

To the Chief Information Officer,
Information Technology

FEDERAL INFORMATION SECURITY MODERNIZATION ACT

Auditor
Scott A. Marler

Audit 2017-15489
December 21, 2017

ABBREVIATIONS

DHS	Department of Homeland Security
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
ICAM	Identity, Credential, and Access Management
IG	Inspector General
IR	Incident Response
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Planning
ISP	Information Security Program
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIV	Personnel Identity Verification
POA&M	Plan of Action and Milestones
TIC	Trusted Internet Connection
TVA	Tennessee Valley Authority

TABLE OF CONTENTS

APPENDICES

Audit 2017-15489 – Federal Information Security Modernization Act

EXECUTIVE SUMMARY

Why the OIG Did This Audit

The Federal Information Security Modernization Act of 2014 (FISMA) requires each agency's Inspector General (IG) to conduct an annual independent evaluation to determine the effectiveness of the information security program (ISP) and practice of its respective agency.

Our objective was to evaluate the Tennessee Valley Authority's (TVA) strategy and the progress of TVA's ISP and agency practices for ensuring compliance with FISMA and applicable standards, including guidelines issued by the Office of Management and Budget and the National Institute of Standards and Technology (NIST). Our audit scope was limited to answering the fiscal year (FY) 2017 IG FISMA metrics (defined in the Appendix).

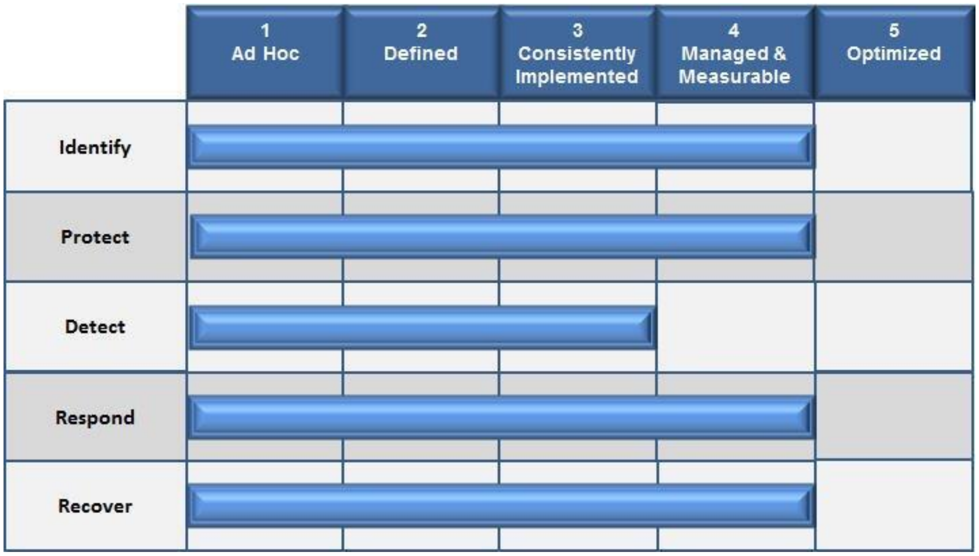
What the OIG Found

During the course of this audit, we utilized the methodology and metrics in the FY2017 IG FISMA Reporting Metrics (as detailed in the Appendix) in our annual independent evaluation to determine the effectiveness of TVA's ISP. Each metric was assessed to determine its maturity level, as described in the following table.

FY2017 IG FISMA Maturity Definitions

Maturity Level	Maturity Level Description
Level 1: *Ad Hoc*	Policies, procedures, and strategy are not formalized; activities are performed in an ad hoc, reactive manner.
Level 2: *Defined*	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: *Consistently Implemented*	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: *Managed and Measurable*	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.
Level 5: *Optimized*	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

The metrics were aligned with the five function areas Identify, Protect, Detect, Respond, and Recover from the NIST Framework for Improving Critical Infrastructure Cybersecurity. The FY2017 IG FISMA metrics recommend a majority of the functions be at a maturity level 4, managed and measurable, or higher to be considered effective. The metric results were used to determine the overall function area maturity as presented below.



Based on our analysis of the metrics and associated maturity levels defined with FY2017 IG FISMA Metrics, we found TVA's ISP was operating in an effective manner.

What the OIG Recommends

We recommend the Chief Information Officer, Information Technology, perform a risk assessment of the FY2017 IG FISMA metrics rated at a level 3 (consistently implemented) and determine actions necessary to reduce cybersecurity risk to the agency in FY2018.

TVA Management's Comments

In response to our draft audit report, TVA management agreed with our audit findings and recommendations. See Appendix B for TVA management's complete response.

BACKGROUND

The Federal Information Security Modernization Act of 2014 (FISMA) requires each agency's Inspector General (IG) to conduct an annual independent evaluation to determine the effectiveness of the information security program (ISP) and practice of its respective agency. The fiscal year (FY) 2017 IG FISMA Reporting Metrics (see the Appendix) were developed by the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and the Council of the Inspectors General on Integrity and Efficiency, in consultation with the Federal Chief Information Officer Council. In FY2016, the IG metrics were aligned with the five function areas in the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity. In addition, two of these function areas (Detect and Respond) were transitioned in FY2016 to maturity models, while the other function areas (Identity, Protect, and Recover) utilized maturity model indicators. The FY2017 FISMA Reporting Metrics transitioned the remaining functions to full maturity models and reorganized the models into seven domains within the five function areas to be more intuitive as shown in Table 1.

FY2017 FISMA Functions and Corresponding Domains	
Function	**Domain**
Identify	Risk Management
Protect	Configuration Management Identity and Access Management Security Training
Detect	Information Security Continuous Monitoring (ISCM)
Respond	Incident Response (IR)
Recover	Contingency Planning

Table 1

The results of our review were provided to OMB and DHS through use of their online reporting tool on October 30, 2017.[1]

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to evaluate TVA's strategy and the progress of TVA's ISP and agency practices for ensuring compliance with FISMA and applicable standards, including guidelines issued by the OMB and the NIST. Our audit scope was limited to answering the FY2017 IG FISMA metrics (see the Appendix). Our fieldwork was completed between May 2017 and October 2017.

[1] FY2017 Annual FISMA Report – Inspector General Section Report.

To accomplish our objective, we:

- Interviewed personnel in the Information Technology (IT) organization and TVA operating groups as necessary to gain an understanding and clarification of the policies, processes, and current state.
- Reviewed documentation provided by TVA organizations to corroborate our understanding and assess TVA's current state, including:
  - Relevant TVA agency-wide and business unit specific policies, procedures, and documents (such as Standard Programs and Processes, Standard Operating Procedures, and Work Instructions).
  - Relevant process flow charts, training materials and exercises, presentations, reports, logs, and outputs, to corroborate implementation of policies and procedures and Authority to Operate assessments of key TVA systems.
  - TVA's FY2016 10-K.
  - Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors Memorandum dated August 5, 2005, from the Executive Office of the President, OMB.
  - Memorandum of Agreement between TVA and DHS, Office of Cybersecurity and Communication, dated May 16, 2016, regarding EINSTEIN.[2]
  - TVA's SOX testing of IT controls related to backup testing.
  - Trusted Internet Connection (TIC) compliance implementation, current state, and compliance supporting documentation.
- Reviewed previous OIG FISMA reviews for FY2013[3] and FY2016[4] to leverage initial metric exemptions.
- Reviewed previous OIG patching audit issued in FY2017[5] for relevant findings.
- Selected a judgmental random sample of 23 of 15,250 users that had logical access to review the appropriateness of screening prior to gaining access to systems by using a random number generator. Since this was a judgmental sample, these results of the sample cannot be projected to the population.

During the course of this audit, we answered the FY2017 IG FISMA metric questions to determine the effectiveness of TVA's ISP by assessing the maturity of the eight domains. Table 2 on the following page outlines the five maturity model levels.

[2] EINSTEIN is a federal government program that provides additional cyber security monitoring to participating agencies.

[3] Audit Report 2013-15175, FISMA Evaluation, September 30, 2013.

[4] Audit 2016-15407, FISMA, January 11, 2017.

[5] Audit 2016-15369, Cyber Security Patch Management of High-Risk Desktops and Laptops, July 19, 2017.

FY2017 IG FISMA Metric Levels	
Maturity Level	**Maturity Level Description**
Level 1: *Ad Hoc*	Policies, procedures, and strategy are not formalized; activities are performed in an ad hoc, reactive manner.
Level 2: *Defined*	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: *Consistently Implemented*	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: *Managed and Measurable*	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.
Level 5: *Optimized*	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Table 2

A maturity level of 4 (managed and measurable) was considered to be effective. In cases where questions for maturity level descriptions were not provided for level 4 or above, a maturity level of 3 (consistently implemented) was considered effective. Ratings throughout the seven domains were determined by simple majority of the question results, effective or not effective.

The ratings for the five functions were determined in the same manner using the domain ratings. Functions that score at or above the level 4 (managed and measurable) maturity ranking have "effective" programs within that area, as prescribed by the IG FISMA metrics. The same simple majority rule was used to determine TVA's overall agency rating, based on the function scores. See the Appendix (beginning on page 2 of 40) for detailed information on the maturity level scoring methodology.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

FINDINGS

Based on our analysis of the metrics and associated maturity levels defined within the FY2017 IG FISMA metrics, we found TVA's security program was operating in an effective manner. The FY2017 IG FISMA metrics recommend a majority of the functions be at a maturity level 4 (managed and measurable) or higher to be considered effective. TVA had four of the five functions rated at a level 4 (managed and measurable). See Figure 1 on the following page for the individual function ratings.

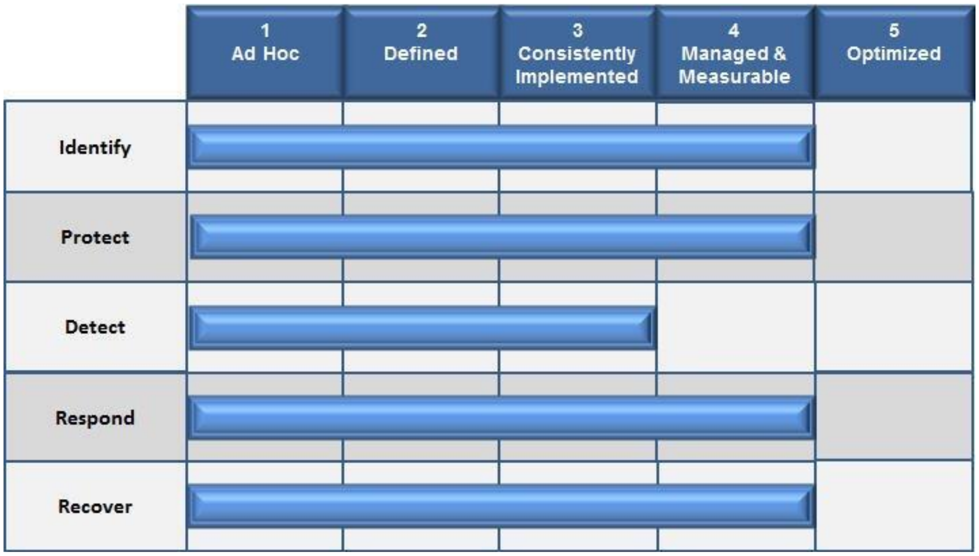


Figure 1

IDENTIFY

The Identify function includes understanding the business context, the resources that support critical functions, and the related cybersecurity risks. This understanding enables an organization to focus and prioritize efforts, consistent with its risk management strategy and business need. Within the context of the FY2017 IG FISMA metrics, the Identify function also includes activities related to risk management.

Our analysis of the Identify metrics found appropriate risk management policies and procedures have been defined, implemented, and are managed and monitored. TVA has defined policies and/or processes for software inventory, risk management, and the use of Plan of Action and Milestones (POA&M). Also, TVA has implemented processes to (1) ensure software is subject to monitoring processes defined with the ISCM strategy; (2) maintain an inventory of information systems, including cloud systems, public facing Web sites, and third-party systems; (3) maintain an inventory of hardware; (4) utilize a risk profile to facilitate a determination of risk for a system; (5) manage POA&Ms; (6) perform security architecture reviews on new hardware and software prior to installation on TVA's network; and (7) perform system risk assessments, which includes verification that appropriate system security controls are implemented on a consistent basis. In addition, TVA is monitoring and analyzing qualitative and quantitative performance measures on the effectiveness of its risk management program and POA&M activities.

However, we found TVA has not fully implemented (1) a network access control solution; (2) risk dashboards for TVA's IT, key risk indicators, risk evaluation, and cyber security risk management tracking processes; (3) diagnostic and reporting frameworks, including dashboards for enterprise level risk management; or

(4) the monitoring, measuring, and reporting of information security performance of contractor operated systems and services.

As a result of our testing of the Identify maturity model, we determined TVA was operating at a level 4 (managed and measurable) maturity level.

PROTECT

The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event by developing and implementing appropriate safeguards to ensure delivery of critical infrastructure services. Within the context of the FY2017 IG FISMA metrics, the Protect function includes the domain's configuration management; identity, credential, and access management (ICAM); and security training.

Configuration management – TVA has defined roles and responsibilities within configuration management policies and procedures. Also, TVA has developed and implemented processes for baseline configurations, common secure configurations, automated tools to help maintain security configurations for information systems, and the collection and reporting of change control metrics and has incorporated lessons learned within those processes. Additionally, TVA has developed and implemented change control policies and procedures that include determining which changes are configuration changes, the review of proposed changes for approval and consideration of security impacts, and classifications of systems.

However, TVA is not collecting and reporting on metrics to track the effectiveness of configuration management. While TVA has implemented automated tools for flaw remediation and patch management, not all systems within TVA are managed by these tools. In addition, automated mechanisms such as application whitelisting and network management tools have not been fully deployed to detect unauthorized hardware and software and to take immediate actions to limit any security impact.

As a result of our testing of the configuration management maturity model, we determined TVA was operating at a level 3 (consistently implemented) maturity level.

ICAM – TVA has defined, developed, and implemented an ICAM strategy which includes policies and procedures that define roles and responsibilities, personnel risk designations and screening, access and acceptable use agreements, remote access, and the provisioning and management of user accounts, including privileged accounts. In addition, TVA uses automated mechanisms for the management of user accounts, including privileged accounts.

However, TVA has not completed all ICAM milestones to transition to its "to-be" ICAM architecture. In addition, while TVA has policies and processes to conduct screening prior to gaining access to systems, our testing of a sample of 23 users found 1 did not have screening prior to gaining access to systems.

As a result of our testing of the ICAM maturity model, we determined TVA was operating at a level 4 (managed and measurable) maturity level.

Security training – TVA has a security awareness plan in place that has defined roles and responsibilities, requires the completion of security awareness training, utilizes a phishing program, and provides specialized training as needed for specialized roles. TVA collects and analyzes training data to improve exam questions and training module content. However, TVA does not correlate training exercises with the full population of users with significant security responsibilities. In addition, TVA has not performed a centralized assessment of the IT workforce for skills, knowledge, and abilities to provide tailored awareness and security training.

As a result of our testing of the security training maturity model, we determined TVA was operating at a level 4 (managed and measurable) maturity level.

TVA management also provided sufficient evidence supporting their position that two areas in the FY2017 IG FISMA metrics in the Protect function were not applicable. These two areas are the (1) enforcement of personnel identity verification (PIV) or NIST's Level of Assurance 4 requiring something in a user's possession to authenticate to the network utilizing encryption and (2) use of TIC security controls to route traffic through defined access points. As a result, the related FISMA metrics listed in Table 3 were passed with a note explaining the agency's stance.

Function Domain	Related Metric(s)	TVA Position
Identity and Access Management	28 29	TVA does not enforce PIV or NIST Level of Assurance 4* credentials for all privileged users or at least 85% of nonprivileged users. IT management determined TVA is exempt from this requirement and validated this through TVA's Office of General Counsel.
Configuration Management	20	TVA does not utilize a TIC provider for defined access points. According to the TVA's Cybersecurity Director, TVA performed a detailed review that resulted in a formal decision to not utilize a TIC provider, which is specifically mentioned in the Respond maturity model for technology. Instead, TVA management decided to continue investing in internal network and internet security programs that have been customized to meet TVA needs and ensure ongoing security posture.

* NIST Special Publication 800-63-2, Electronic Authentication Guideline, states Level of Assurance 4 requires authentication based on proof of possession of a key through a cryptographic protocol using a hard cryptographic token.

Table 3

Based on our analysis of the configuration management, ICAM, and security and privacy training maturity models we determined TVA was operating at a level 4 (managed and measurable) maturity level for the Protect function.

DETECT

The Detect function enables timely discovery of cybersecurity events by developing and implementing actions to identify their occurrence. Within the context of the FY2017 IG FISMA metrics, the Detect function includes ISCM.

Our analysis of the Detect maturity metrics found ISCM policies and procedures have been defined, developed, and implemented; however, qualitative and quantitative performance measures will not be implemented until 2019. TVA's Cybersecurity also has an organization-wide strategy that supports clear visibility into assets, awareness into vulnerabilities, up-to-date threat information, and mission/business impacts.

As a result of our testing of the Detect maturity model, we determined TVA was operating at a level 3 (consistently implemented) maturity level.

RESPOND

The Respond function supports the ability to contain the impact of a potential cybersecurity event by developing and implementing activities to take action when a cybersecurity event is detected. Within the context of the FY2017 IG FISMA metrics, the Respond function includes IR.

Our analysis of the Respond metrics found appropriate IR policies and procedures have been defined, implemented, and are managed and monitored. These include processes for IR and detection and incident handling supported by various technologies that are interoperable to the extent possible. In addition, qualitative and quantitative IR metrics are defined, collected, and analyzed to monitor and report on the IR effectiveness.

As a result of our testing of the Respond maturity model, we determined TVA was operating at a level 4 (managed and measurable) maturity level.

RECOVER

The Recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Activities within the Recover function develop and implement plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. Within the context of the FY2017 IG FISMA metrics, the Recover function includes contingency planning.

Our analysis of the Recover metrics found appropriate contingency planning policies and procedures have been defined, implemented, and are managed and monitored. TVA has defined and implemented its information system contingency planning (ISCP) policies, procedures, and strategies, including roles and responsibilities, scope, resource requirements, training, exercise and testing schedules, plan maintenance schedules, backups and storage, use of alternate processing and storage sites, technical contingency planning considerations for specific types of systems, and appropriate delegation of authority. Also, TVA has established appropriate teams that are ready to implement its ISCP strategies. In addition, Business Continuity Services is responsible for monitoring and tracking the effectiveness of ISCP activities at TVA as well as maintaining metrics for tests, training and exercise completion, successful database backups and media recovery.

As a result of our testing of the Recover maturity model, we determined TVA was operating at a level 4 (managed and measurable) maturity level.

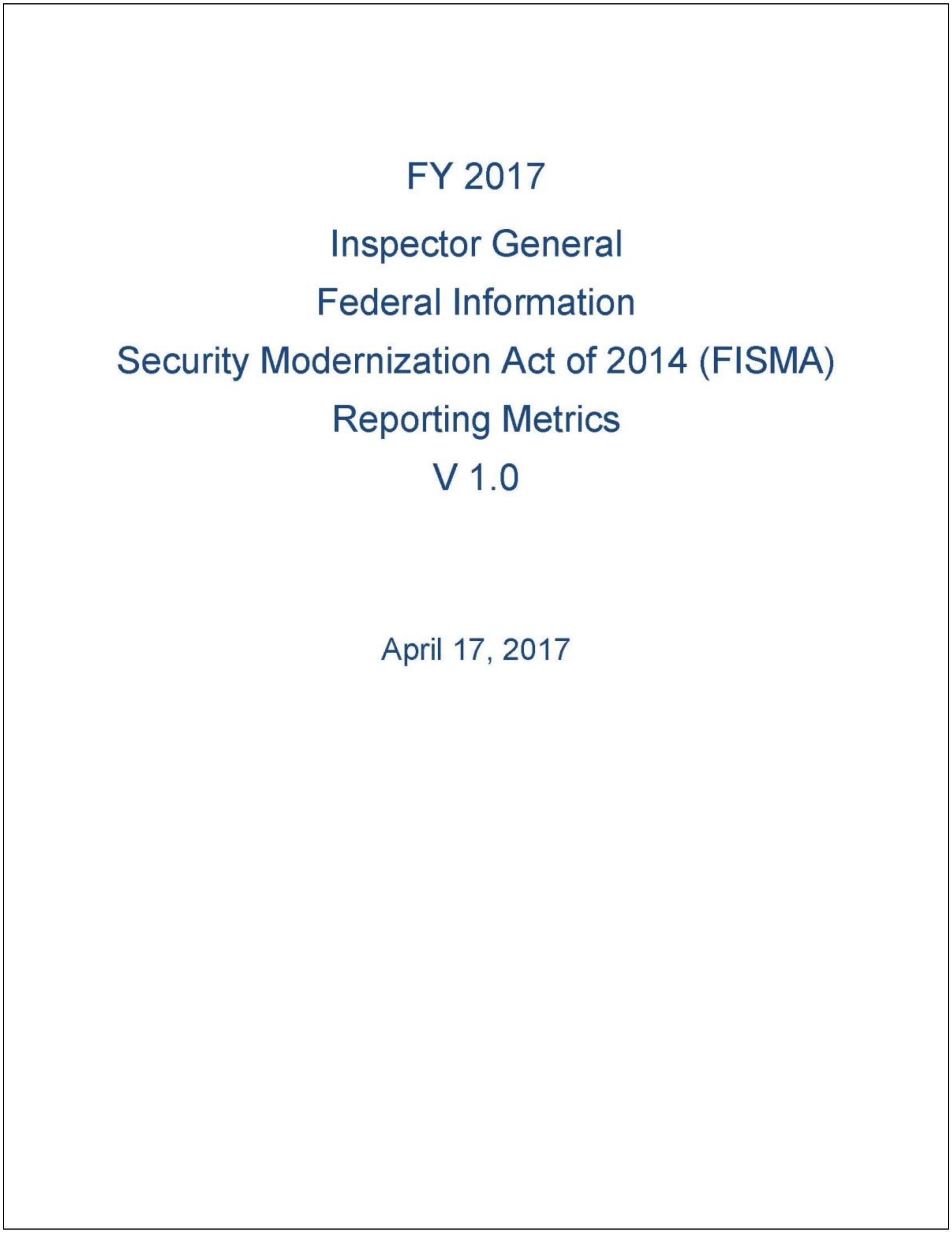
CONCLUSION

Based on our analysis of the metrics and associated maturity levels defined with FY2017 IG FISMA Metrics, we found TVA's security program was operating in an effective manner.

RECOMMENDATION

We recommend the Chief Information Officer, IT, perform a risk assessment of the FY2017 IG FISMA metrics rated at a level 3 (consistently implemented) and determine actions necessary to reduce cybersecurity risk to the agency in FY2018.

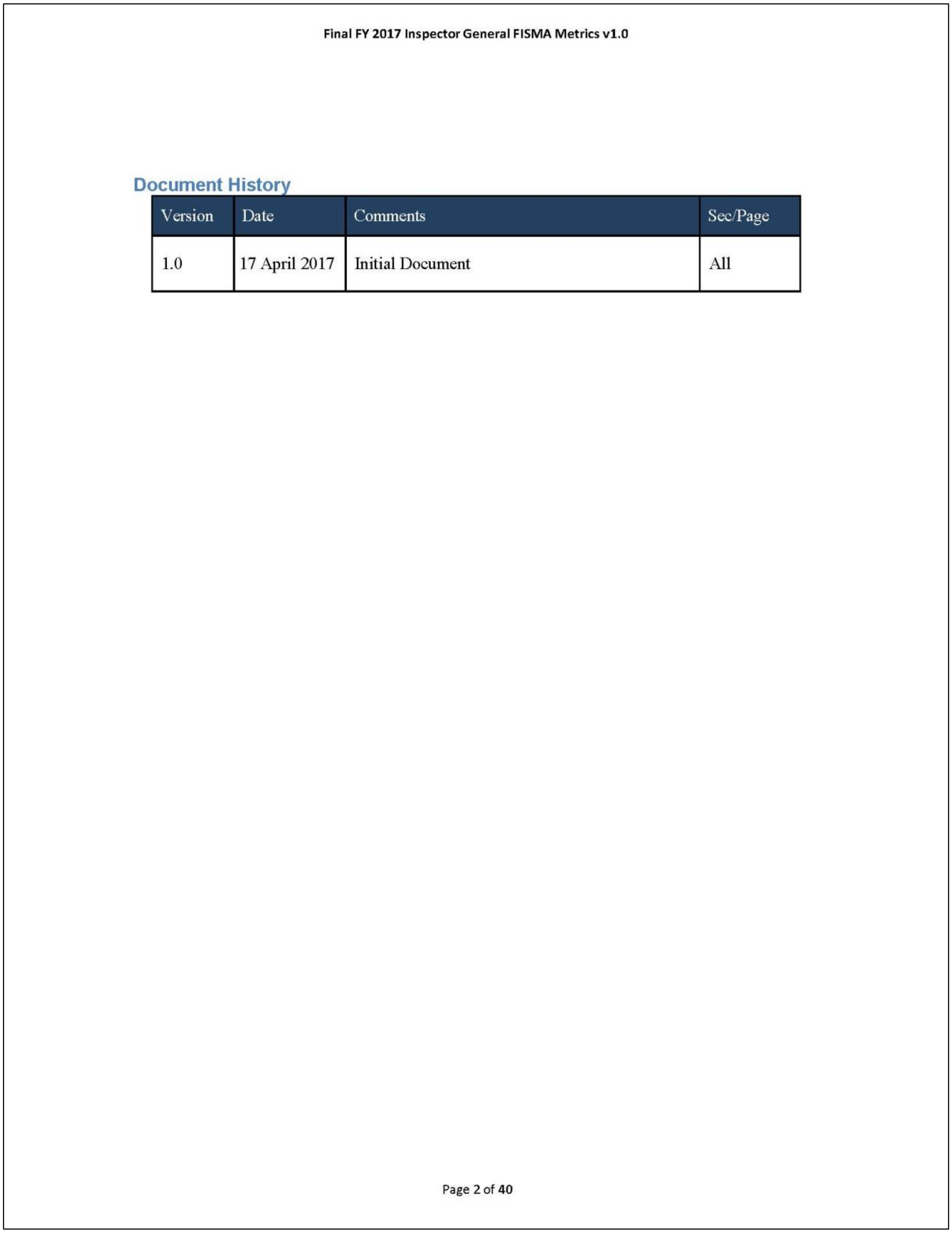
TVA Management's Comments – In response to our draft audit report, TVA management agreed with our audit findings and recommendations. See Appendix B for TVA management's complete response.



FY 2017

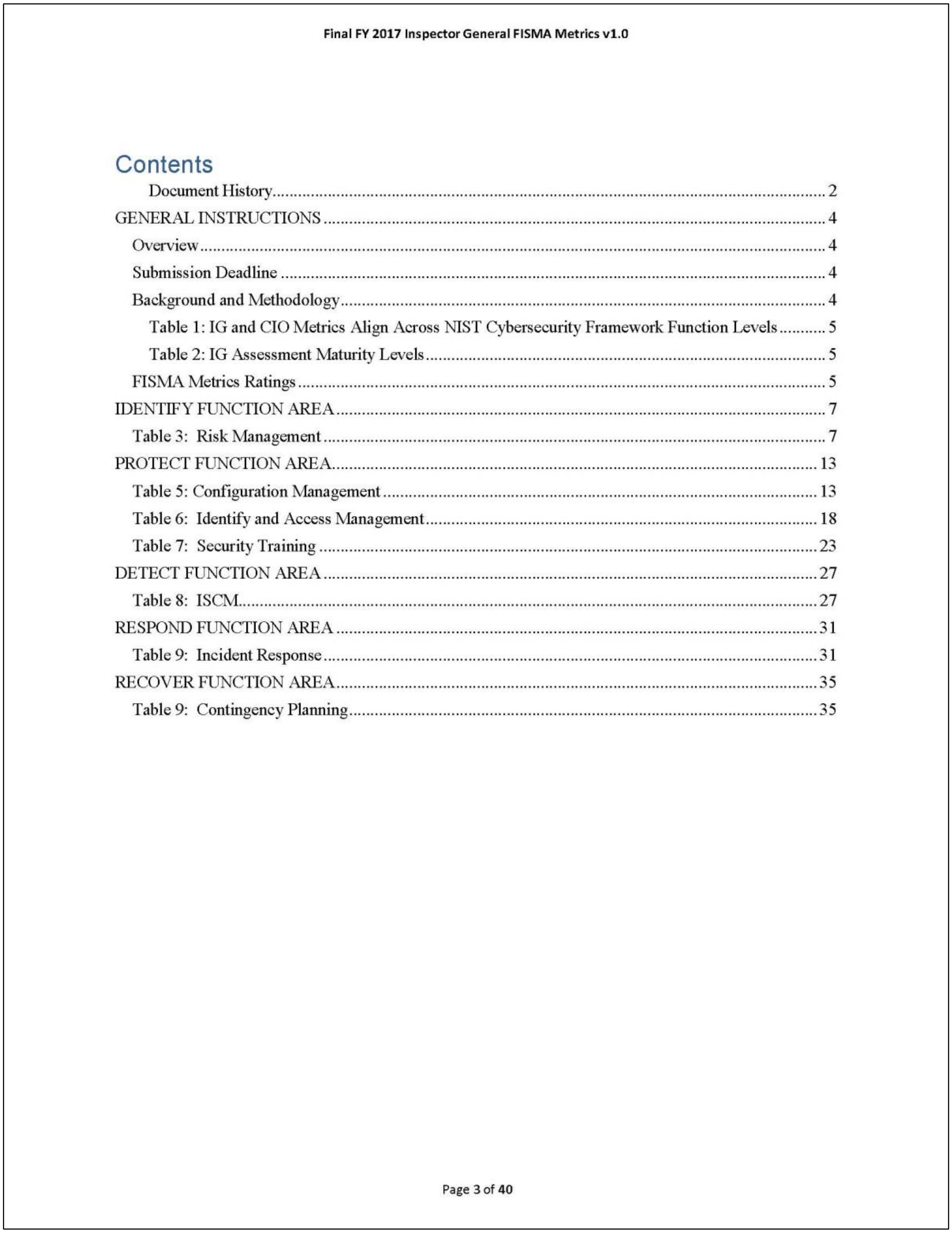
Inspector General
Federal Information
Security Modernization Act of 2014 (FISMA)
Reporting Metrics
V 1.0

April 17, 2017

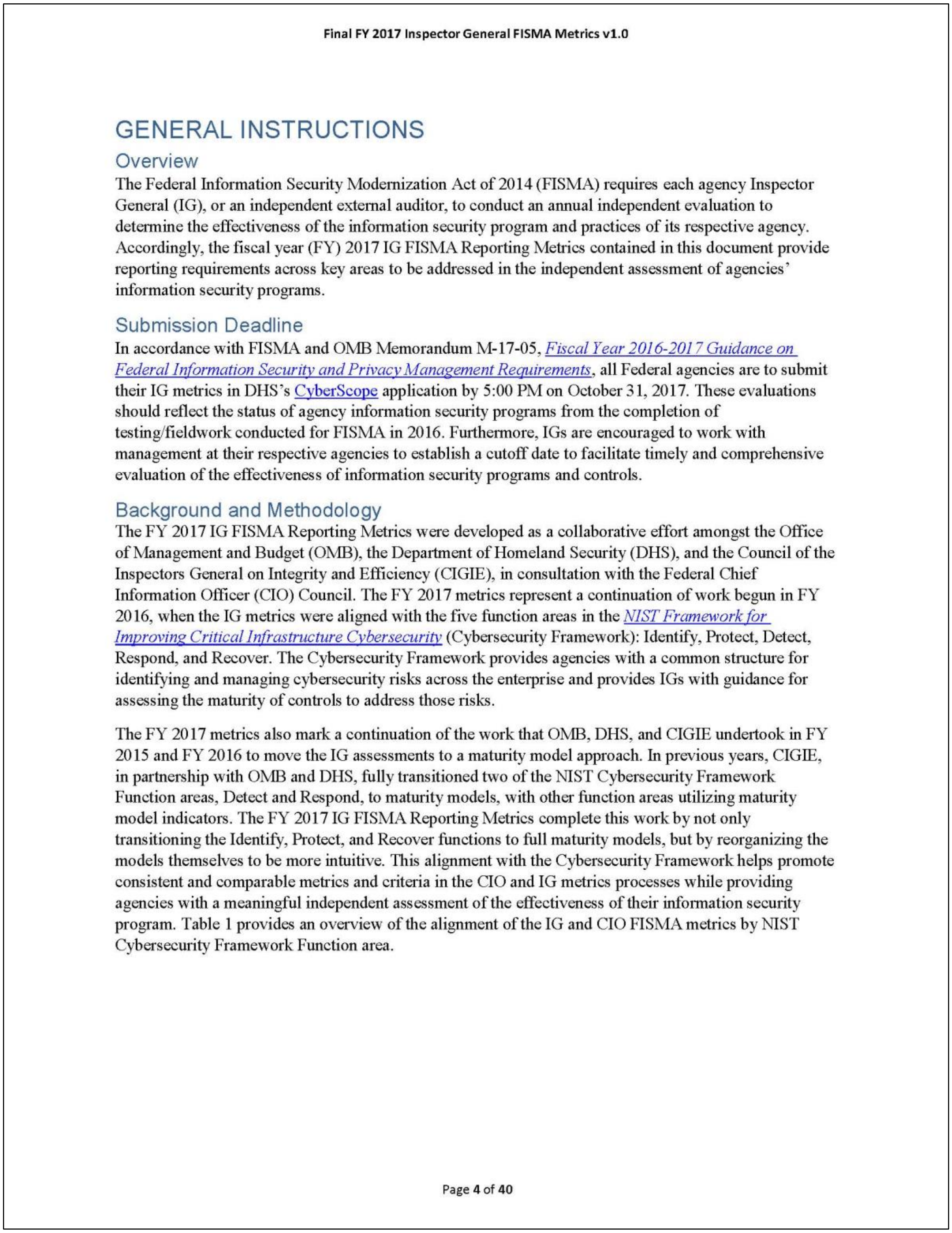


Document History

Version	Date	Comments	Sec/Page
1.0	17 April 2017	Initial Document	All



Contents



GENERAL INSTRUCTIONS

Overview

The Federal Information Security Modernization Act of 2014 (FISMA) requires each agency Inspector General (IG), or an independent external auditor, to conduct an annual independent evaluation to determine the effectiveness of the information security program and practices of its respective agency. Accordingly, the fiscal year (FY) 2017 IG FISMA Reporting Metrics contained in this document provide reporting requirements across key areas to be addressed in the independent assessment of agencies' information security programs.

Submission Deadline

In accordance with FISMA and OMB Memorandum M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements*, all Federal agencies are to submit their IG metrics in DHS's CyberScope application by 5:00 PM on October 31, 2017. These evaluations should reflect the status of agency information security programs from the completion of testing/fieldwork conducted for FISMA in 2016. Furthermore, IGs are encouraged to work with management at their respective agencies to establish a cutoff date to facilitate timely and comprehensive evaluation of the effectiveness of information security programs and controls.

Background and Methodology

The FY 2017 IG FISMA Reporting Metrics were developed as a collaborative effort amongst the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in consultation with the Federal Chief Information Officer (CIO) Council. The FY 2017 metrics represent a continuation of work begun in FY 2016, when the IG metrics were aligned with the five function areas in the *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.

The FY 2017 metrics also mark a continuation of the work that OMB, DHS, and CIGIE undertook in FY 2015 and FY 2016 to move the IG assessments to a maturity model approach. In previous years, CIGIE, in partnership with OMB and DHS, fully transitioned two of the NIST Cybersecurity Framework Function areas, Detect and Respond, to maturity models, with other function areas utilizing maturity model indicators. The FY 2017 IG FISMA Reporting Metrics complete this work by not only transitioning the Identify, Protect, and Recover functions to full maturity models, but by reorganizing the models themselves to be more intuitive. This alignment with the Cybersecurity Framework helps promote consistent and comparable metrics and criteria in the CIO and IG metrics processes while providing agencies with a meaningful independent assessment of the effectiveness of their information security program. Table 1 provides an overview of the alignment of the IG and CIO FISMA metrics by NIST Cybersecurity Framework Function area.

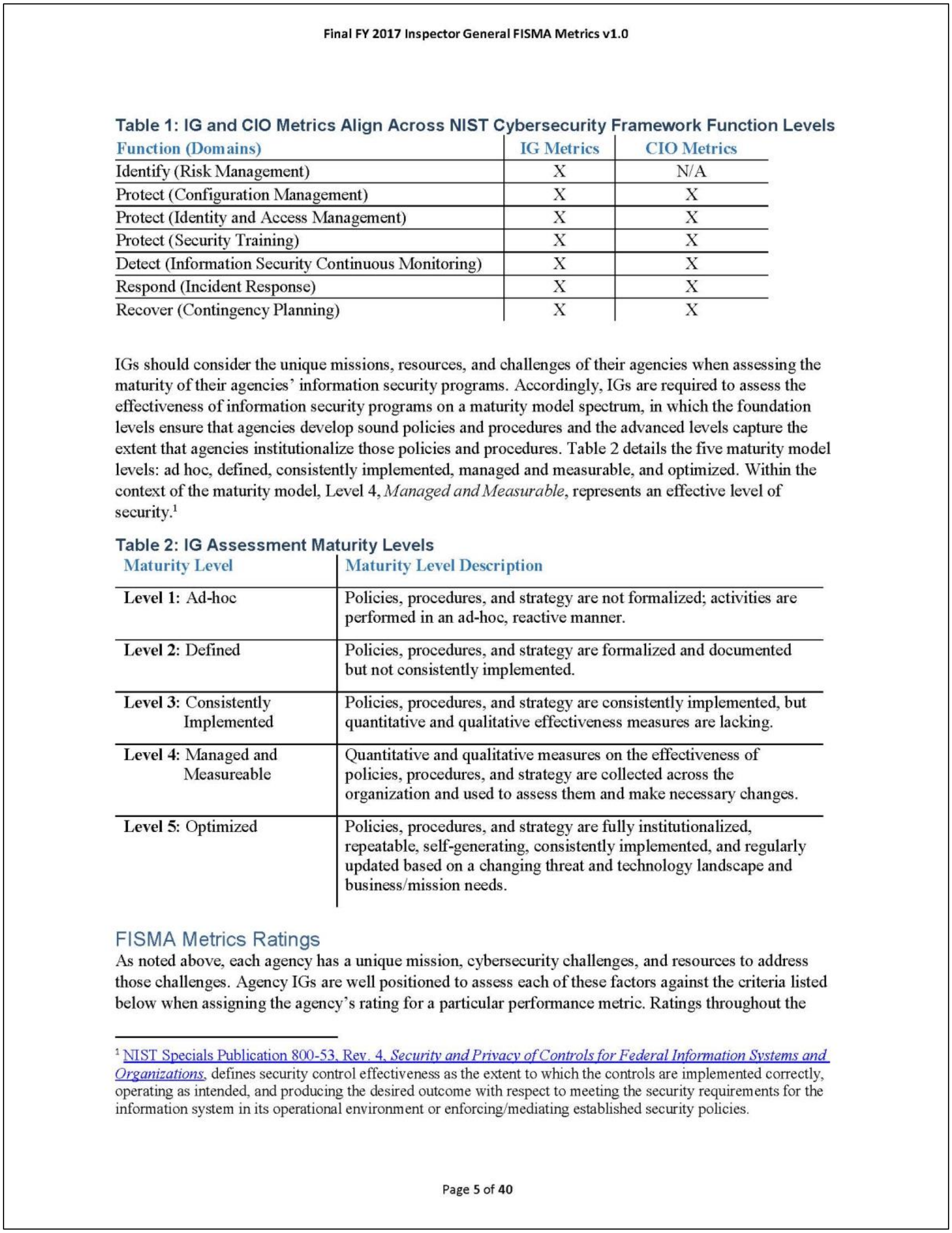


Table 1: IG and CIO Metrics Align Across NIST Cybersecurity Framework Function Levels

Function (Domains)	IG Metrics	CIO Metrics
Identify (Risk Management)	X	N/A
Protect (Configuration Management)	X	X
Protect (Identity and Access Management)	X	X
Protect (Security Training)	X	X
Detect (Information Security Continuous Monitoring)	X	X
Respond (Incident Response)	X	X
Recover (Contingency Planning)	X	X

IGs should consider the unique missions, resources, and challenges of their agencies when assessing the maturity of their agencies' information security programs. Accordingly, IGs are required to assess the effectiveness of information security programs on a maturity model spectrum, in which the foundation levels ensure that agencies develop sound policies and procedures and the advanced levels capture the extent that agencies institutionalize those policies and procedures. Table 2 details the five maturity model levels: ad hoc, defined, consistently implemented, managed and measurable, and optimized. Within the context of the maturity model, Level 4, *Managed and Measurable*, represents an effective level of security.[1]

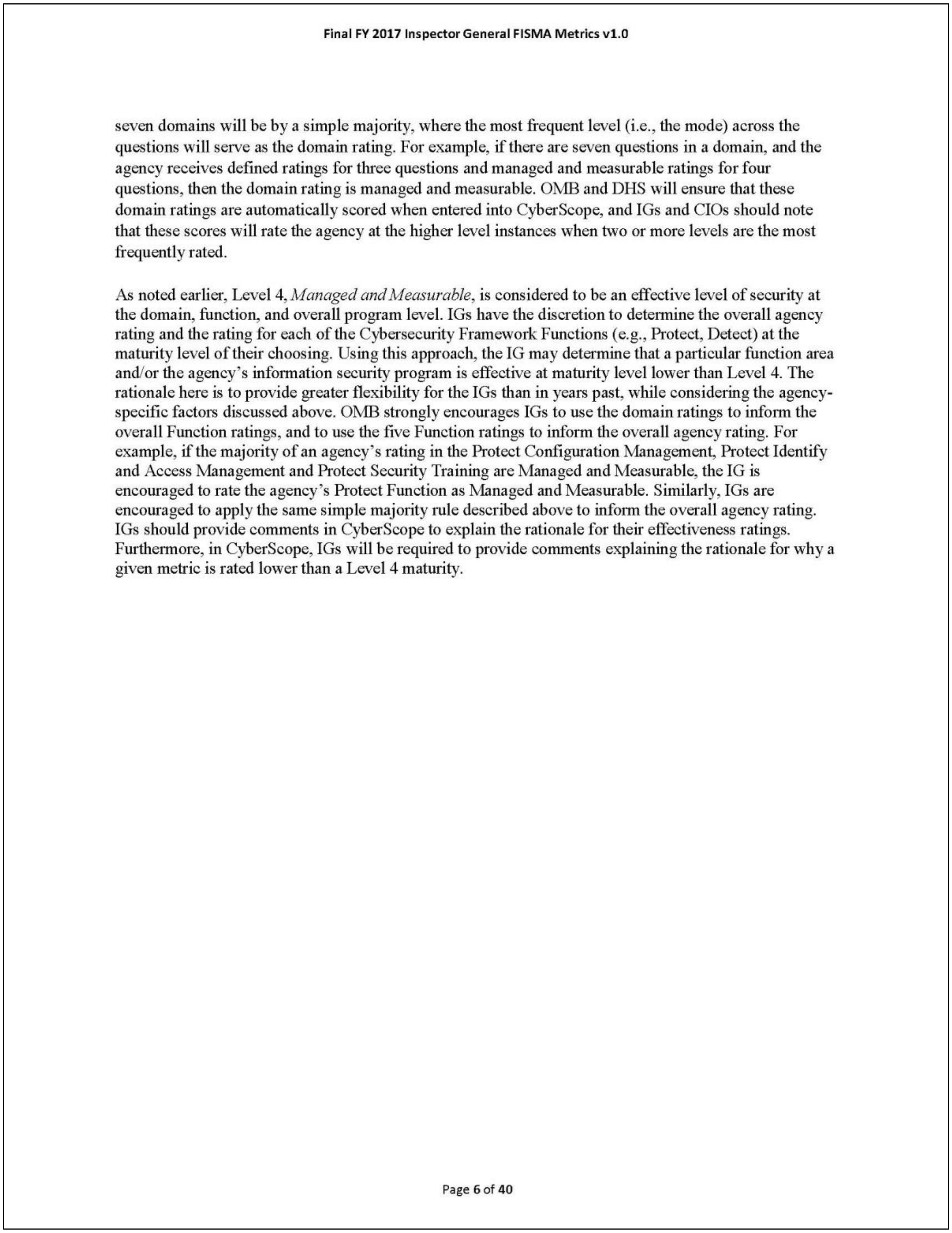
Table 2: IG Assessment Maturity Levels

Maturity Level	Maturity Level Description
Level 1: Ad-hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measureable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

FISMA Metrics Ratings

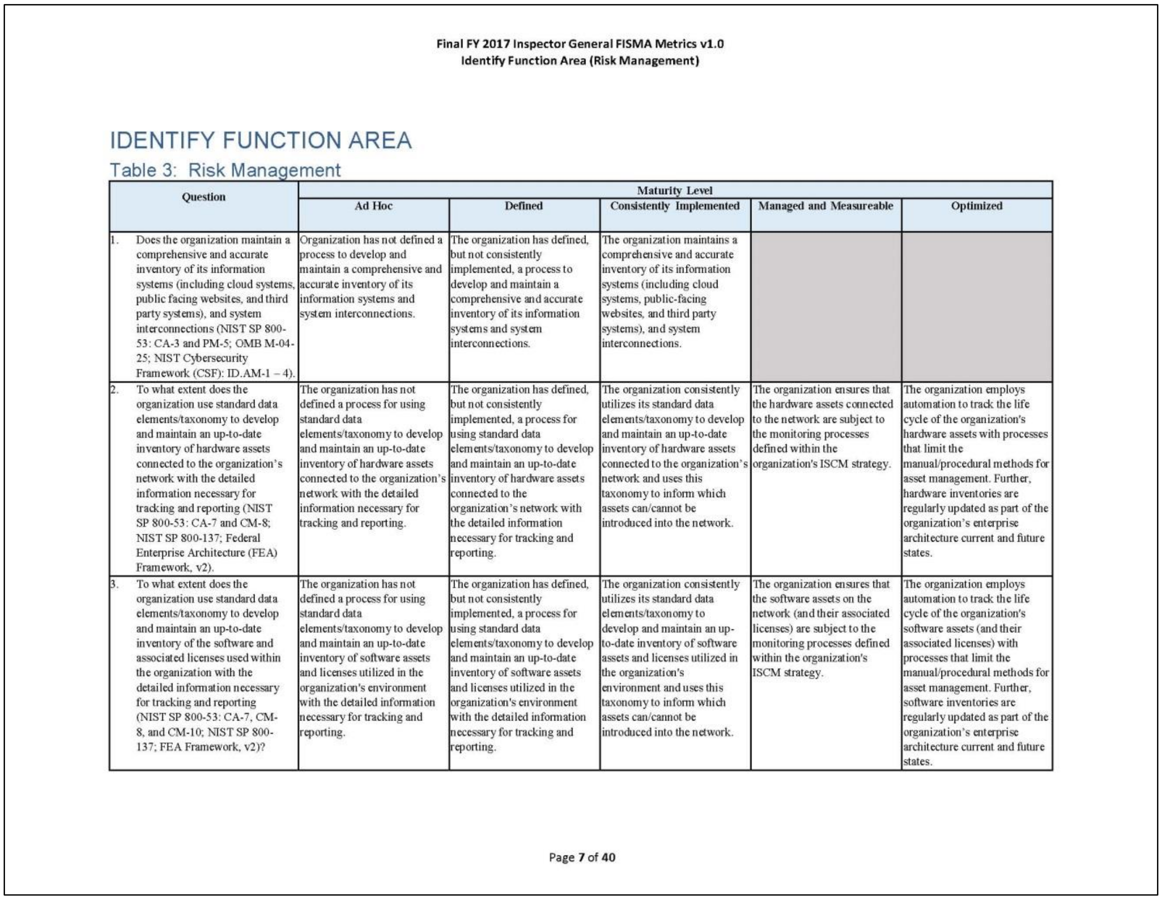
As noted above, each agency has a unique mission, cybersecurity challenges, and resources to address those challenges. Agency IGs are well positioned to assess each of these factors against the criteria listed below when assigning the agency's rating for a particular performance metric. Ratings throughout the

[1] NIST Specials Publication 800-53, Rev. 4, *Security and Privacy of Controls for Federal Information Systems and Organizations*, defines security control effectiveness as 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 information system in its operational environment or enforcing/mediating established security policies.



seven domains will be by a simple majority, where the most frequent level (i.e., the mode) across the questions will serve as the domain rating. For example, if there are seven questions in a domain, and the agency receives defined ratings for three questions and managed and measurable ratings for four questions, then the domain rating is managed and measurable. OMB and DHS will ensure that these domain ratings are automatically scored when entered into CyberScope, and IGs and CIOs should note that these scores will rate the agency at the higher level instances when two or more levels are the most frequently rated.

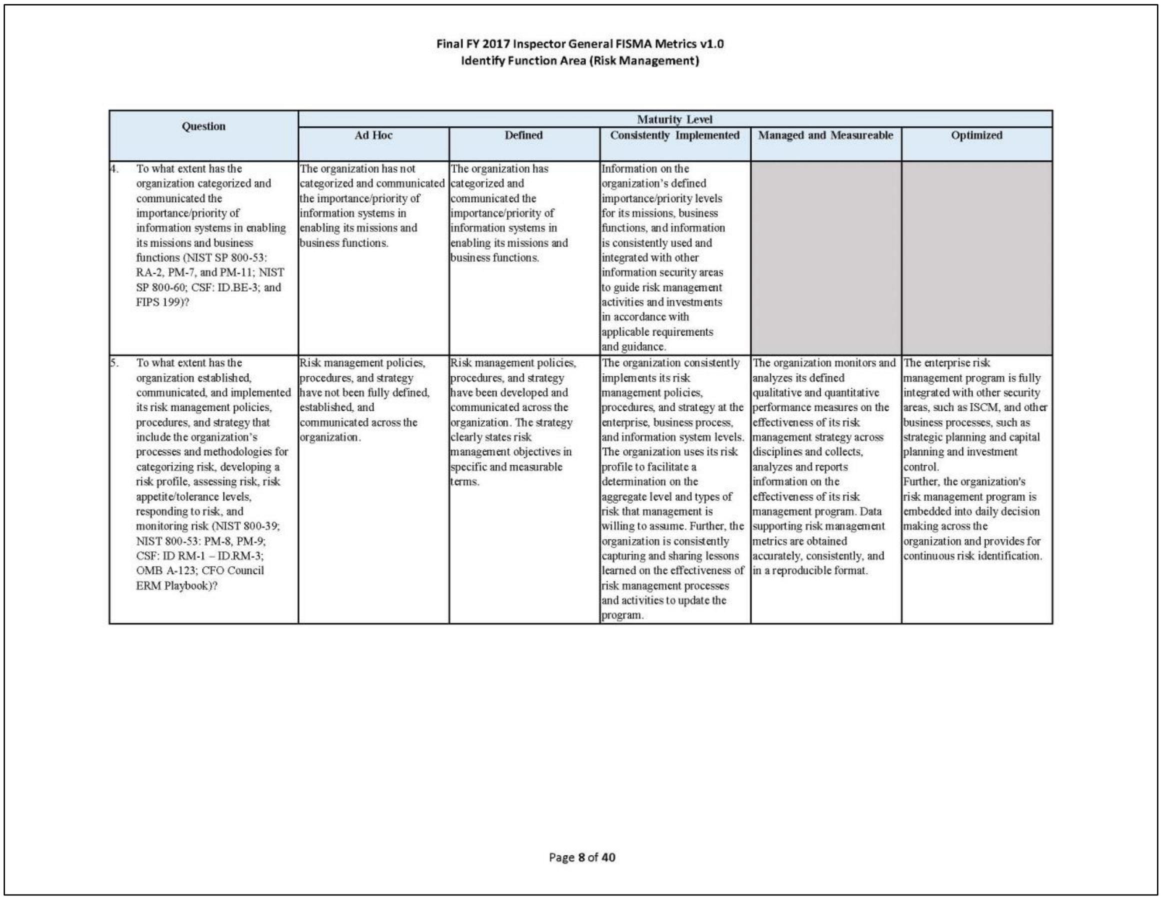
As noted earlier, Level 4, *Managed and Measurable*, is considered to be an effective level of security at the domain, function, and overall program level. IGs have the discretion to determine the overall agency rating and the rating for each of the Cybersecurity Framework Functions (e.g., Protect, Detect) at the maturity level of their choosing. Using this approach, the IG may determine that a particular function area and/or the agency's information security program is effective at maturity level lower than Level 4. The rationale here is to provide greater flexibility for the IGs than in years past, while considering the agency-specific factors discussed above. OMB strongly encourages IGs to use the domain ratings to inform the overall Function ratings, and to use the five Function ratings to inform the overall agency rating. For example, if the majority of an agency's rating in the Protect Configuration Management, Protect Identify and Access Management and Protect Security Training are Managed and Measurable, the IG is encouraged to rate the agency's Protect Function as Managed and Measurable. Similarly, IGs are encouraged to apply the same simple majority rule described above to inform the overall agency rating. IGs should provide comments in CyberScope to explain the rationale for their effectiveness ratings. Furthermore, in CyberScope, IGs will be required to provide comments explaining the rationale for why a given metric is rated lower than a Level 4 maturity.



IDENTIFY FUNCTION AREA

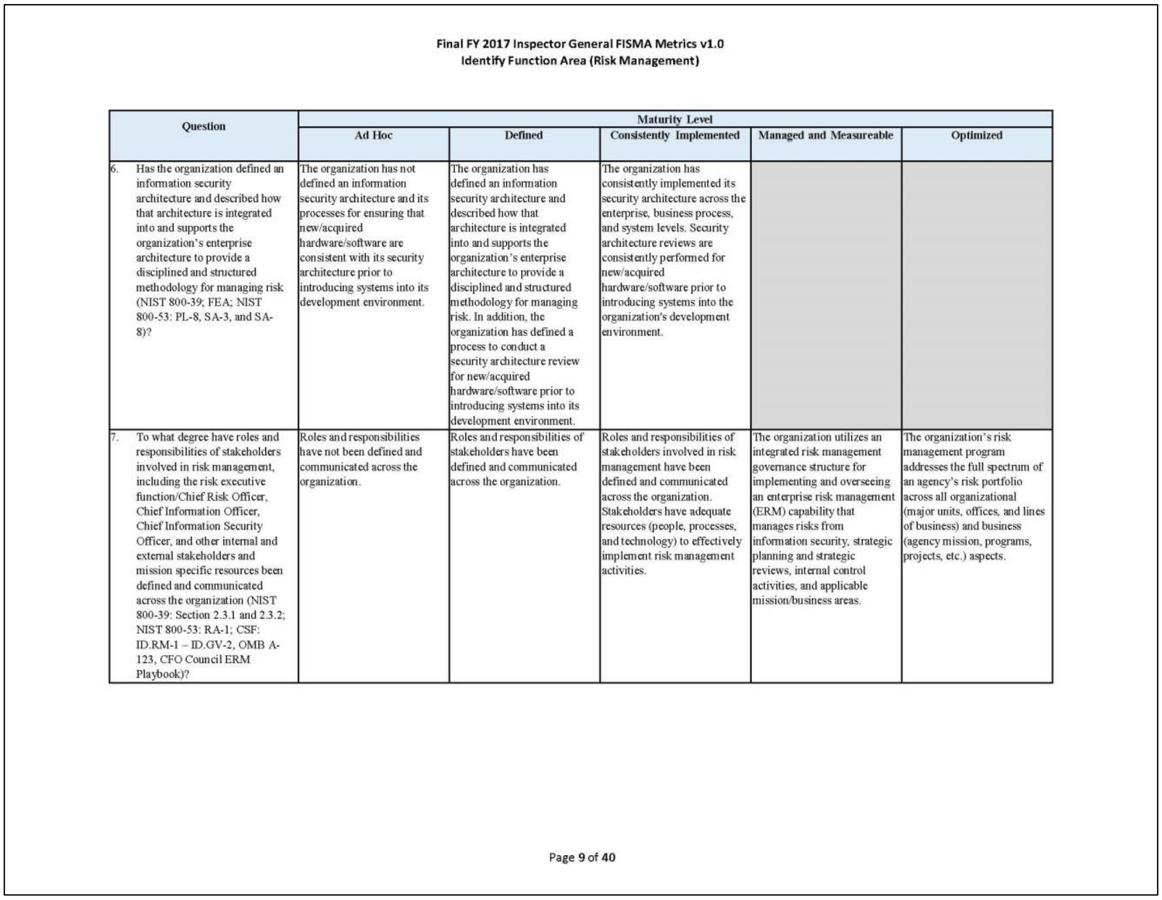
Table 3: Risk Management

Question		Maturity Level				
		Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
1.	Does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third party systems), and system interconnections (NIST SP 800-53: CA-3 and PM-5; OMB M-04-25; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4).	Organization has not defined a process to develop and maintain a comprehensive and accurate inventory of its information systems and system interconnections.	The organization has defined, but not consistently implemented, a process to develop and maintain a comprehensive and accurate inventory of its information systems and system interconnections.	The organization maintains a comprehensive and accurate inventory of its information systems (including cloud systems, public-facing websites, and third party systems), and system interconnections.		
2.	To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting (NIST SP 800-53: CA-7 and CM-8; NIST SP 800-137; Federal Enterprise Architecture (FEA) Framework, v2).	The organization has not defined a process for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting.	The organization has defined, but not consistently implemented, a process for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting.	The organization consistently utilizes its standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network and uses this taxonomy to inform which assets can/cannot be introduced into the network.	The organization ensures that the hardware assets connected to the network are subject to the monitoring processes defined within the organization's ISCM strategy.	The organization employs automation to track the life cycle of the organization's hardware assets with processes that limit the manual/procedural methods for asset management. Further, hardware inventories are regularly updated as part of the organization's enterprise architecture current and future states.
3.	To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting (NIST SP 800-53: CA-7, CM-8, and CM-10; NIST SP 800-137; FEA Framework, v2)?	The organization has not defined a process for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses utilized in the organization's environment with the detailed information necessary for tracking and reporting.	The organization has defined, but not consistently implemented, a process for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses utilized in the organization's environment with the detailed information necessary for tracking and reporting.	The organization consistently utilizes its standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses utilized in the organization's environment and uses this taxonomy to inform which assets can/cannot be introduced into the network.	The organization ensures that the software assets on the network (and their associated licenses) are subject to the monitoring processes defined within the organization's ISCM strategy.	The organization employs automation to track the life cycle of the organization's software assets (and their associated licenses) with processes that limit the manual/procedural methods for asset management. Further, software inventories are regularly updated as part of the organization's enterprise architecture current and future states.



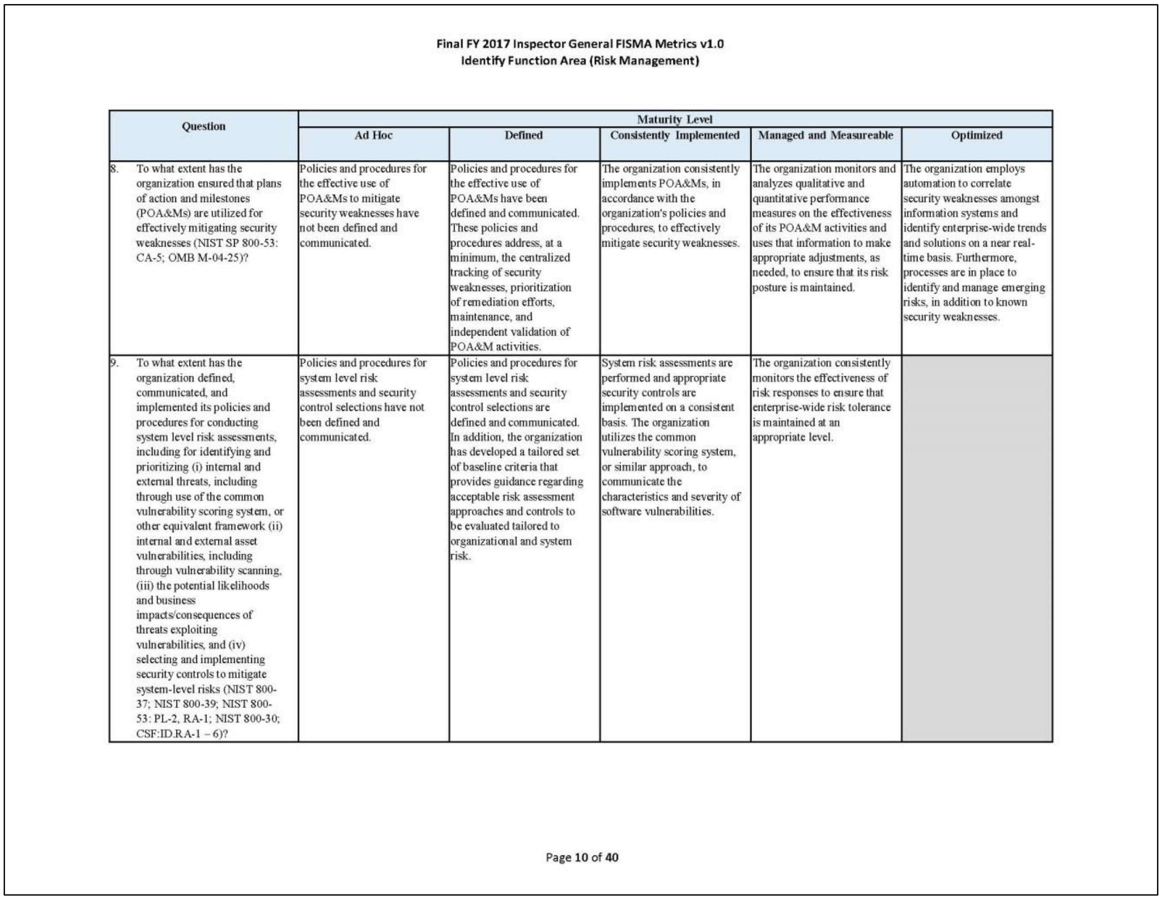
Final FY 2017 Inspector General FISMA Metrics v1.0
Identify Function Area (Risk Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
4. To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions (NIST SP 800-53: RA-2, PM-7, and PM-11; NIST SP 800-60; CSF: ID.BE-3; and FIPS 199)?	The organization has not categorized and communicated the importance/priority of information systems in enabling its missions and business functions.	The organization has categorized and communicated the importance/priority of information systems in enabling its missions and business functions.	Information on the organization's defined importance/priority levels for its missions, business functions, and information is consistently used and integrated with other information security areas to guide risk management activities and investments in accordance with applicable requirements and guidance.		
5. To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy that include the organization's processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk (NIST 800-39; NIST 800-53: PM-8, PM-9; CSF: ID RM-1 – ID.RM-3; OMB A-123; CFO Council ERM Playbook)?	Risk management policies, procedures, and strategy have not been fully defined, established, and communicated across the organization.	Risk management policies, procedures, and strategy have been developed and communicated across the organization. The strategy clearly states risk management objectives in specific and measurable terms.	The organization consistently implements its risk management policies, procedures, and strategy at the enterprise, business process, and information system levels. The organization uses its risk profile to facilitate a determination on the aggregate level and types of risk that management is willing to assume. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of risk management processes and activities to update the program.	The organization monitors and analyzes its defined qualitative and quantitative performance measures on the effectiveness of its risk management strategy across disciplines and collects, analyzes and reports information on the effectiveness of its risk management program. Data supporting risk management metrics are obtained accurately, consistently, and in a reproducible format.	The enterprise risk management program is fully integrated with other security areas, such as ISCM, and other business processes, such as strategic planning and capital planning and investment control. Further, the organization's risk management program is embedded into daily decision making across the organization and provides for continuous risk identification.



Final FY 2017 Inspector General FISMA Metrics v1.0
Identify Function Area (Risk Management)

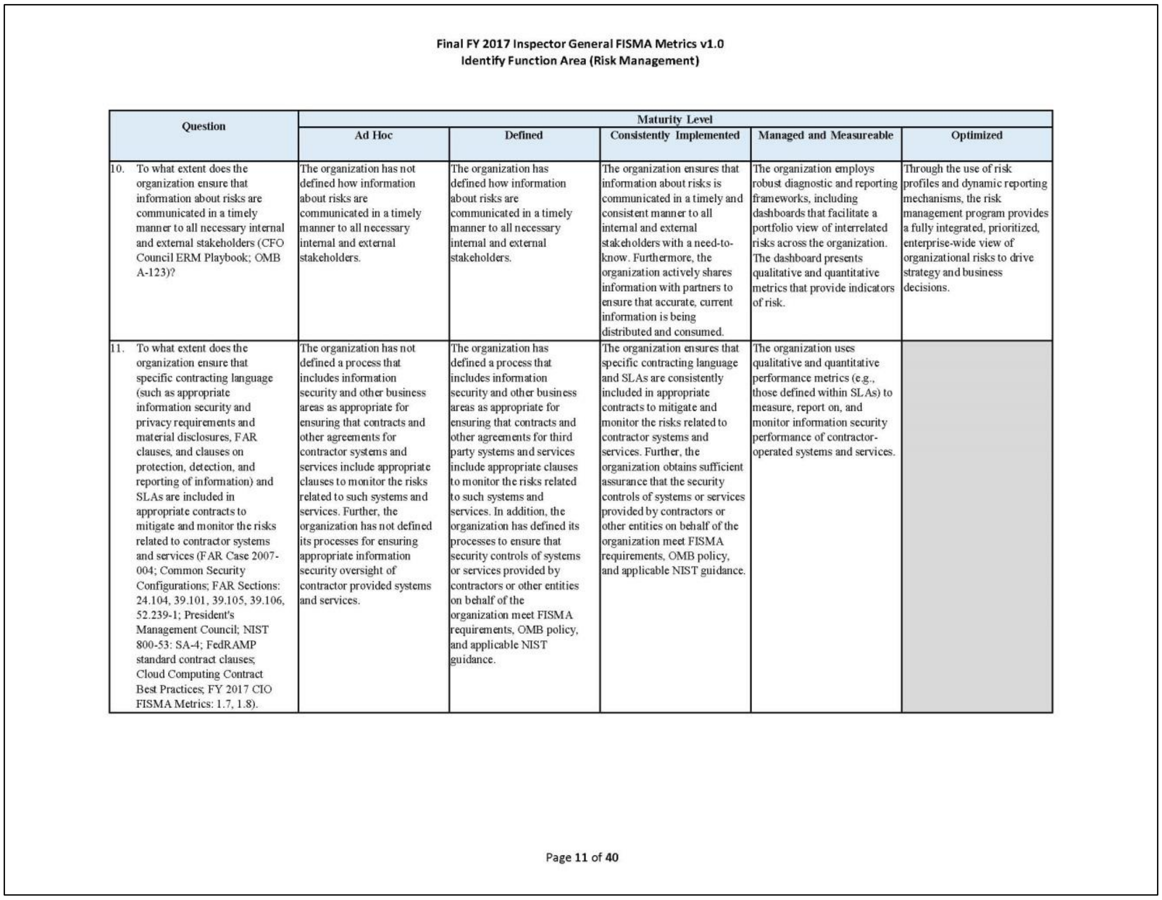
Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
6. Has the organization defined an information security architecture and described how that architecture is integrated into and supports the organization's enterprise architecture to provide a disciplined and structured methodology for managing risk (NIST 800-39; FEA; NIST 800-53: PL-8, SA-3, and SA-8)?	The organization has not defined an information security architecture and its processes for ensuring that new/acquired hardware/software are consistent with its security architecture prior to introducing systems into its development environment.	The organization has defined an information security architecture and described how that architecture is integrated into and supports the organization's enterprise architecture to provide a disciplined and structured methodology for managing risk. In addition, the organization has defined a process to conduct a security architecture review for new/acquired hardware/software prior to introducing systems into its development environment.	The organization has consistently implemented its security architecture across the enterprise, business process, and system levels. Security architecture reviews are consistently performed for new/acquired hardware/software prior to introducing systems into the organization's development environment.		
7. To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer, Chief Information Officer, Chief Information Security Officer, and other internal and external stakeholders and mission specific resources been defined and communicated across the organization (NIST 800-39: Section 2.3.1 and 2.3.2; NIST 800-53: RA-1; CSF: ID.RM-1 – ID.GV-2, OMB A-123, CFO Council ERM Playbook)?	Roles and responsibilities have not been defined and communicated across the organization.	Roles and responsibilities of stakeholders have been defined and communicated across the organization.	Roles and responsibilities of stakeholders involved in risk management have been defined and communicated across the organization. Stakeholders have adequate resources (people, processes, and technology) to effectively implement risk management activities.	The organization utilizes an integrated risk management governance structure for implementing and overseeing an enterprise risk management (ERM) capability that manages risks from information security, strategic planning and strategic reviews, internal control activities, and applicable mission/business areas.	The organization's risk management program addresses the full spectrum of an agency's risk portfolio across all organizational (major units, offices, and lines of business) and business (agency mission, programs, projects, etc.) aspects.



Final FY 2017 Inspector General FISMA Metrics v1.0
Identify Function Area (Risk Management)

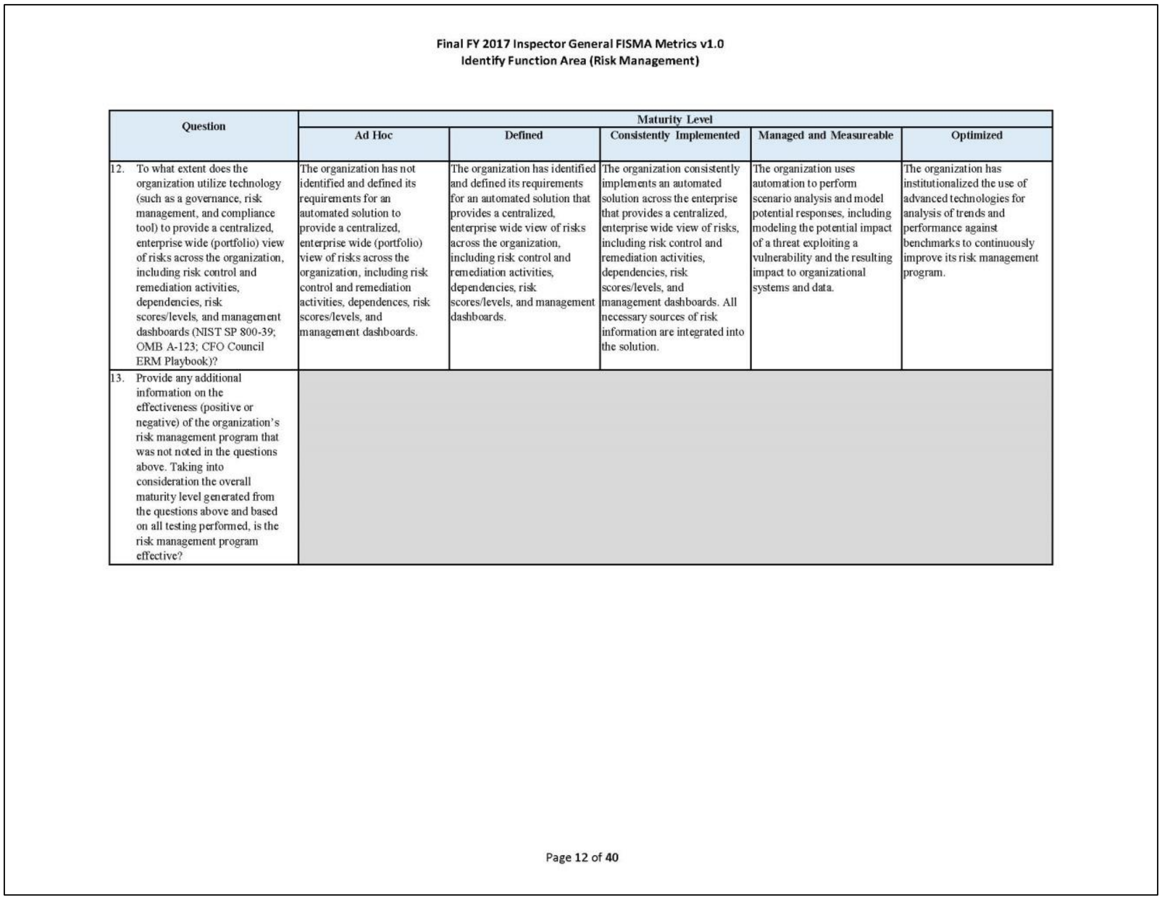
Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
8. To what extent has the organization ensured that plans of action and milestones (POA&Ms) are utilized for effectively mitigating security weaknesses (NIST SP 800-53: CA-5; OMB M-04-25)?	Policies and procedures for the effective use of POA&Ms to mitigate security weaknesses have not been defined and communicated.	Policies and procedures for the effective use of POA&Ms have been defined and communicated. These policies and procedures address, at a minimum, the centralized tracking of security weaknesses, prioritization of remediation efforts, maintenance, and independent validation of POA&M activities.	The organization consistently implements POA&Ms, in accordance with the organization's policies and procedures, to effectively mitigate security weaknesses.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its POA&M activities and uses that information to make appropriate adjustments, as needed, to ensure that its risk posture is maintained.	The organization employs automation to correlate security weaknesses amongst information systems and identify enterprise-wide trends and solutions on a near real-time basis. Furthermore, processes are in place to identify and manage emerging risks, in addition to known security weaknesses.
9. To what extent has the organization defined, communicated, and implemented its policies and procedures for conducting system level risk assessments, including for identifying and prioritizing (i) internal and external threats, including through use of the common vulnerability scoring system, or other equivalent framework (ii) internal and external asset vulnerabilities, including through vulnerability scanning, (iii) the potential likelihoods and business impacts/consequences of threats exploiting vulnerabilities, and (iv) selecting and implementing security controls to mitigate system-level risks (NIST 800-37; NIST 800-39; NIST 800-53: PL-2, RA-1; NIST 800-30; CSF:ID.RA-1 – 6)?	Policies and procedures for system level risk assessments and security control selections have not been defined and communicated.	Policies and procedures for system level risk assessments and security control selections are defined and communicated. In addition, the organization has developed a tailored set of baseline criteria that provides guidance regarding acceptable risk assessment approaches and controls to be evaluated tailored to organizational and system risk.	System risk assessments are performed and appropriate security controls are implemented on a consistent basis. The organization utilizes the common vulnerability scoring system, or similar approach, to communicate the characteristics and severity of software vulnerabilities.	The organization consistently monitors the effectiveness of risk responses to ensure that enterprise-wide risk tolerance is maintained at an appropriate level.	

Page 10 of 40



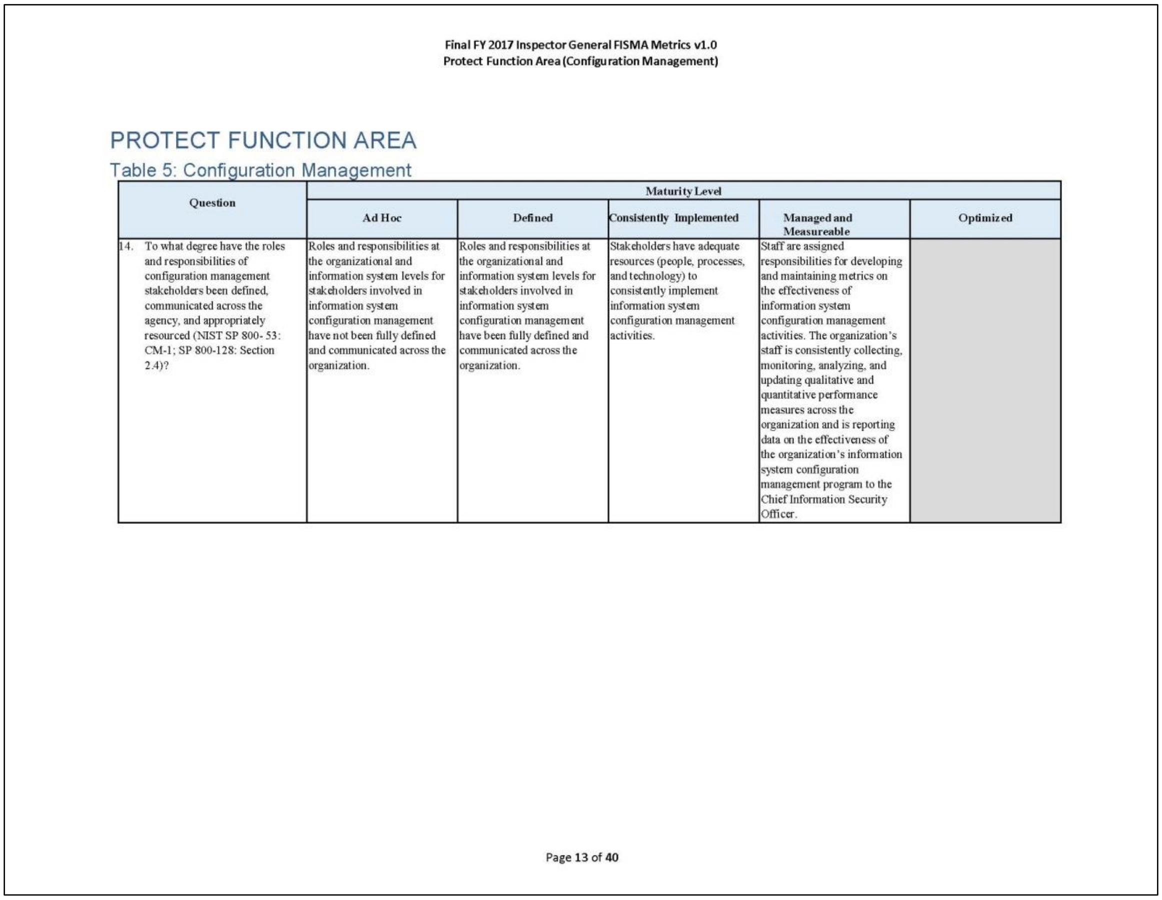
Final FY 2017 Inspector General FISMA Metrics v1.0
Identify Function Area (Risk Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
10. To what extent does the organization ensure that information about risks are communicated in a timely manner to all necessary internal and external stakeholders (CFO Council ERM Playbook; OMB A-123)?	The organization has not defined how information about risks are communicated in a timely manner to all necessary internal and external stakeholders.	The organization has defined how information about risks are communicated in a timely manner to all necessary internal and external stakeholders.	The organization ensures that information about risks is communicated in a timely and consistent manner to all internal and external stakeholders with a need-to-know. Furthermore, the organization actively shares information with partners to ensure that accurate, current information is being distributed and consumed.	The organization employs robust diagnostic and reporting frameworks, including dashboards that facilitate a portfolio view of interrelated risks across the organization. The dashboard presents qualitative and quantitative metrics that provide indicators of risk.	Through the use of risk profiles and dynamic reporting mechanisms, the risk management program provides a fully integrated, prioritized, enterprise-wide view of organizational risks to drive strategy and business decisions.
11. To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information) and SLAs are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services (FAR Case 2007-004; Common Security Configurations; FAR Sections: 24.104, 39.101, 39.105, 39.106, 52.239-1; President's Management Council; NIST 800-53: SA-4; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; FY 2017 CIO FISMA Metrics: 1.7, 1.8).	The organization has not defined a process that includes information security and other business areas as appropriate for ensuring that contracts and other agreements for contractor systems and services include appropriate clauses to monitor the risks related to such systems and services. Further, the organization has not defined its processes for ensuring appropriate information security oversight of contractor provided systems and services.	The organization has defined a process that includes information security and other business areas as appropriate for ensuring that contracts and other agreements for third party systems and services include appropriate clauses to monitor the risks related to such systems and services. In addition, the organization has defined its processes to ensure that security controls of systems or services provided by contractors or other entities on behalf of the organization meet FISMA requirements, OMB policy, and applicable NIST guidance.	The organization ensures that specific contracting language and SLAs are consistently included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services. Further, the organization obtains sufficient assurance that the security controls of systems or services provided by contractors or other entities on behalf of the organization meet FISMA requirements, OMB policy, and applicable NIST guidance.	The organization uses qualitative and quantitative performance metrics (e.g., those defined within SLAs) to measure, report on, and monitor information security performance of contractor-operated systems and services.	



Final FY 2017 Inspector General FISMA Metrics v1.0
Identify Function Area (Risk Management)

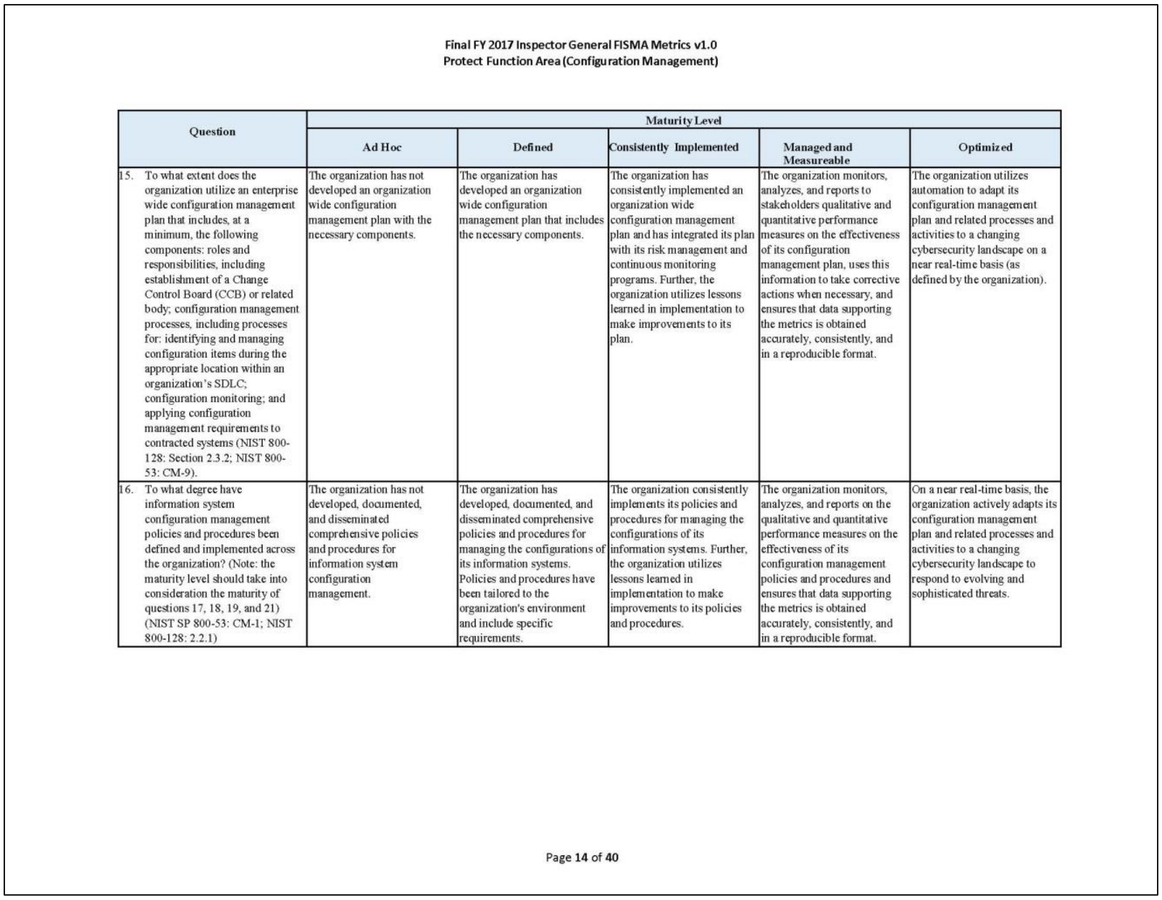
Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
12. To what extent does the organization utilize technology (such as a governance, risk management, and compliance tool) to provide a centralized, enterprise wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123; CFO Council ERM Playbook)?	The organization has not identified and defined its requirements for an automated solution to provide a centralized, enterprise wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependences, risk scores/levels, and management dashboards.	The organization has identified and defined its requirements for an automated solution that provides a centralized, enterprise wide view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards.	The organization consistently implements an automated solution across the enterprise that provides a centralized, enterprise wide view of risks, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards. All necessary sources of risk information are integrated into the solution.	The organization uses automation to perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting impact to organizational systems and data.	The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its risk management program.
13. 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. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?					



PROTECT FUNCTION AREA

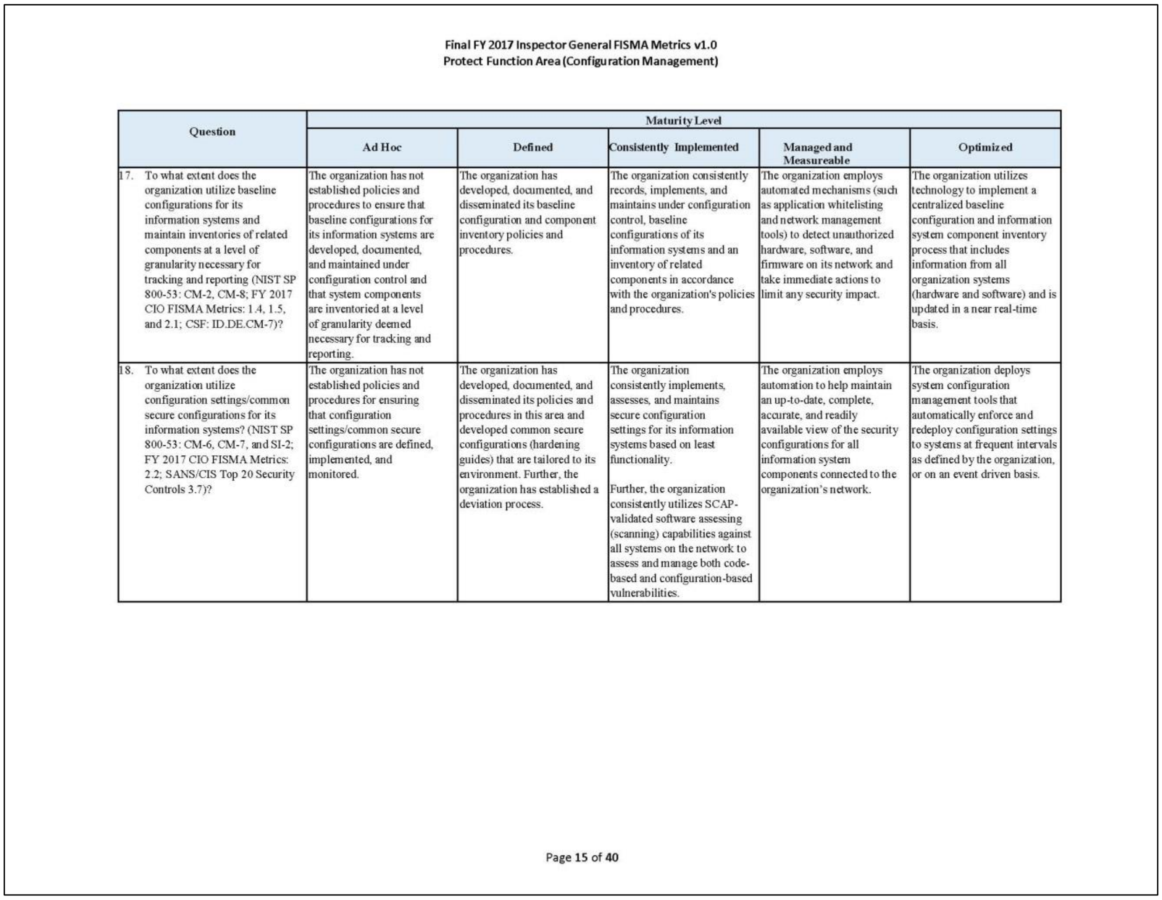
Table 5: Configuration Management

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
14. To what degree have the roles and responsibilities of configuration management stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800- 53: CM-1; SP 800-128: Section 2.4)?	Roles and responsibilities at the organizational and information system levels for stakeholders involved in information system configuration management have not been fully defined and communicated across the organization.	Roles and responsibilities at the organizational and information system levels for stakeholders involved in information system configuration management have been fully defined and communicated across the organization.	Stakeholders have adequate resources (people, processes, and technology) to consistently implement information system configuration management activities.	Staff are assigned responsibilities for developing and maintaining metrics on the effectiveness of information system configuration management activities. The organization's staff is consistently collecting, monitoring, analyzing, and updating qualitative and quantitative performance measures across the organization and is reporting data on the effectiveness of the organization's information system configuration management program to the Chief Information Security Officer.	



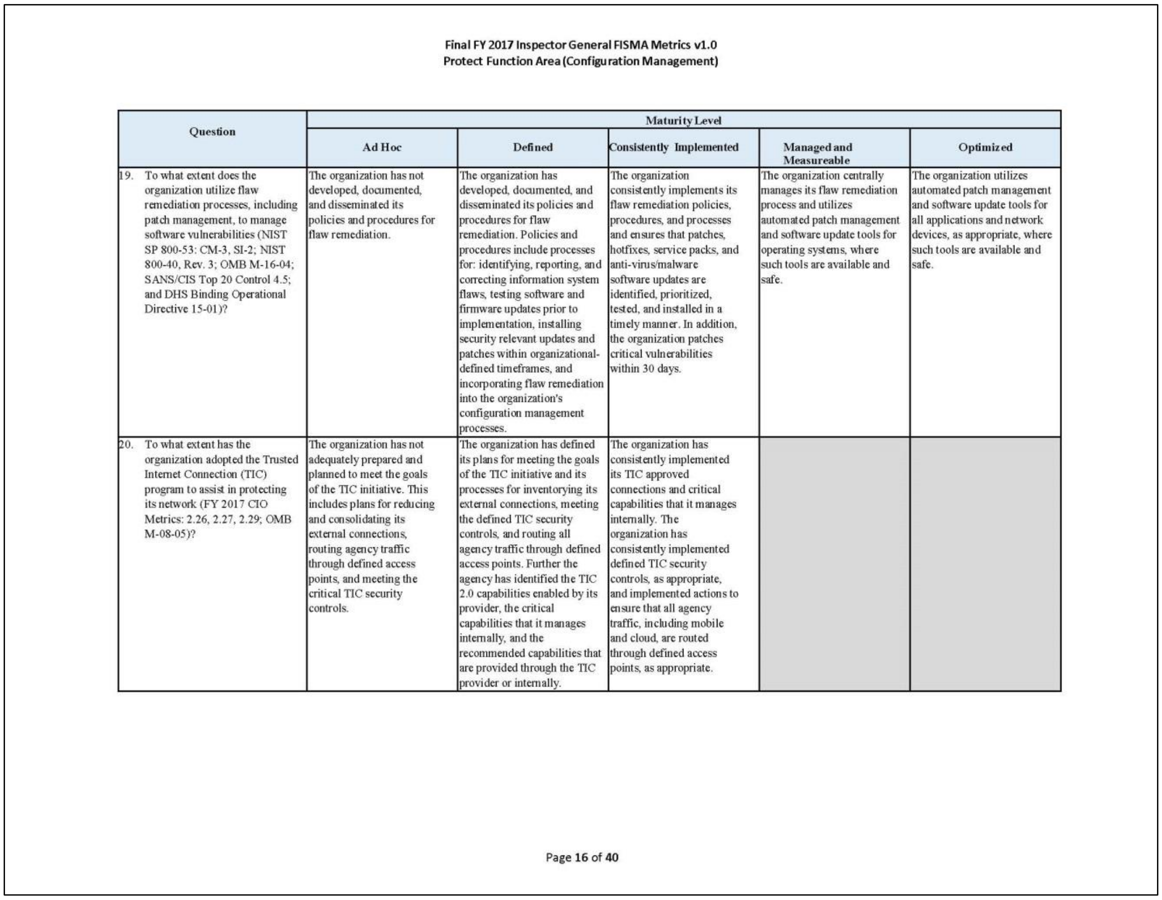
Final FY 2017 Inspector General FISMA Metrics v1.0
Protect Function Area (Configuration Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
15. To what extent does the organization utilize an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate location within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contracted systems (NIST 800-128: Section 2.3.2; NIST 800-53: CM-9).	The organization has not developed an organization wide configuration management plan with the necessary components.	The organization has developed an organization wide configuration management plan that includes the necessary components.	The organization has consistently implemented an organization wide configuration management plan and has integrated its plan with its risk management and continuous monitoring programs. Further, the organization utilizes lessons learned in implementation to make improvements to its plan.	The organization monitors, analyzes, and reports to stakeholders qualitative and quantitative performance measures on the effectiveness of its configuration management plan, uses this information to take corrective actions when necessary, and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.	The organization utilizes automation to adapt its configuration management plan and related processes and activities to a changing cybersecurity landscape on a near real-time basis (as defined by the organization).
16. To what degree have information system configuration management policies and procedures been defined and implemented across the organization? (Note: the maturity level should take into consideration the maturity of questions 17, 18, 19, and 21) (NIST SP 800-53: CM-1; NIST 800-128: 2.2.1)	The organization has not developed, documented, and disseminated comprehensive policies and procedures for information system configuration management.	The organization has developed, documented, and disseminated comprehensive policies and procedures for managing the configurations of its information systems. Policies and procedures have been tailored to the organization's environment and include specific requirements.	The organization consistently implements its policies and procedures for managing the configurations of its information systems. Further, the organization utilizes lessons learned in implementation to make improvements to its policies and procedures.	The organization monitors, analyzes, and reports on the qualitative and quantitative performance measures on the effectiveness of its configuration management policies and procedures and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.	On a near real-time basis, the organization actively adapts its configuration management plan and related processes and activities to a changing cybersecurity landscape to respond to evolving and sophisticated threats.



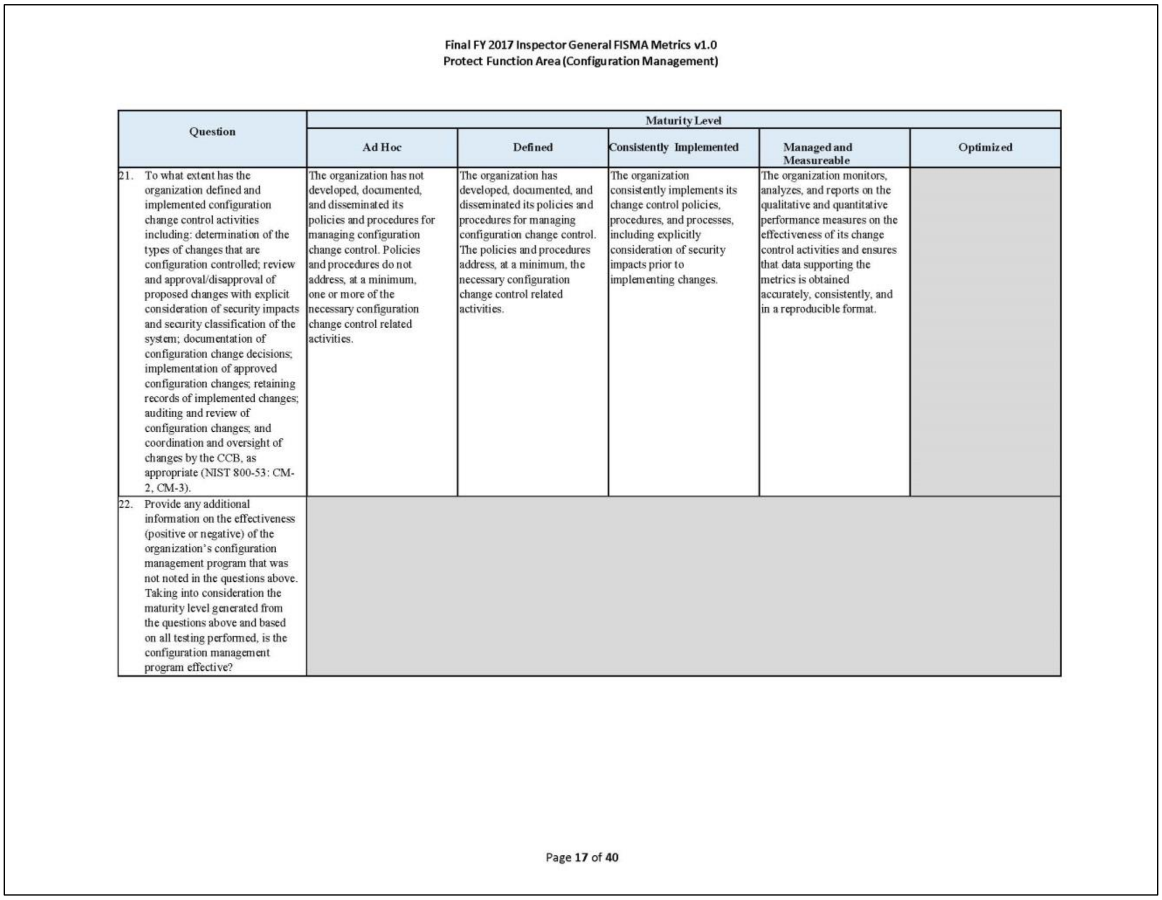
Final FY 2017 Inspector General FISMA Metrics v1.0
Protect Function Area (Configuration Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
17. To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53: CM-2, CM-8; FY 2017 CIO FISMA Metrics: 1.4, 1.5, and 2.1; CSF: ID.DE.CM-7)?	The organization has not established policies and procedures to ensure that baseline configurations for its information systems are developed, documented, and maintained under configuration control and that system components are inventoried at a level of granularity deemed necessary for tracking and reporting.	The organization has developed, documented, and disseminated its baseline configuration and component inventory policies and procedures.	The organization consistently records, implements, and maintains under configuration control, baseline configurations of its information systems and an inventory of related components in accordance with the organization's policies and procedures.	The organization employs automated mechanisms (such as application whitelisting and network management tools) to detect unauthorized hardware, software, and firmware on its network and take immediate actions to limit any security impact.	The organization utilizes technology to implement a centralized baseline configuration and information system component inventory process that includes information from all organization systems (hardware and software) and is updated in a near real-time basis.
18. To what extent does the organization utilize configuration settings/common secure configurations for its information systems? (NIST SP 800-53: CM-6, CM-7, and SI-2; FY 2017 CIO FISMA Metrics: 2.2; SANS/CIS Top 20 Security Controls 3.7)?	The organization has not established policies and procedures for ensuring that configuration settings/common secure configurations are defined, implemented, and monitored.	The organization has developed, documented, and disseminated its policies and procedures in this area and developed common secure configurations (hardening guides) that are tailored to its environment. Further, the organization has established a deviation process.	The organization consistently implements, assesses, and maintains secure configuration settings for its information systems based on least functionality. Further, the organization consistently utilizes SCAP-validated software assessing (scanning) capabilities against all systems on the network to assess and manage both code-based and configuration-based vulnerabilities.	The organization employs automation to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for all information system components connected to the organization's network.	The organization deploys system configuration management tools that automatically enforce and redeploy configuration settings to systems at frequent intervals as defined by the organization, or on an event driven basis.



Final FY 2017 Inspector General FISMA Metrics v1.0
Protect Function Area (Configuration Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
19. To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53: CM-3, SI-2; NIST 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20 Control 4.5; and DHS Binding Operational Directive 15-01)?	The organization has not developed, documented, and disseminated its policies and procedures for flaw remediation.	The organization has developed, documented, and disseminated its policies and procedures for flaw remediation. Policies and procedures include processes for: identifying, reporting, and correcting information system flaws, testing software and firmware updates prior to implementation, installing security relevant updates and patches within organizational-defined timeframes, and incorporating flaw remediation into the organization's configuration management processes.	The organization consistently implements its flaw remediation policies, procedures, and processes and ensures that patches, hotfixes, service packs, and anti-virus/malware software updates are identified, prioritized, tested, and installed in a timely manner. In addition, the organization patches critical vulnerabilities within 30 days.	The organization centrally manages its flaw remediation process and utilizes automated patch management and software update tools for operating systems, where such tools are available and safe.	The organization utilizes automated patch management and software update tools for all applications and network devices, as appropriate, where such tools are available and safe.
20. To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (FY 2017 CIO Metrics: 2.26, 2.27, 2.29; OMB M-08-05)?	The organization has not adequately prepared and planned to meet the goals of the TIC initiative. This includes plans for reducing and consolidating its external connections, routing agency traffic through defined access points, and meeting the critical TIC security controls.	The organization has defined its plans for meeting the goals of the TIC initiative and its processes for inventorying its external connections, meeting the defined TIC security controls, and routing all agency traffic through defined access points. Further the agency has identified the TIC 2.0 capabilities enabled by its provider, the critical capabilities that it manages internally, and the recommended capabilities that are provided through the TIC provider or internally.	The organization has consistently implemented its TIC approved connections and critical capabilities that it manages internally. The organization has consistently implemented defined TIC security controls, as appropriate, and implemented actions to ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate.		



Final FY 2017 Inspector General FISMA Metrics v1.0
Protect Function Area (Configuration Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
21. To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, as appropriate (NIST 800-53: CM-2, CM-3).	The organization has not developed, documented, and disseminated its policies and procedures for managing configuration change control. Policies and procedures do not address, at a minimum, one or more of the necessary configuration change control related activities.	The organization has developed, documented, and disseminated its policies and procedures for managing configuration change control. The policies and procedures address, at a minimum, the necessary configuration change control related activities.	The organization consistently implements its change control policies, procedures, and processes, including explicitly consideration of security impacts prior to implementing changes.	The organization monitors, analyzes, and reports on the qualitative and quantitative performance measures on the effectiveness of its change control activities and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.	
22. 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. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?					

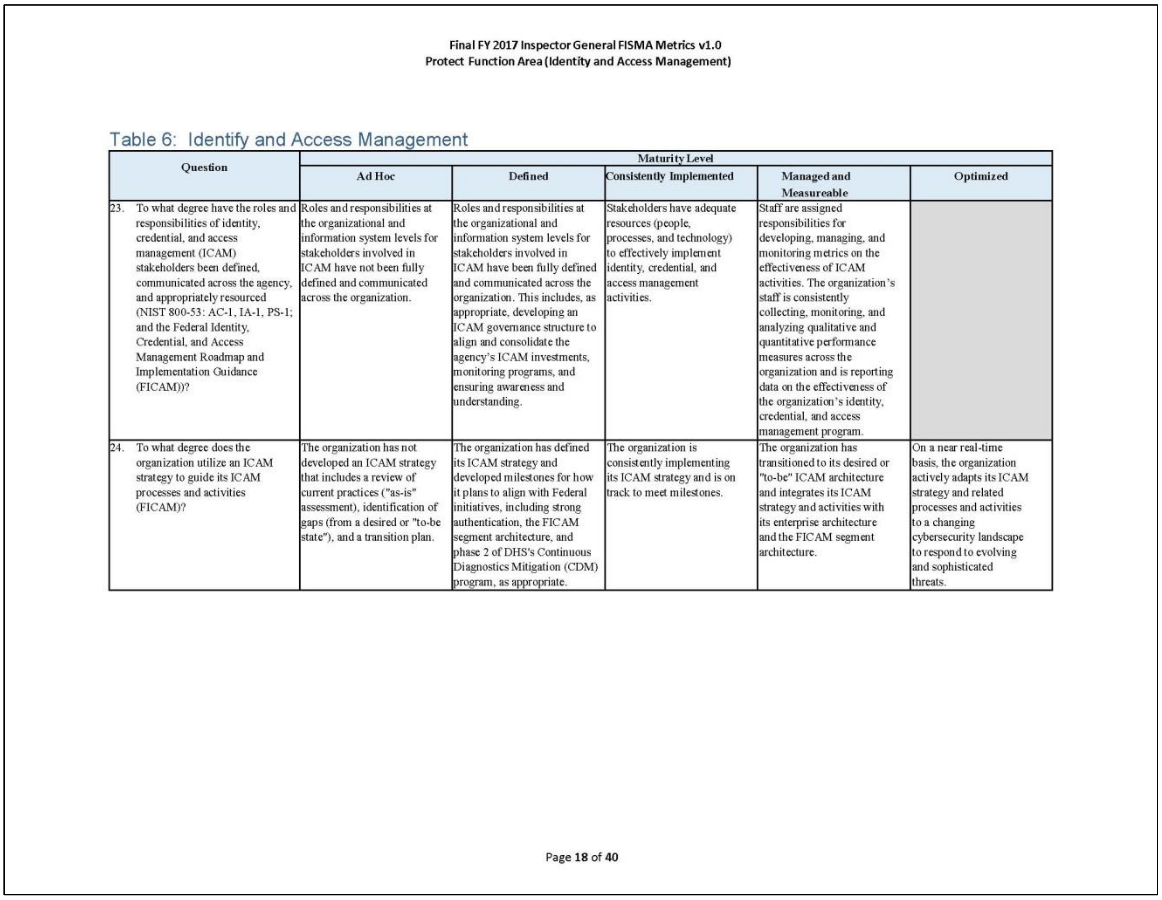
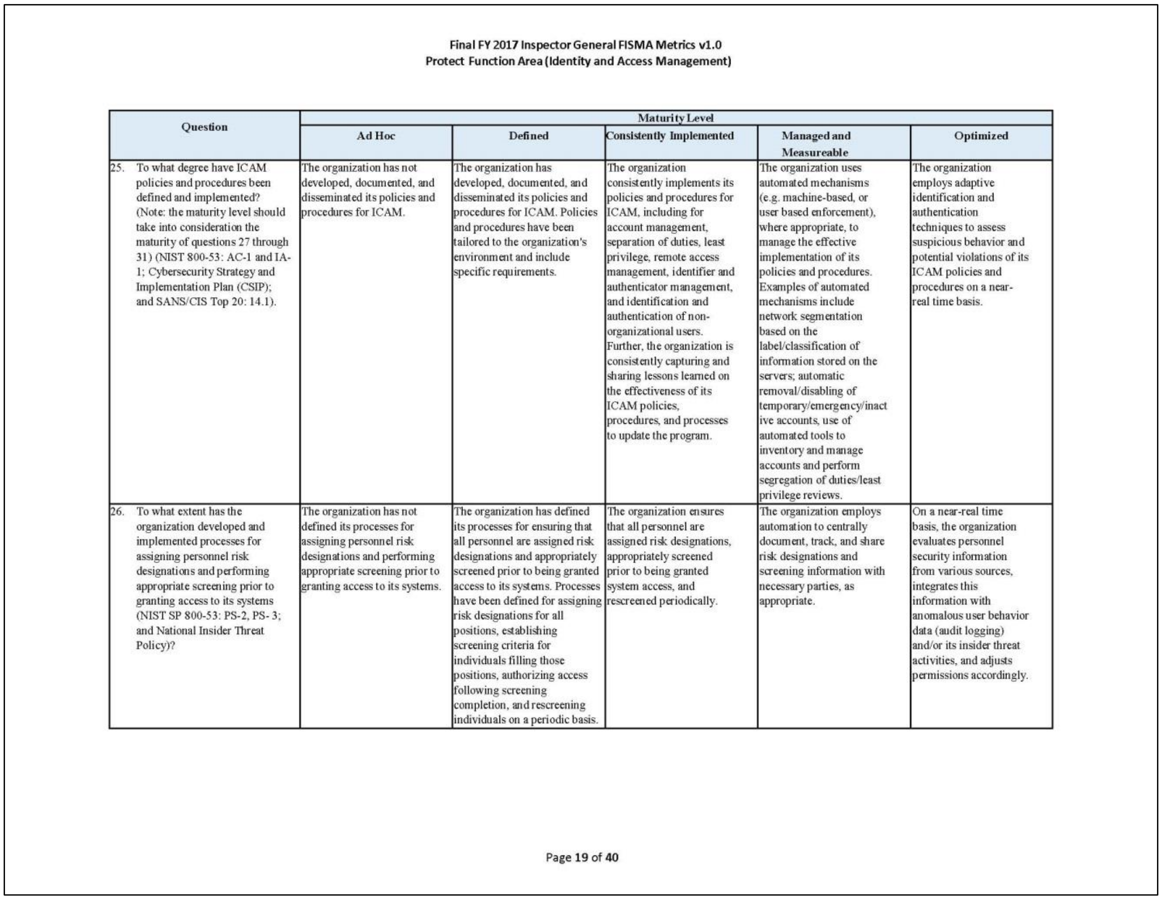


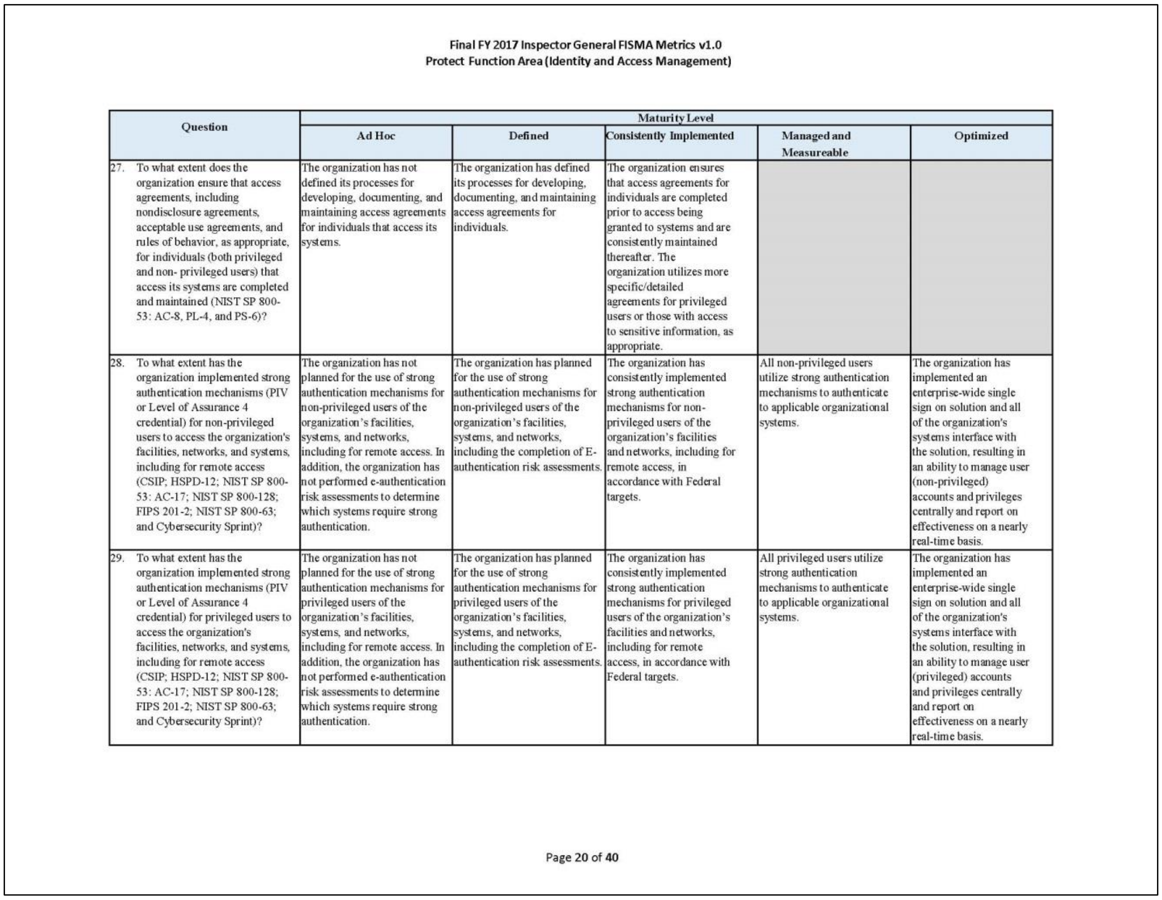
Table 6: Identify and Access Management

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
23. To what degree have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated across the agency, and appropriately resourced (NIST 800-53: AC-1, IA-1, PS-1; and the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?	Roles and responsibilities at the organizational and information system levels for stakeholders involved in ICAM have not been fully defined and communicated across the organization.	Roles and responsibilities at the organizational and information system levels for stakeholders involved in ICAM have been fully defined and communicated across the organization. This includes, as appropriate, developing an ICAM governance structure to align and consolidate the agency's ICAM investments, monitoring programs, and ensuring awareness and understanding.	Stakeholders have adequate resources (people, processes, and technology) to effectively implement identity, credential, and access management activities.	Staff are assigned responsibilities for developing, managing, and monitoring metrics on the effectiveness of ICAM activities. The organization's staff is consistently collecting, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is reporting data on the effectiveness of the organization's identity, credential, and access management program.	▨
24. To what degree does the organization utilize an ICAM strategy to guide its ICAM processes and activities (FICAM)?	The organization has not developed an ICAM strategy that includes a review of current practices ("as-is" assessment), identification of gaps (from a desired or "to-be state"), and a transition plan.	The organization has defined its ICAM strategy and developed milestones for how it plans to align with Federal initiatives, including strong authentication, the FICAM segment architecture, and phase 2 of DHS's Continuous Diagnostics Mitigation (CDM) program, as appropriate.	The organization is consistently implementing its ICAM strategy and is on track to meet milestones.	The organization has transitioned to its desired or "to-be" ICAM architecture and integrates its ICAM strategy and activities with its enterprise architecture and the FICAM segment architecture.	On a near real-time basis, the organization actively adapts its ICAM strategy and related processes and activities to a changing cybersecurity landscape to respond to evolving and sophisticated threats.



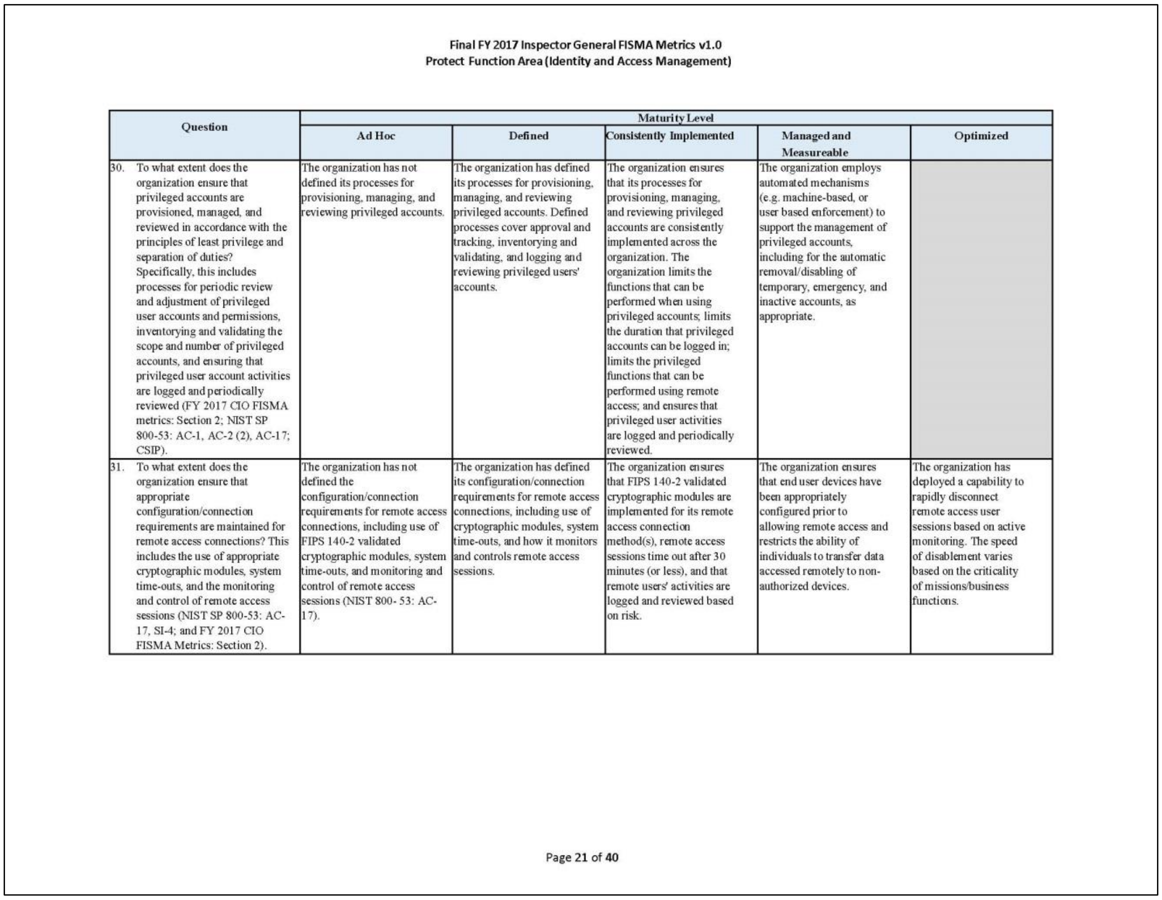
Final FY 2017 Inspector General FISMA Metrics v1.0
Protect Function Area (Identity and Access Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
25. To what degree have ICAM policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 27 through 31) (NIST 800-53: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); and SANS/CIS Top 20: 14.1).	The organization has not developed, documented, and disseminated its policies and procedures for ICAM.	The organization has developed, documented, and disseminated its policies and procedures for ICAM. Policies and procedures have been tailored to the organization's environment and include specific requirements.	The organization consistently implements its policies and procedures for ICAM, including for account management, separation of duties, least privilege, remote access management, identifier and authenticator management, and identification and authentication of non-organizational users. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its ICAM policies, procedures, and processes to update the program.	The organization uses automated mechanisms (e.g. machine-based, or user based enforcement), where appropriate, to manage the effective implementation of its policies and procedures. Examples of automated mechanisms include network segmentation based on the label/classification of information stored on the servers; automatic removal/disabling of temporary/emergency/inactive accounts, use of automated tools to inventory and manage accounts and perform segregation of duties/least privilege reviews.	The organization employs adaptive identification and authentication techniques to assess suspicious behavior and potential violations of its ICAM policies and procedures on a near-real time basis.
26. To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems (NIST SP 800-53: PS-2, PS- 3; and National Insider Threat Policy)?	The organization has not defined its processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems.	The organization has defined its processes for ensuring that all personnel are assigned risk designations and appropriately screened prior to being granted access to its systems. Processes have been defined for assigning risk designations for all positions, establishing screening criteria for individuals filling those positions, authorizing access following screening completion, and rescreening individuals on a periodic basis.	The organization ensures that all personnel are assigned risk designations, appropriately screened prior to being granted system access, and rescreened periodically.	The organization employs automation to centrally document, track, and share risk designations and screening information with necessary parties, as appropriate.	On a near-real time basis, the organization evaluates personnel security information from various sources, integrates this information with anomalous user behavior data (audit logging) and/or its insider threat activities, and adjusts permissions accordingly.



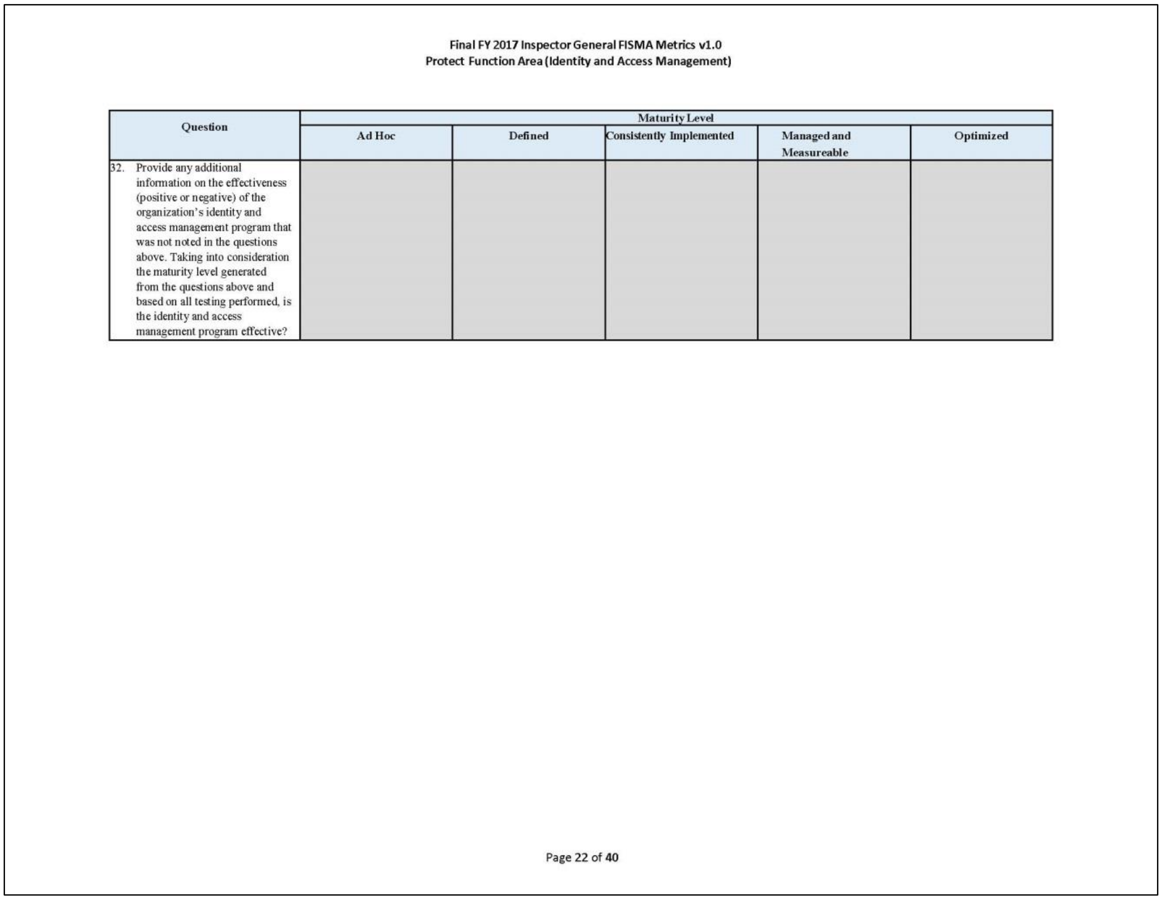
Final FY 2017 Inspector General FISMA Metrics v1.0
Protect Function Area (Identity and Access Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
27. To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non- privileged users) that access its systems are completed and maintained (NIST SP 800-53: AC-8, PL-4, and PS-6)?	The organization has not defined its processes for developing, documenting, and maintaining access agreements for individuals that access its systems.	The organization has defined its processes for developing, documenting, and maintaining access agreements for individuals.	The organization ensures that access agreements for individuals are completed prior to access being granted to systems and are consistently maintained thereafter. The organization utilizes more specific/detailed agreements for privileged users or those with access to sensitive information, as appropriate.		
28. To what extent has the organization implemented strong authentication mechanisms (PIV or Level of Assurance 4 credential) for non-privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; and Cybersecurity Sprint)?	The organization has not planned for the use of strong authentication mechanisms for non-privileged users of the organization's facilities, systems, and networks, including for remote access. In addition, the organization has not performed e-authentication risk assessments to determine which systems require strong authentication.	The organization has planned for the use of strong authentication mechanisms for non-privileged users of the organization's facilities, systems, and networks, including the completion of E-authentication risk assessments.	The organization has consistently implemented strong authentication mechanisms for non-privileged users of the organization's facilities and networks, including for remote access, in accordance with Federal targets.	All non-privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems.	The organization has implemented an enterprise-wide single sign on solution and all of the organization's systems interface with the solution, resulting in an ability to manage user (non-privileged) accounts and privileges centrally and report on effectiveness on a nearly real-time basis.
29. To what extent has the organization implemented strong authentication mechanisms (PIV or Level of Assurance 4 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; and Cybersecurity Sprint)?	The organization has not planned for the use of strong authentication mechanisms for privileged users of the organization's facilities, systems, and networks, including for remote access. In addition, the organization has not performed e-authentication risk assessments to determine which systems require strong authentication.	The organization has planned for the use of strong authentication mechanisms for privileged users of the organization's facilities, systems, and networks, including the completion of E-authentication risk assessments.	The organization has consistently implemented strong authentication mechanisms for privileged users of the organization's facilities and networks, including for remote access, in accordance with Federal targets.	All privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems.	The organization has implemented an enterprise-wide single sign on solution and all of the organization's systems interface with the solution, resulting in an ability to manage user (privileged) accounts and privileges centrally and report on effectiveness on a nearly real-time basis.



Final FY 2017 Inspector General FISMA Metrics v1.0
Protect Function Area (Identity and Access Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
30. To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed (FY 2017 CIO FISMA metrics: Section 2; NIST SP 800-53: AC-1, AC-2 (2), AC-17; CSIP).	The organization has not defined its processes for provisioning, managing, and reviewing privileged accounts.	The organization has defined its processes for provisioning, managing, and reviewing privileged accounts. Defined processes cover approval and tracking, inventorying and validating, and logging and reviewing privileged users' accounts.	The organization ensures that its processes for provisioning, managing, and reviewing privileged accounts are consistently implemented across the organization. The organization limits the functions that can be performed when using privileged accounts; limits the duration that privileged accounts can be logged in; limits the privileged functions that can be performed using remote access; and ensures that privileged user activities are logged and periodically reviewed.	The organization employs automated mechanisms (e.g. machine-based, or user based enforcement) to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate.	
31. To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions (NIST SP 800-53: AC-17, SI-4; and FY 2017 CIO FISMA Metrics: Section 2).	The organization has not defined the configuration/connection requirements for remote access connections, including use of FIPS 140-2 validated cryptographic modules, system time-outs, and monitoring and control of remote access sessions (NIST 800- 53: AC-17).	The organization has defined its configuration/connection requirements for remote access connections, including use of cryptographic modules, system time-outs, and how it monitors and controls remote access sessions.	The organization ensures that FIPS 140-2 validated cryptographic modules are implemented for its remote access connection method(s), remote access sessions time out after 30 minutes (or less), and that remote users' activities are logged and reviewed based on risk.	The organization ensures that end user devices have been appropriately configured prior to allowing remote access and restricts the ability of individuals to transfer data accessed remotely to non-authorized devices.	The organization has deployed a capability to rapidly disconnect remote access user sessions based on active monitoring. The speed of disablement varies based on the criticality of missions/business functions.



Final FY 2017 Inspector General FISMA Metrics v1.0
Protect Function Area (Identity and Access Management)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
32. 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. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?					

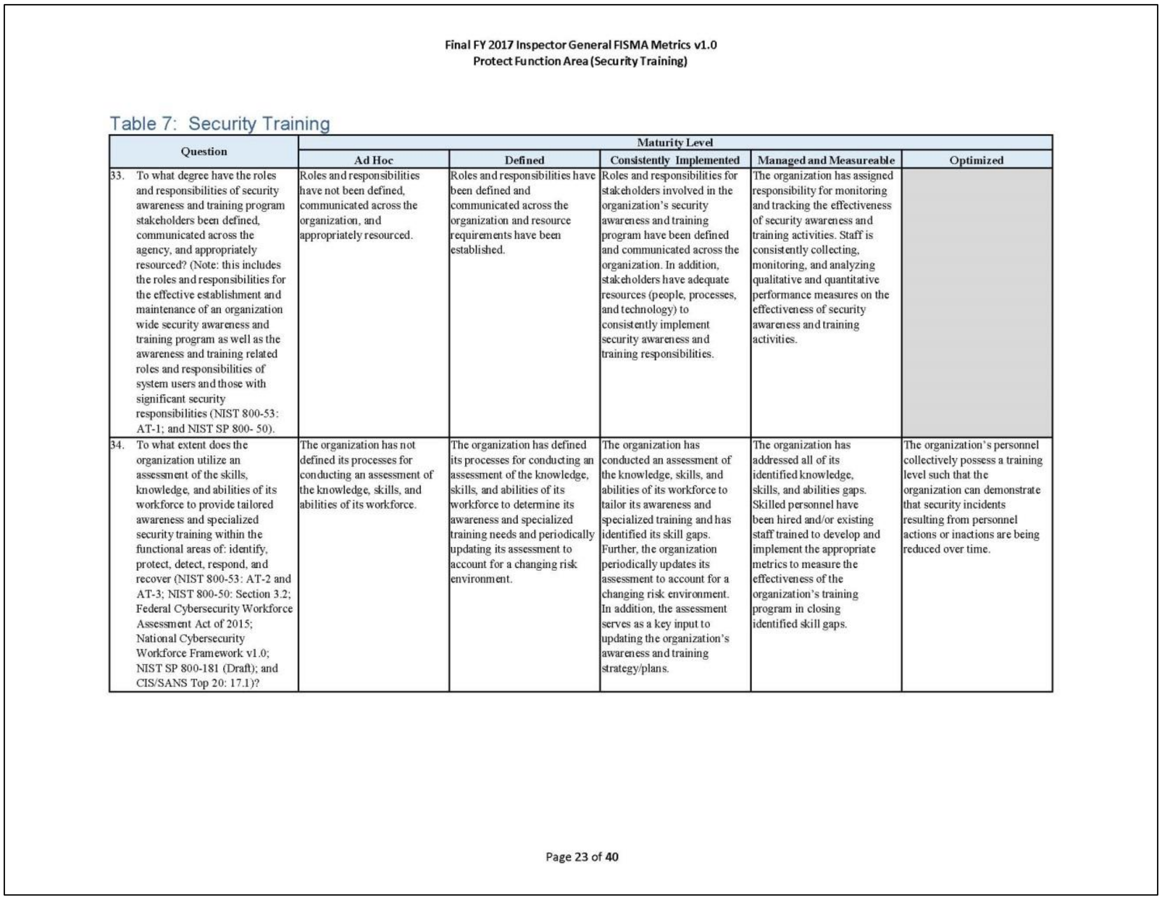
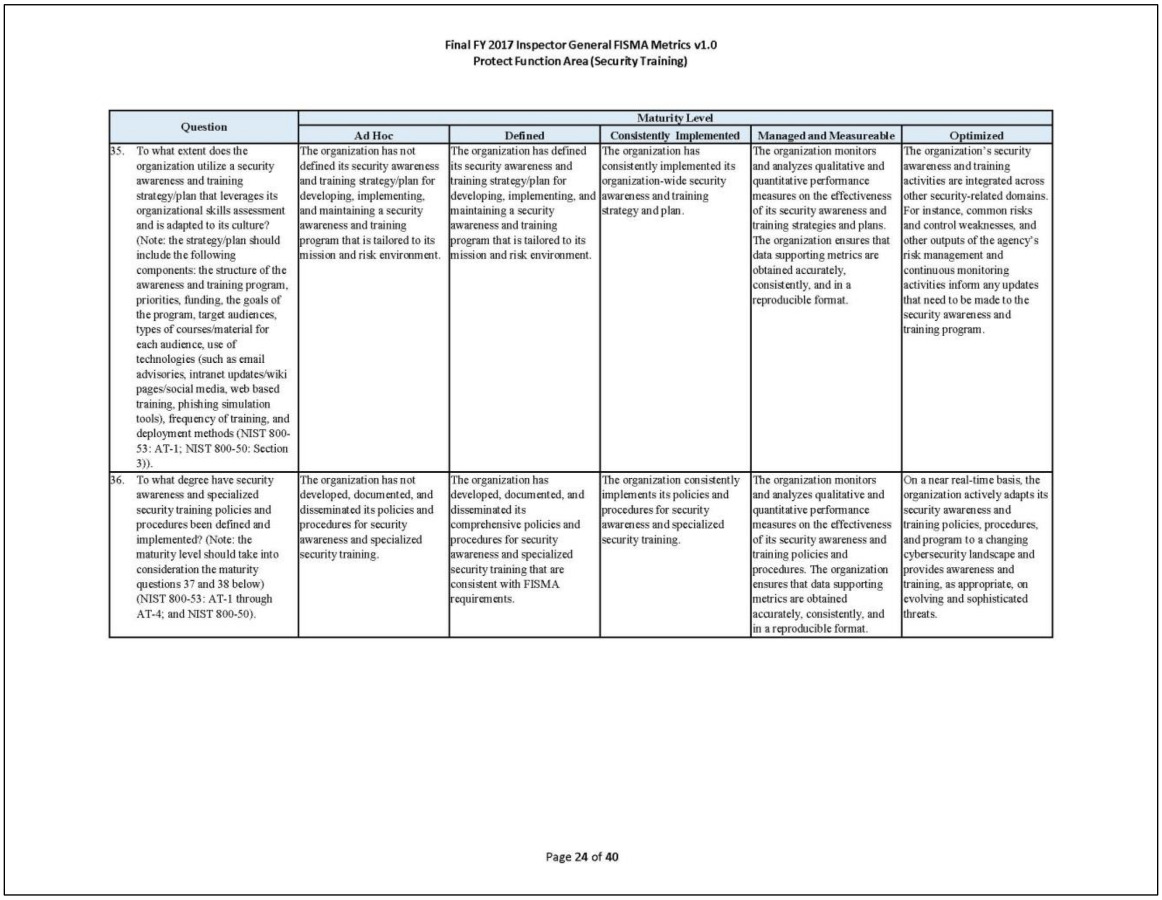


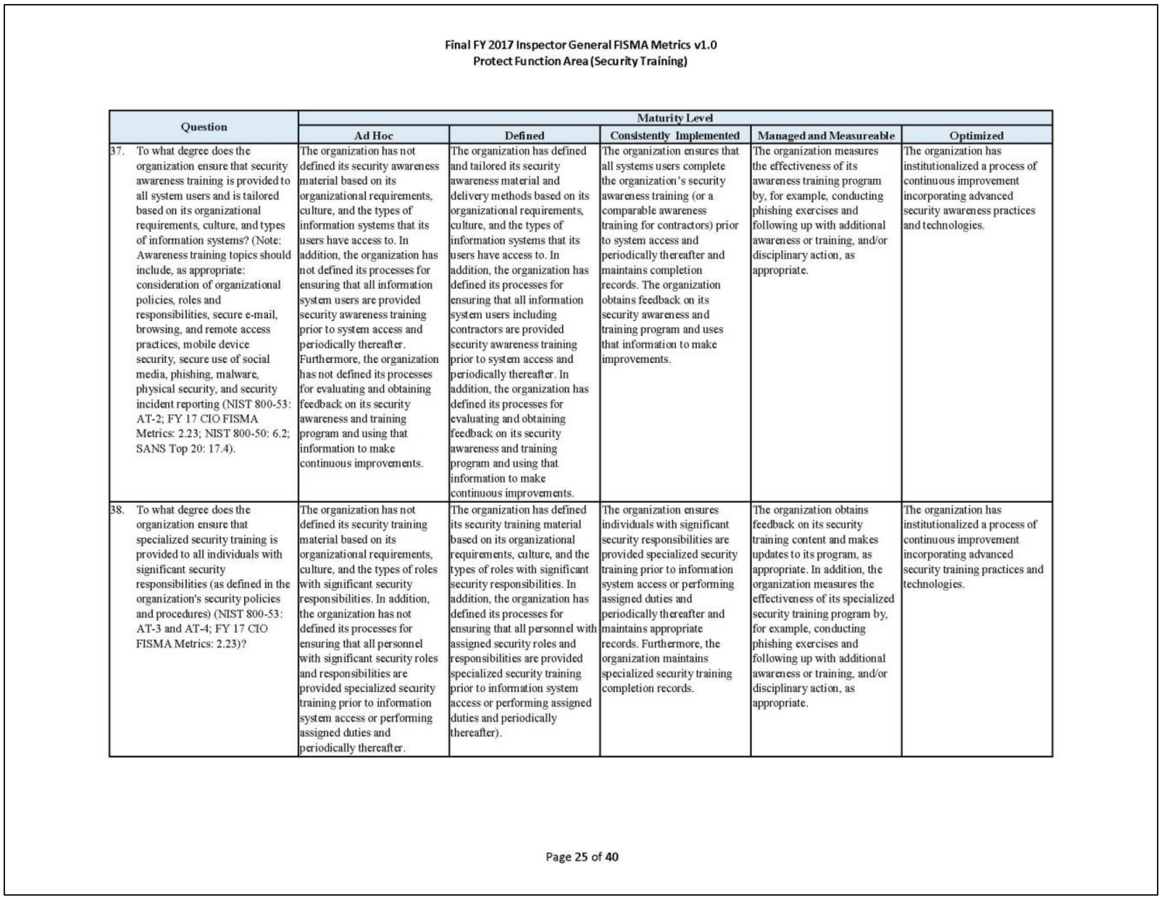
Table 7: Security Training

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
33. To what degree have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated across the agency, and appropriately resourced? (Note: this includes the roles and responsibilities for the effective establishment and maintenance of an organization wide security awareness and training program as well as the awareness and training related roles and responsibilities of system users and those with significant security responsibilities (NIST 800-53: AT-1; and NIST SP 800- 50).	Roles and responsibilities have not been defined, communicated across the organization, and appropriately resourced.	Roles and responsibilities have been defined and communicated across the organization and resource requirements have been established.	Roles and responsibilities for stakeholders involved in the organization's security awareness and training program have been defined and communicated across the organization. In addition, stakeholders have adequate resources (people, processes, and technology) to consistently implement security awareness and training responsibilities.	The organization has assigned responsibility for monitoring and tracking the effectiveness of security awareness and training activities. Staff is consistently collecting, monitoring, and analyzing qualitative and quantitative performance measures on the effectiveness of security awareness and training activities.	
34. To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover (NIST 800-53: AT-2 and AT-3; NIST 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181 (Draft); and CIS/SANS Top 20: 17.1)?	The organization has not defined its processes for conducting an assessment of the knowledge, skills, and abilities of its workforce.	The organization has defined its processes for conducting an assessment of the knowledge, skills, and abilities of its workforce to determine its awareness and specialized training needs and periodically updating its assessment to account for a changing risk environment.	The organization has conducted an assessment of the knowledge, skills, and abilities of its workforce to tailor its awareness and specialized training and has identified its skill gaps. Further, the organization periodically updates its assessment to account for a changing risk environment. In addition, the assessment serves as a key input to updating the organization's awareness and training strategy/plans.	The organization has addressed all of its identified knowledge, skills, and abilities gaps. Skilled personnel have been hired and/or existing staff trained to develop and implement the appropriate metrics to measure the effectiveness of the organization's training program in closing identified skill gaps.	The organization's personnel collectively possess a training level such that the organization can demonstrate that security incidents resulting from personnel actions or inactions are being reduced over time.



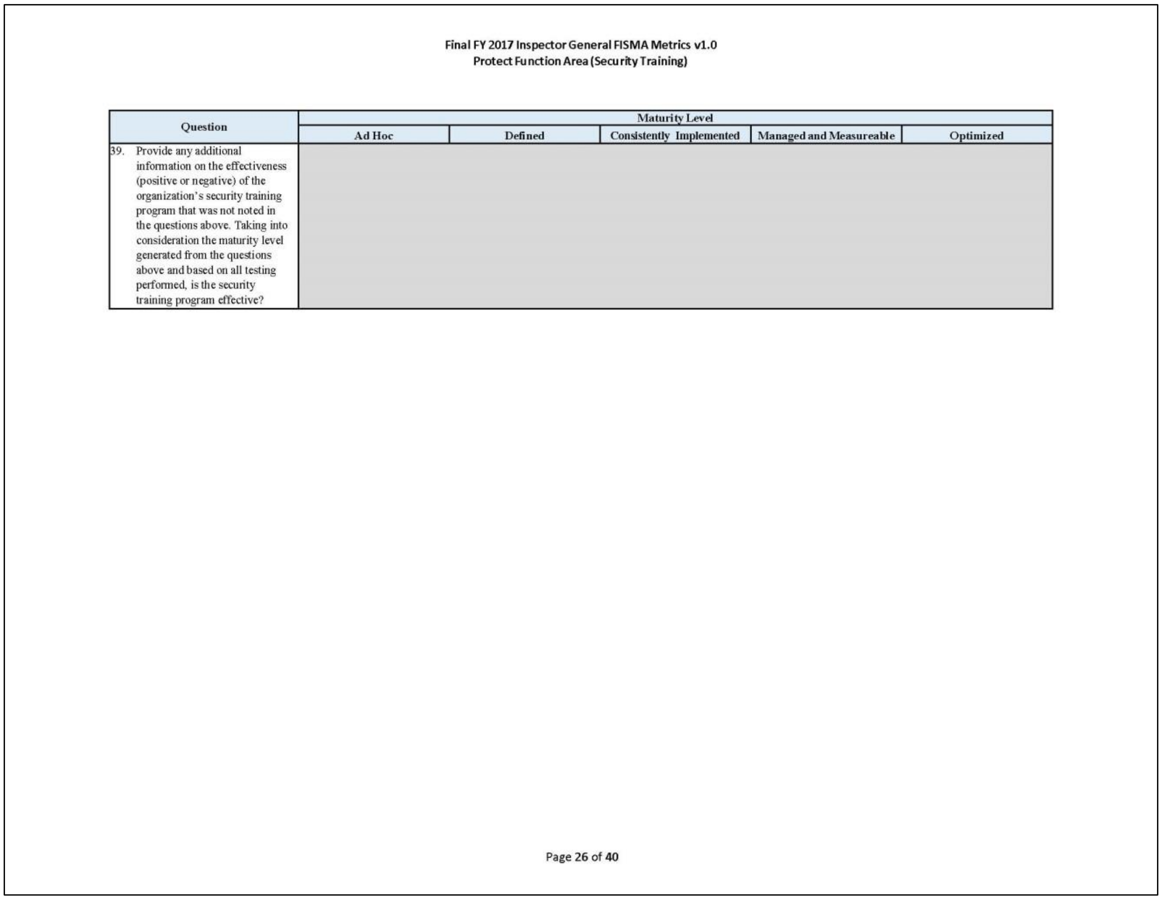
Final FY 2017 Inspector General FISMA Metrics v1.0
Protect Function Area (Security Training)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
35. To what extent does the organization utilize a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to its culture? (Note: the strategy/plan should include the following components: the structure of the awareness and training program, priorities, funding, the goals of the program, target audiences, types of courses/material for each audience, use of technologies (such as email advisories, intranet updates/wiki pages/social media, web based training, phishing simulation tools), frequency of training, and deployment methods (NIST 800-53: AT-1; NIST 800-50: Section 3)).	The organization has not defined its security awareness and training strategy/plan for developing, implementing, and maintaining a security awareness and training program that is tailored to its mission and risk environment.	The organization has defined its security awareness and training strategy/plan for developing, implementing, and maintaining a security awareness and training program that is tailored to its mission and risk environment.	The organization has consistently implemented its organization-wide security awareness and training strategy and plan.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization's security awareness and training activities are integrated across other security-related domains. For instance, common risks and control weaknesses, and other outputs of the agency's risk management and continuous monitoring activities inform any updates that need to be made to the security awareness and training program.
36. To what degree have security awareness and specialized security training policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity questions 37 and 38 below) (NIST 800-53: AT-1 through AT-4; and NIST 800-50).	The organization has not developed, documented, and disseminated its policies and procedures for security awareness and specialized security training.	The organization has developed, documented, and disseminated its comprehensive policies and procedures for security awareness and specialized security training that are consistent with FISMA requirements.	The organization consistently implements its policies and procedures for security awareness and specialized security training.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness and training policies and procedures. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	On a near real-time basis, the organization actively adapts its security awareness and training policies, procedures, and program to a changing cybersecurity landscape and provides awareness and training, as appropriate, on evolving and sophisticated threats.



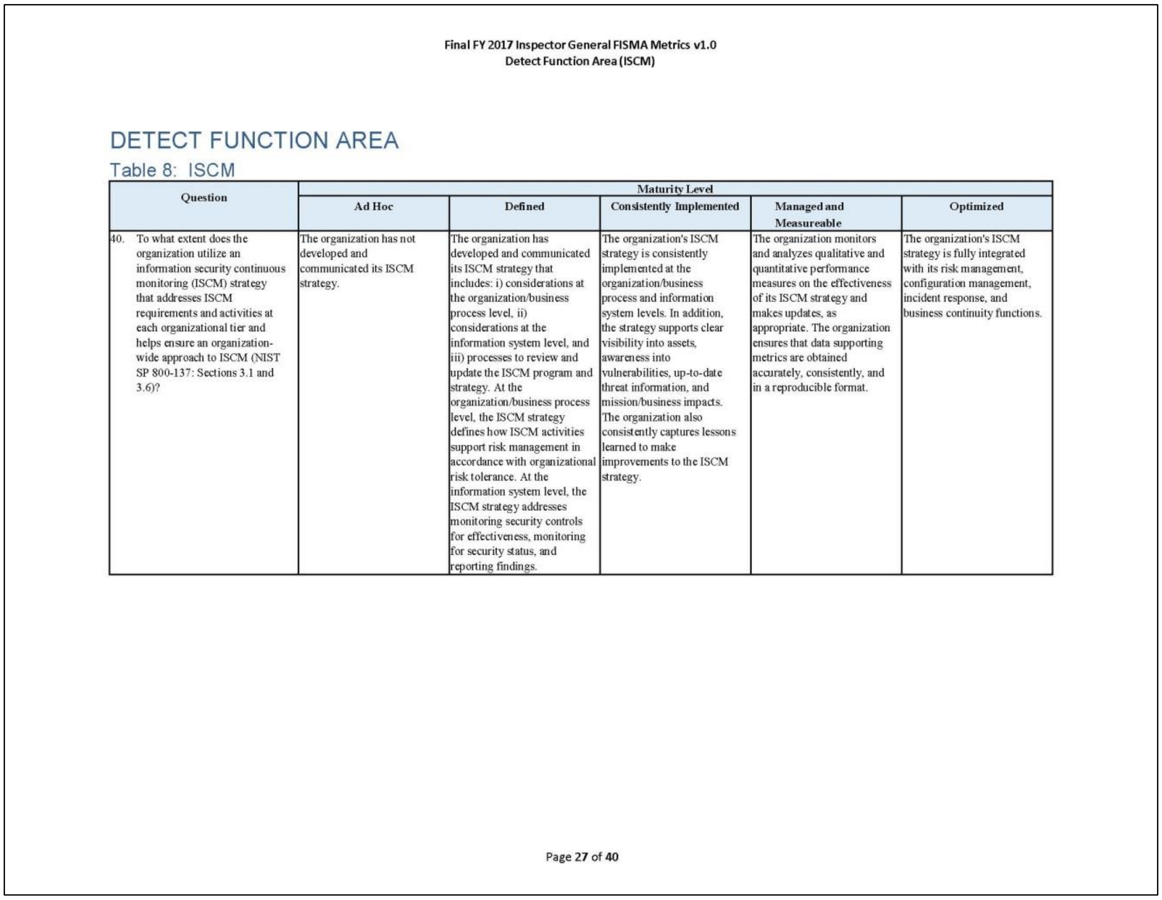
Final FY 2017 Inspector General FISMA Metrics v1.0
Protect Function Area (Security Training)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
37. To what degree does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, and types of information systems? (Note: Awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting (NIST 800-53: AT-2; FY 17 CIO FISMA Metrics: 2.23; NIST 800-50: 6.2; SANS Top 20: 17.4).	The organization has not defined its security awareness material based on its organizational requirements, culture, and the types of information systems that its users have access to. In addition, the organization has not defined its processes for ensuring that all information system users are provided security awareness training prior to system access and periodically thereafter. Furthermore, the organization has not defined its processes for evaluating and obtaining feedback on its security awareness and training program and using that information to make continuous improvements.	The organization has defined and tailored its security awareness material and delivery methods based on its organizational requirements, culture, and the types of information systems that its users have access to. In addition, the organization has defined its processes for ensuring that all information system users including contractors are provided security awareness training prior to system access and periodically thereafter. In addition, the organization has defined its processes for evaluating and obtaining feedback on its security awareness and training program and using that information to make continuous improvements.	The organization ensures that all systems users complete the organization's security awareness training (or a comparable awareness training for contractors) prior to system access and periodically thereafter and maintains completion records. The organization obtains feedback on its security awareness and training program and uses that information to make improvements.	The organization measures the effectiveness of its awareness training program by, for example, conducting phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate.	The organization has institutionalized a process of continuous improvement incorporating advanced security awareness practices and technologies.
38. To what degree does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures) (NIST 800-53: AT-3 and AT-4; FY 17 CIO FISMA Metrics: 2.23)?	The organization has not defined its security training material based on its organizational requirements, culture, and the types of roles with significant security responsibilities. In addition, the organization has not defined its processes for ensuring that all personnel with significant security roles and responsibilities are provided specialized security training prior to information system access or performing assigned duties and periodically thereafter.	The organization has defined its security training material based on its organizational requirements, culture, and the types of roles with significant security responsibilities. In addition, the organization has defined its processes for ensuring that all personnel with assigned security roles and responsibilities are provided specialized security training prior to information system access or performing assigned duties and periodically thereafter).	The organization ensures individuals with significant security responsibilities are provided specialized security training prior to information system access or performing assigned duties and periodically thereafter and maintains appropriate records. Furthermore, the organization maintains specialized security training completion records.	The organization obtains feedback on its security training content and makes updates to its program, as appropriate. In addition, the organization measures the effectiveness of its specialized security training program by, for example, conducting phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate.	The organization has institutionalized a process of continuous improvement incorporating advanced security training practices and technologies.



Final FY 2017 Inspector General FISMA Metrics v1.0
Protect Function Area (Security Training)

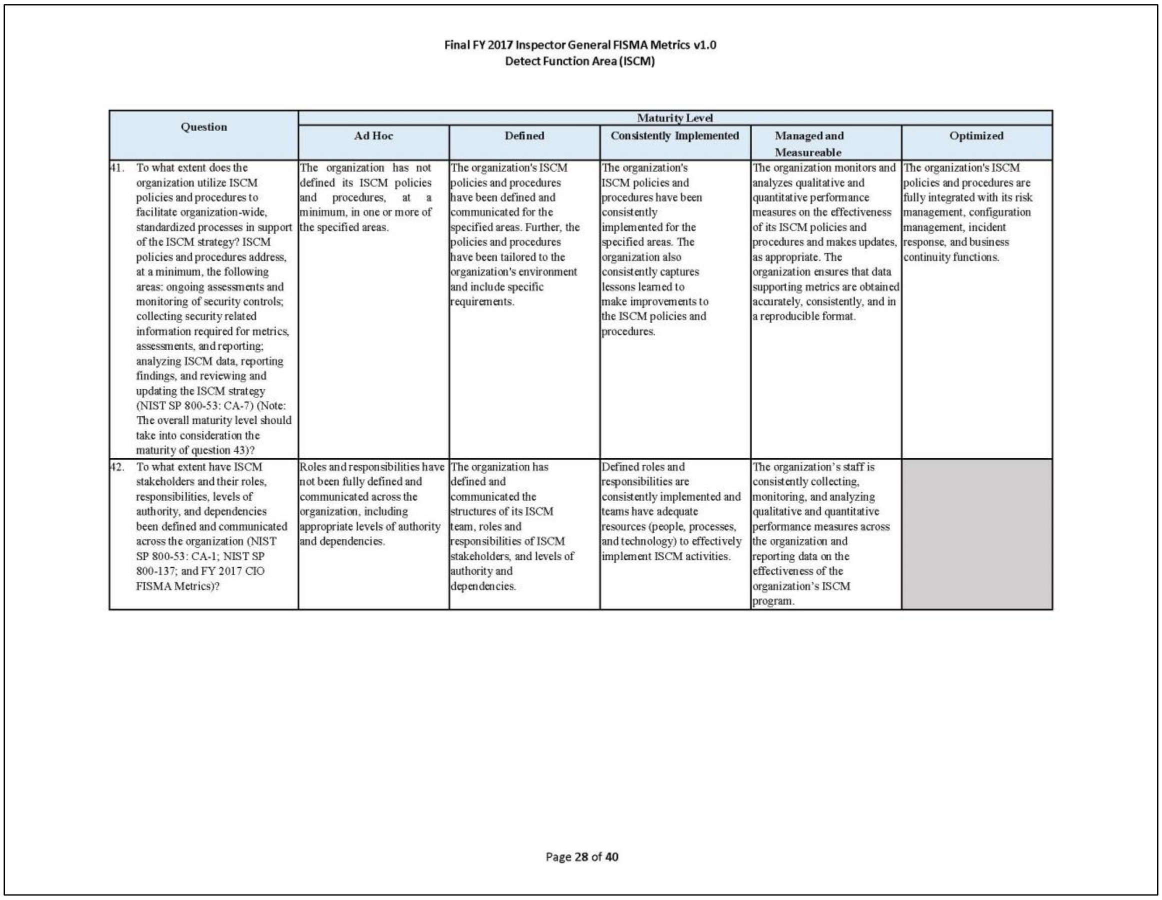
Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
39. Provide any additional information on the effectiveness (positive or negative) of the organization's security training program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the security training program effective?					



DETECT FUNCTION AREA

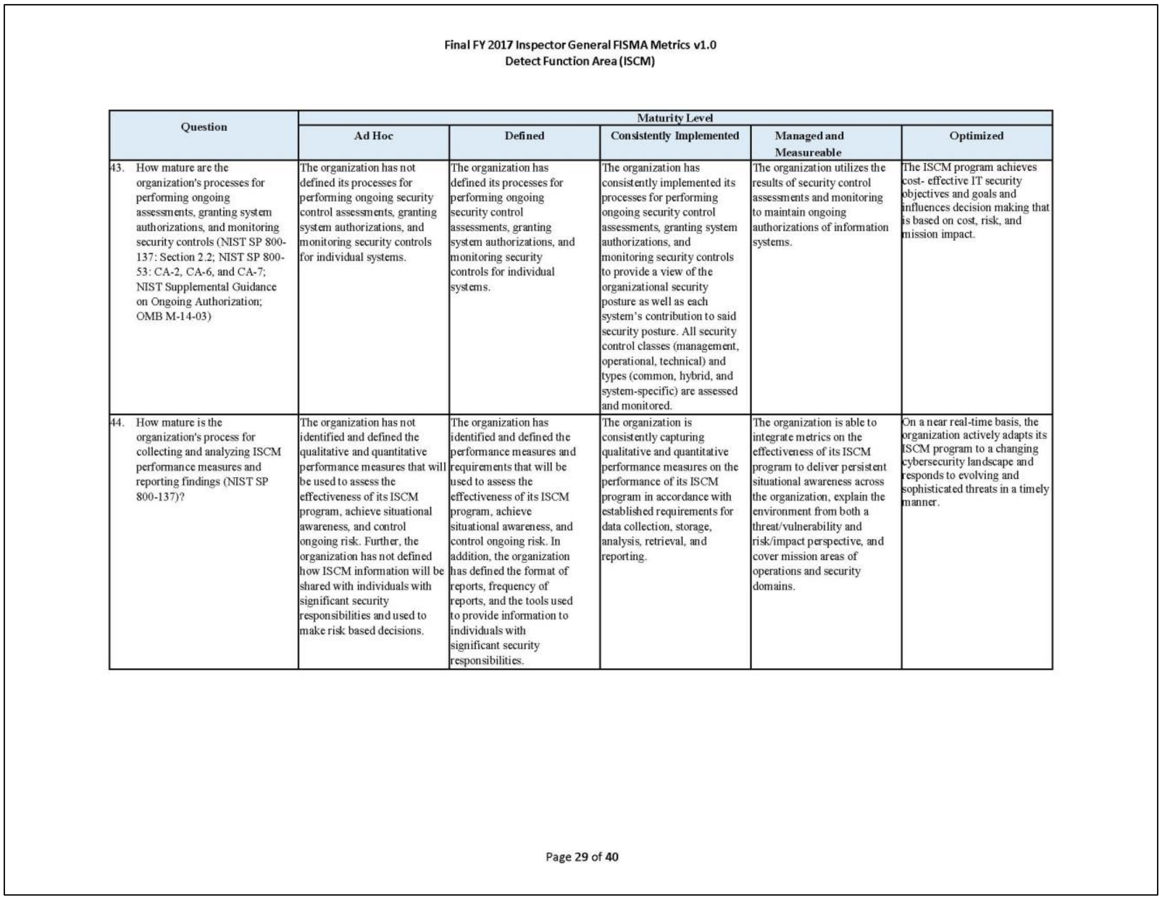
Table 8: ISCM

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
40. To what extent does the organization utilize an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements and activities at each organizational tier and helps ensure an organization-wide approach to ISCM (NIST SP 800-137: Sections 3.1 and 3.6)?	The organization has not developed and communicated its ISCM strategy.	The organization has developed and communicated its ISCM strategy that includes: i) considerations at the organization/business process level, ii) considerations at the information system level, and iii) processes to review and update the ISCM program and strategy. At the organization/business process level, the ISCM strategy defines how ISCM activities support risk management in accordance with organizational risk tolerance. At the information system level, the ISCM strategy addresses monitoring security controls for effectiveness, monitoring for security status, and reporting findings.	The organization's ISCM strategy is consistently implemented at the organization/business process and information system levels. In addition, the strategy supports clear visibility into assets, awareness into vulnerabilities, up-to-date threat information, and mission/business impacts. The organization also consistently captures lessons learned to make improvements to the ISCM strategy.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM strategy and makes updates, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization's ISCM strategy is fully integrated with its risk management, configuration management, incident response, and business continuity functions.



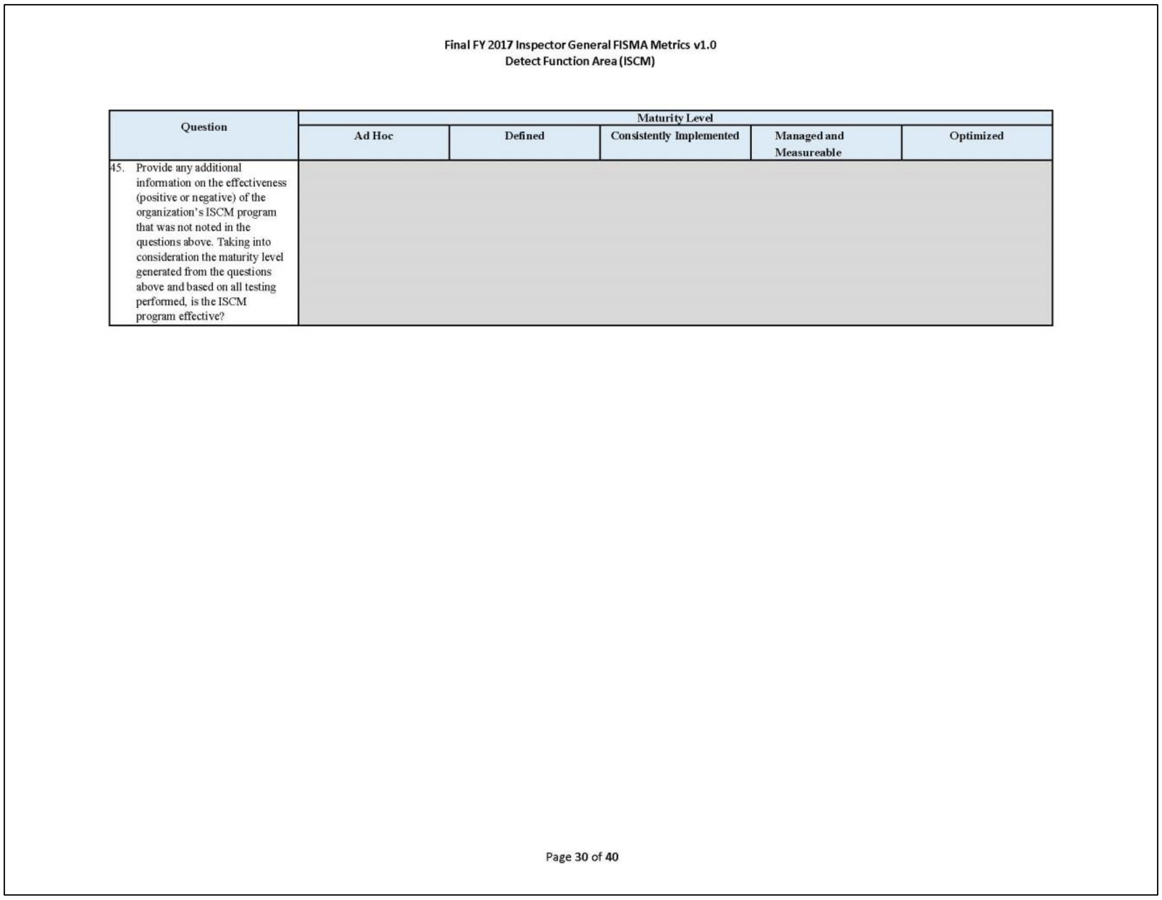
Final FY 2017 Inspector General FISMA Metrics v1.0
Detect Function Area (ISCM)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
41. To what extent does the organization utilize ISCM policies and procedures to facilitate organization-wide, standardized processes in support of the ISCM strategy? ISCM policies and procedures address, at a minimum, the following areas: ongoing assessments and monitoring of security controls; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and reviewing and updating the ISCM strategy (NIST SP 800-53: CA-7) (Note: The overall maturity level should take into consideration the maturity of question 43)?	The organization has not defined its ISCM policies and procedures, at a minimum, in one or more of the specified areas.	The organization's ISCM policies and procedures have been defined and communicated for the specified areas. Further, the policies and procedures have been tailored to the organization's environment and include specific requirements.	The organization's ISCM policies and procedures have been consistently implemented for the specified areas. The organization also consistently captures lessons learned to make improvements to the ISCM policies and procedures.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM policies and procedures and makes updates, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization's ISCM policies and procedures are fully integrated with its risk management, configuration management, incident response, and business continuity functions.
42. To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53: CA-1; NIST SP 800-137; and FY 2017 CIO FISMA Metrics)?	Roles and responsibilities have not been fully defined and communicated across the organization, including appropriate levels of authority and dependencies.	The organization has defined and communicated the structures of its ISCM team, roles and responsibilities of ISCM stakeholders, and levels of authority and dependencies.	Defined roles and responsibilities are consistently implemented and teams have adequate resources (people, processes, and technology) to effectively implement ISCM activities.	The organization's staff is consistently collecting, monitoring, and analyzing qualitative and quantitative performance measures across the organization and reporting data on the effectiveness of the organization's ISCM program.	



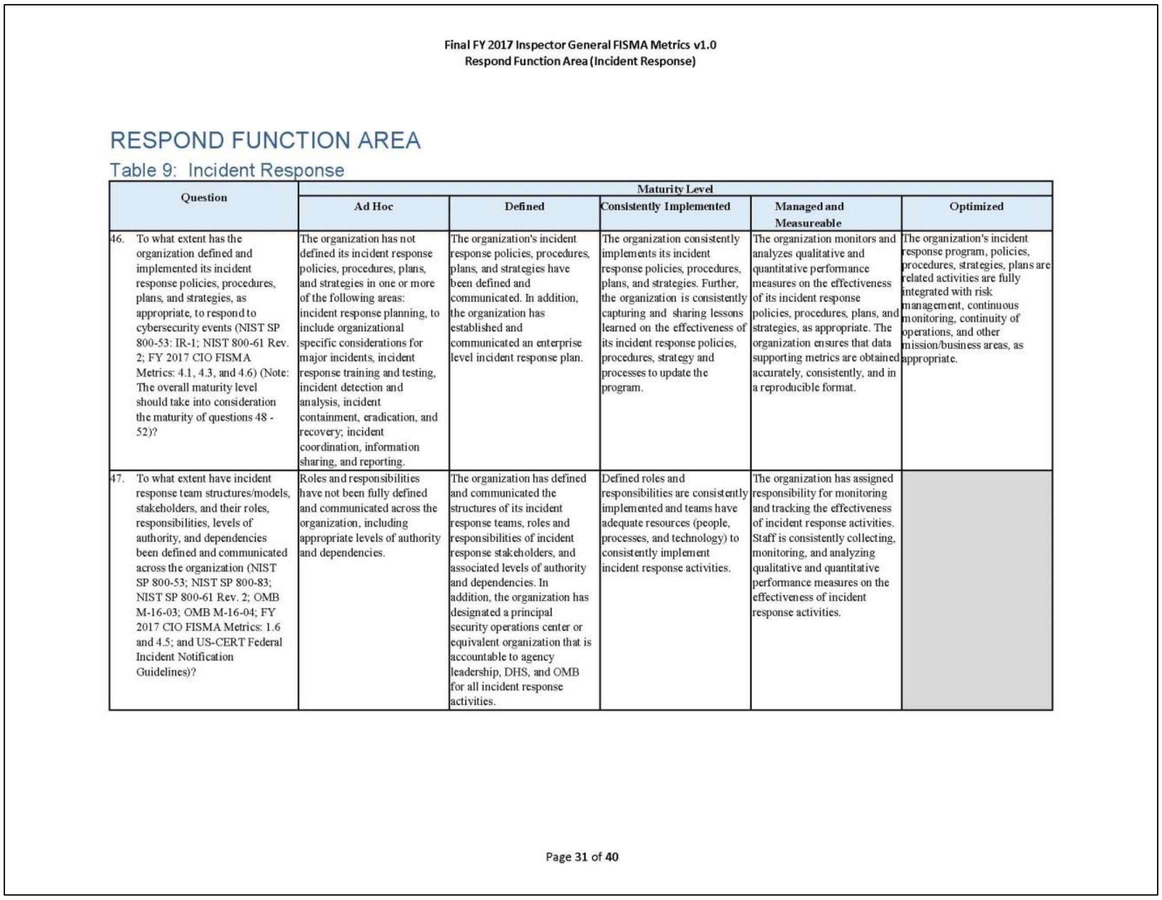
Final FY 2017 Inspector General FISMA Metrics v1.0
Detect Function Area (ISCM)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
43. How mature are the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security controls (NIST SP 800-137: Section 2.2; NIST SP 800-53: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; OMB M-14-03)	The organization has not defined its processes for performing ongoing security control assessments, granting system authorizations, and monitoring security controls for individual systems.	The organization has defined its processes for performing ongoing security control assessments, granting system authorizations, and monitoring security controls for individual systems.	The organization has consistently implemented its processes for performing ongoing security control assessments, granting system authorizations, and monitoring security controls to provide a view of the organizational security posture as well as each system's contribution to said security posture. All security control classes (management, operational, technical) and types (common, hybrid, and system-specific) are assessed and monitored.	The organization utilizes the results of security control assessments and monitoring to maintain ongoing authorizations of information systems.	The ISCM program achieves cost- effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact.
44. How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137)?	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. Further, the organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk based decisions.	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. In addition, the organization has defined the format of reports, frequency of reports, and the tools used to provide information to individuals with significant security responsibilities.	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.	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.	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.



Final FY 2017 Inspector General FISMA Metrics v1.0
Detect Function Area (ISCM)

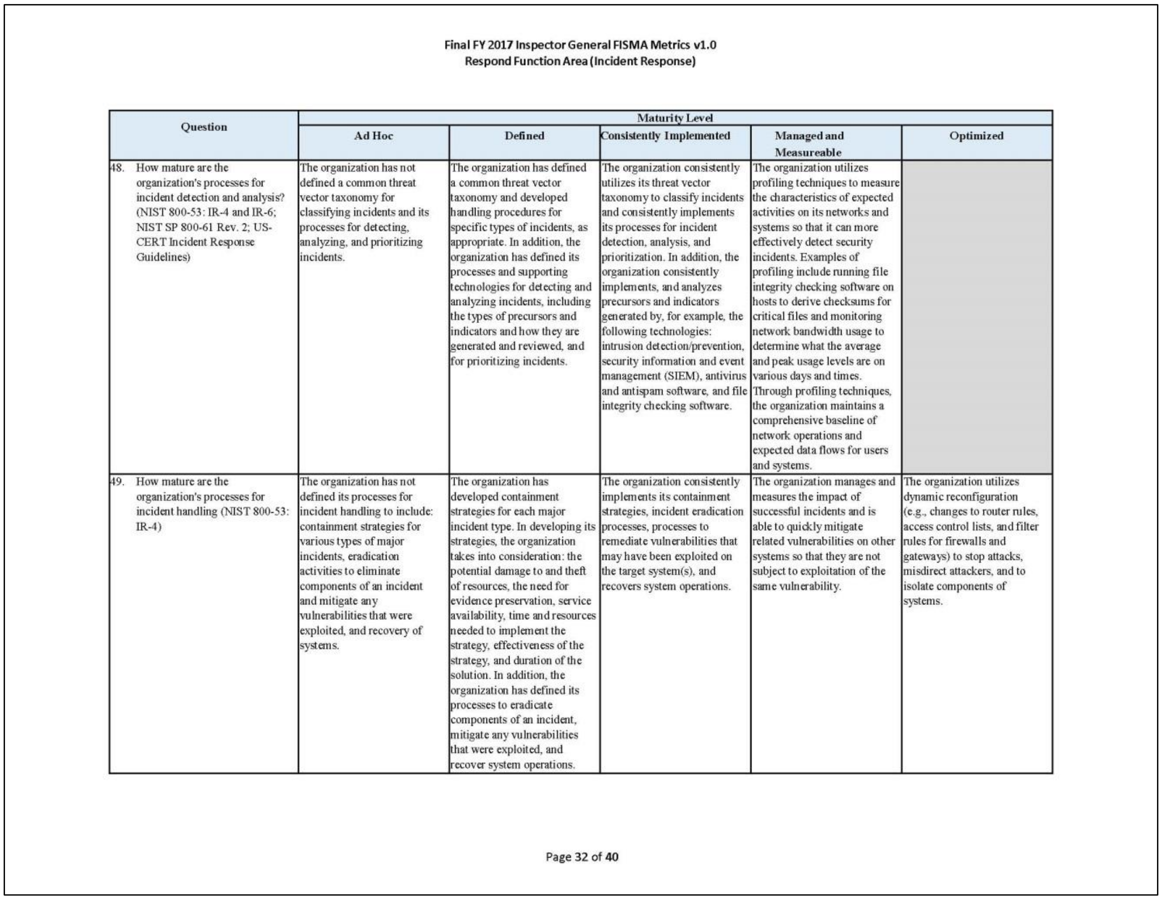
Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
45. Provide any additional information on the effectiveness (positive or negative) of the organization's ISCM program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?					



RESPOND FUNCTION AREA

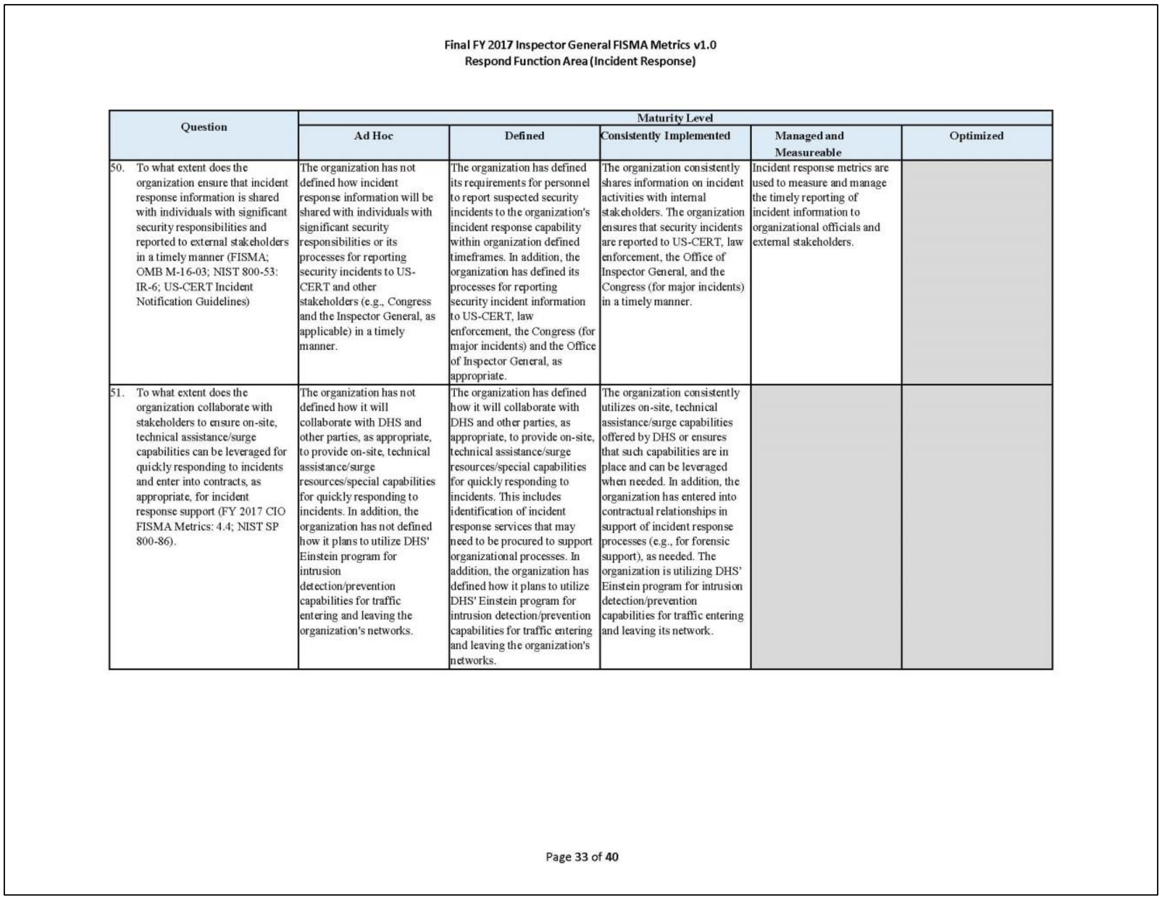
Table 9: Incident Response

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
46. To what extent has the organization defined and implemented its incident response policies, procedures, plans, and strategies, as appropriate, to respond to cybersecurity events (NIST SP 800-53: IR-1; NIST 800-61 Rev. 2; FY 2017 CIO FISMA Metrics: 4.1, 4.3, and 4.6) (Note: The overall maturity level should take into consideration the maturity of questions 48 - 52)?	The organization has not defined its incident response policies, procedures, plans, and strategies in one or more of the following areas: incident response planning, to include organizational specific considerations for major incidents, incident response training and testing, incident detection and analysis, incident containment, eradication, and recovery; incident coordination, information sharing, and reporting.	The organization's incident response policies, procedures, plans, and strategies have been defined and communicated. In addition, the organization has established and communicated an enterprise level incident response plan.	The organization consistently implements its incident response policies, procedures, plans, and strategies. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident response policies, procedures, strategy and processes to update the program.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident response policies, procedures, plans, and strategies, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization's incident response program, policies, procedures, strategies, plans are related activities are fully integrated with risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate.
47. To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-16-03; OMB M-16-04; FY 2017 CIO FISMA Metrics: 1.6 and 4.5; and US-CERT Federal Incident Notification Guidelines)?	Roles and responsibilities have not been fully defined and communicated across the organization, including appropriate levels of authority and dependencies.	The organization has defined and communicated the structures of its incident response teams, roles and responsibilities of incident response stakeholders, and associated levels of authority and dependencies. In addition, the organization has designated a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities.	Defined roles and responsibilities are consistently implemented and teams have adequate resources (people, processes, and technology) to consistently implement incident response activities.	The organization has assigned responsibility for monitoring and tracking the effectiveness of incident response activities. Staff is consistently collecting, monitoring, and analyzing qualitative and quantitative performance measures on the effectiveness of incident response activities.	



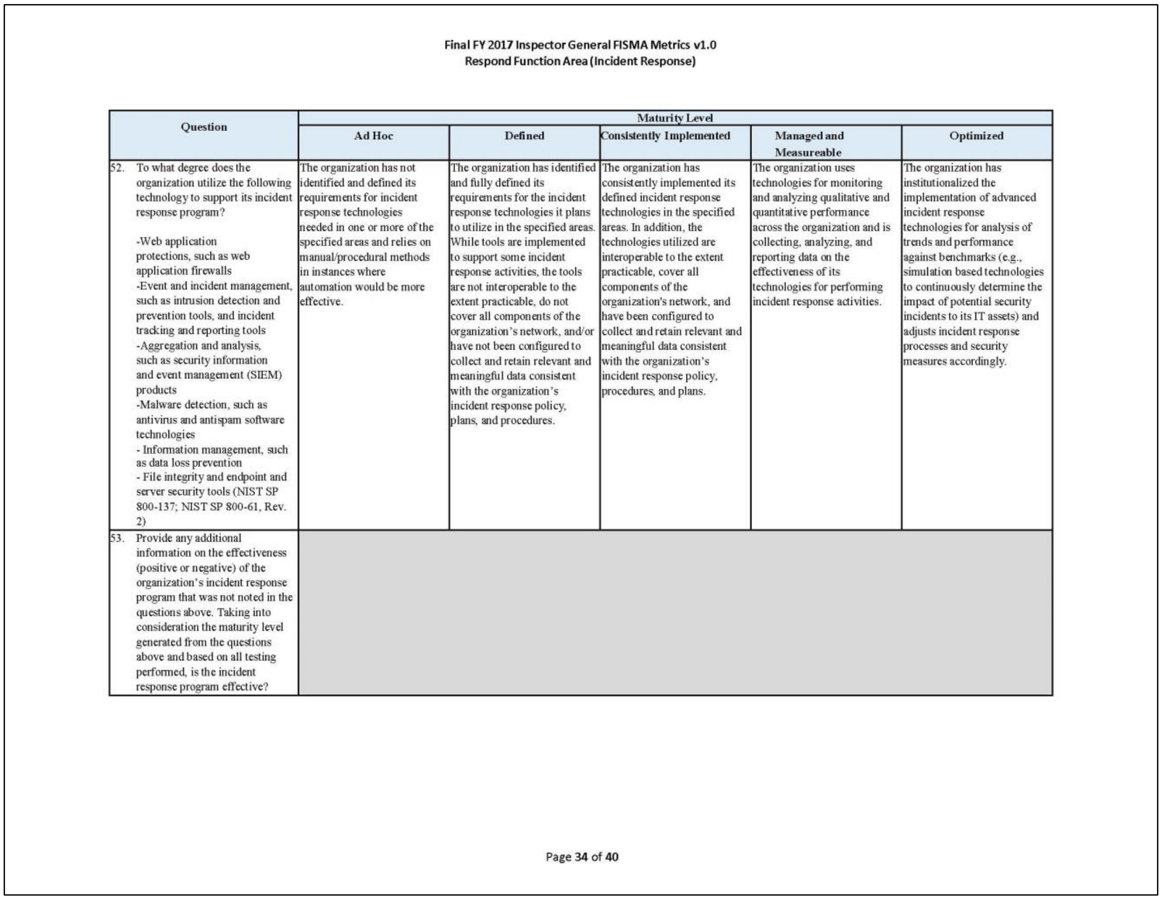
Final FY 2017 Inspector General FISMA Metrics v1.0
Respond Function Area (Incident Response)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
48. How mature are the organization's processes for incident detection and analysis? (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; US-CERT Incident Response Guidelines)	The organization has not defined a common threat vector taxonomy for classifying incidents and its processes for detecting, analyzing, and prioritizing incidents.	The organization has defined a common threat vector taxonomy and developed handling procedures for specific types of incidents, as appropriate. In addition, the organization has defined its processes and supporting technologies for detecting and analyzing incidents, including the types of precursors and indicators and how they are generated and reviewed, and for prioritizing incidents.	The organization consistently utilizes its threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis, and prioritization. In addition, the organization consistently implements, and analyzes precursors and indicators generated by, for example, the following technologies: intrusion detection/prevention, security information and event management (SIEM), antivirus and antispam software, and file integrity checking software.	The organization utilizes profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents. Examples of profiling include running file integrity checking software on hosts to derive checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times. Through profiling techniques, the organization maintains a comprehensive baseline of network operations and expected data flows for users and systems.	
49. How mature are the organization's processes for incident handling (NIST 800-53: IR-4)	The organization has not defined its processes for incident handling to include: containment strategies for various types of major incidents, eradication activities to eliminate components of an incident and mitigate any vulnerabilities that were exploited, and recovery of systems.	The organization has developed containment strategies for each major incident type. In developing its strategies, the organization takes into consideration: the potential damage to and theft of resources, the need for evidence preservation, service availability, time and resources needed to implement the strategy, effectiveness of the strategy, and duration of the solution. In addition, the organization has defined its processes to eradicate components of an incident, mitigate any vulnerabilities that were exploited, and recover system operations.	The organization consistently implements its containment strategies, incident eradication processes, processes to remediate vulnerabilities that may have been exploited on the target system(s), and recovers system operations.	The organization manages and measures the impact of successful incidents and is able to quickly mitigate related vulnerabilities on other systems so that they are not subject to exploitation of the same vulnerability.	The organization utilizes dynamic reconfiguration (e.g., changes to router rules, access control lists, and filter rules for firewalls and gateways) to stop attacks, misdirect attackers, and to isolate components of systems.



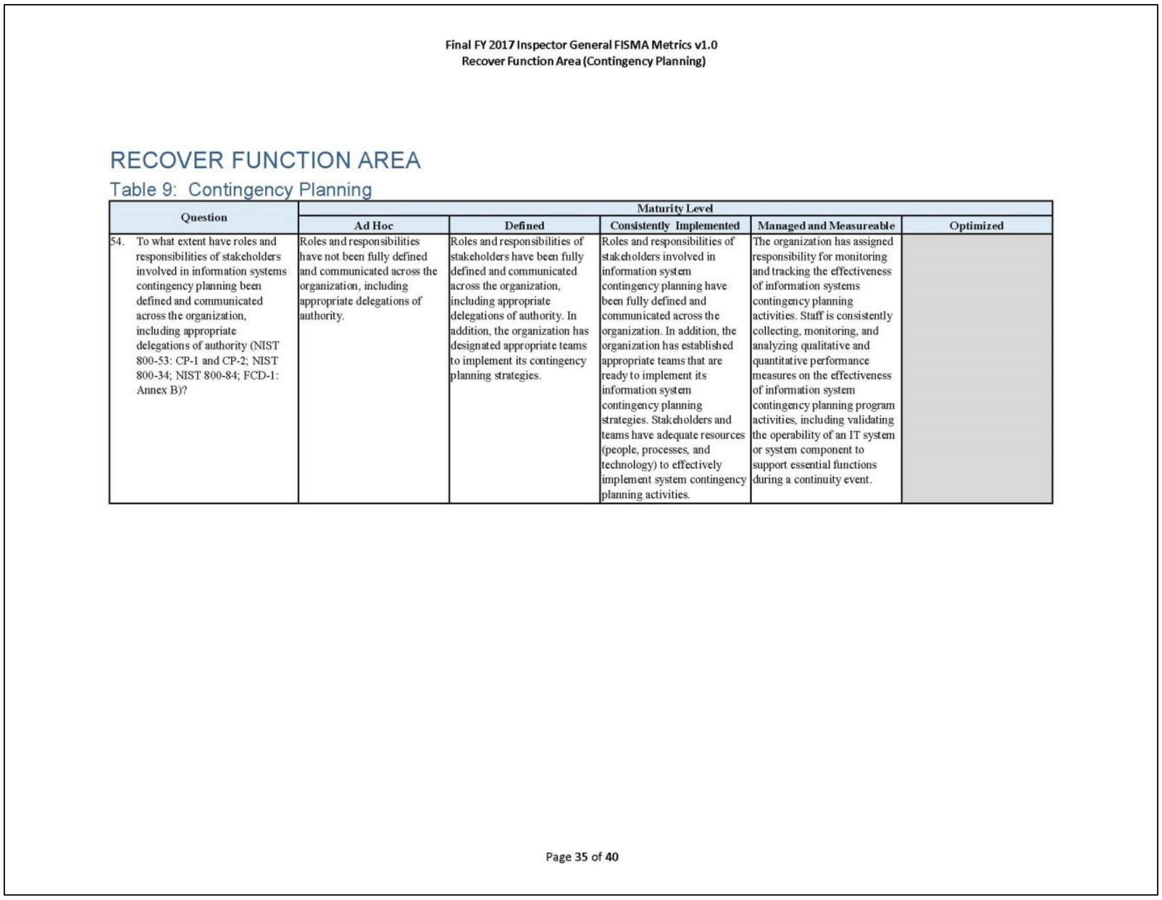
Final FY 2017 Inspector General FISMA Metrics v1.0
Respond Function Area (Incident Response)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
50. To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; OMB M-16-03; NIST 800-53: IR-6; US-CERT Incident Notification Guidelines)	The organization has not defined how incident response information will be shared with individuals with significant security responsibilities or its processes for reporting security incidents to US-CERT and other stakeholders (e.g., Congress and the Inspector General, as applicable) in a timely manner.	The organization has defined its requirements for personnel to report suspected security incidents to the organization's incident response capability within organization defined timeframes. In addition, the organization has defined its processes for reporting security incident information to US-CERT, law enforcement, the Congress (for major incidents) and the Office of Inspector General, as appropriate.	The organization consistently shares information on incident activities with internal stakeholders. The organization ensures that security incidents are reported to US-CERT, law enforcement, the Office of Inspector General, and the Congress (for major incidents) in a timely manner.	Incident response metrics are used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.	
51. To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents and enter into contracts, as appropriate, for incident response support (FY 2017 CIO FISMA Metrics: 4.4; NIST SP 800-86).	The organization has not 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. In addition, 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.	The organization has 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. This includes identification of incident response services that may need to be procured to support organizational processes. In addition, the organization has defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving the organization's networks.	The organization consistently utilizes on-site, technical assistance/surge capabilities offered by DHS or ensures that such capabilities are in place and can be leveraged when needed. In addition, the organization has entered into contractual relationships in support of incident response processes (e.g., for forensic support), as needed. The organization is utilizing DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving its network.		



Final FY 2017 Inspector General FISMA Metrics v1.0
Respond Function Area (Incident Response)

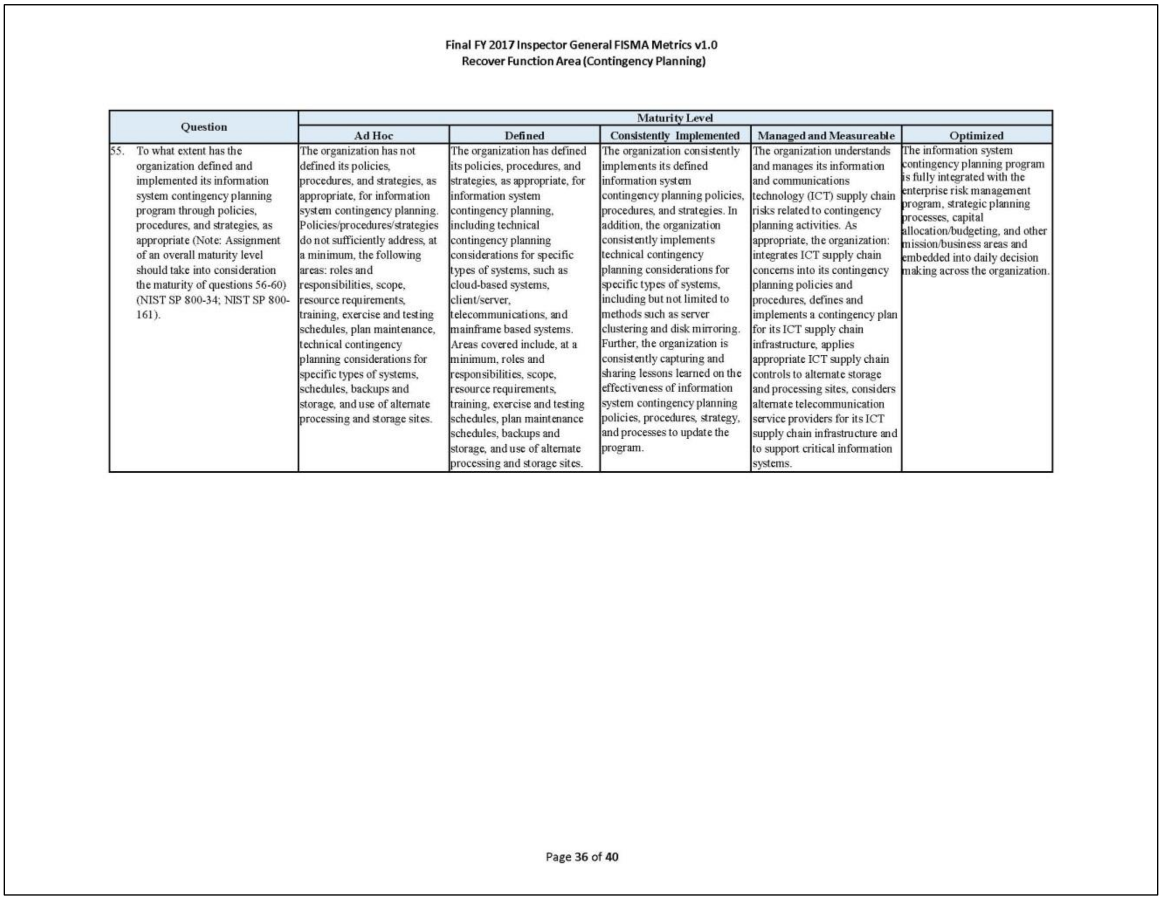
Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
52. To what degree does the organization utilize the following technology to support its incident response program? -Web application protections, such as web application firewalls -Event and incident 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 antivirus and antispam software technologies - Information management, such as data loss prevention - File integrity and endpoint and server security tools (NIST SP 800-137; NIST SP 800-61, Rev. 2)	The organization has not identified and defined its requirements for incident response technologies needed in one or more of the specified areas and relies on manual/procedural methods in instances where automation would be more effective.	The organization has identified and fully defined its requirements for the incident response technologies it plans to utilize in the specified areas. 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.	The organization has consistently implemented its defined incident response technologies in the specified areas. In addition, the technologies utilized 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.	The organization uses technologies for 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.	The organization has institutionalized the implementation of advanced incident response technologies for analysis of trends and performance against benchmarks (e.g., 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.
53. Provide any additional information on the effectiveness (positive or negative) of the organization's incident response program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the incident response program effective?					



RECOVER FUNCTION AREA

Table 9: Contingency Planning

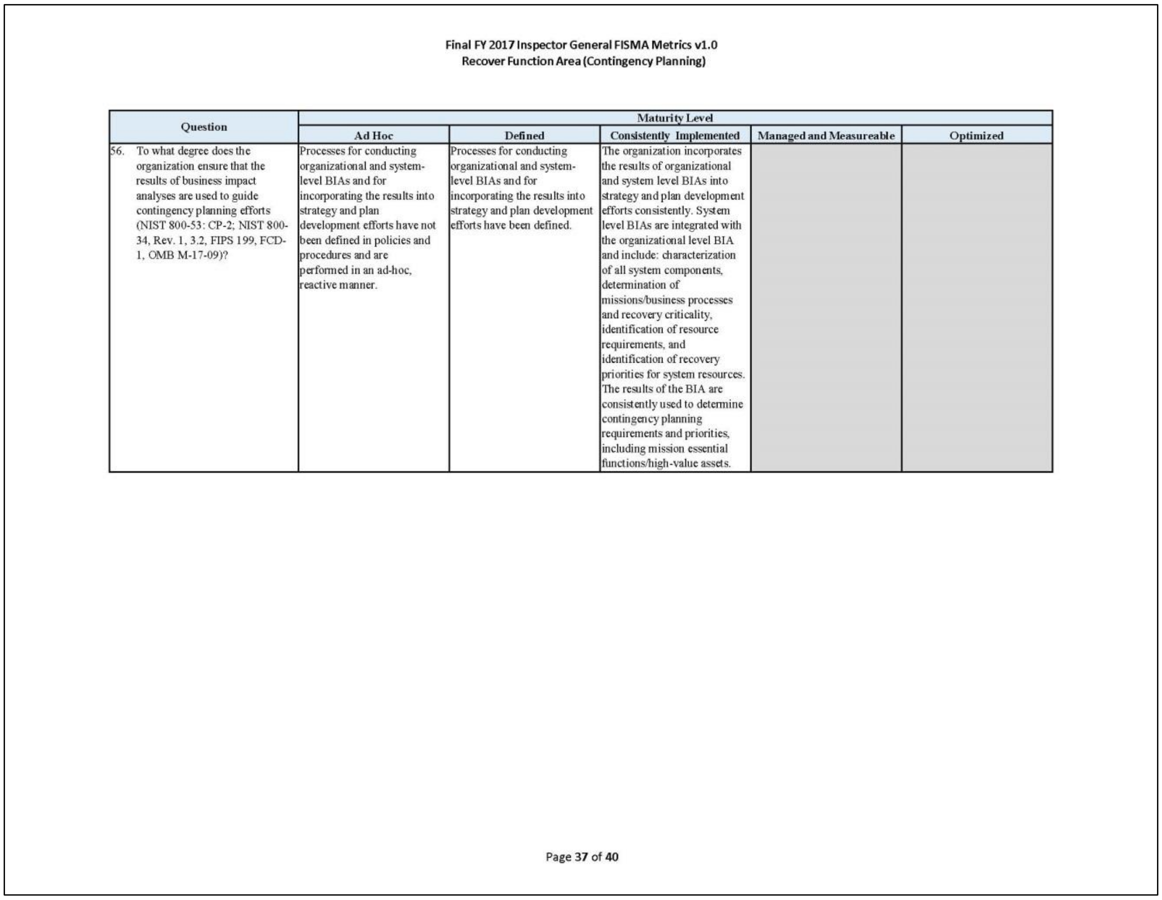
Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
54. To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined and communicated across the organization, including appropriate delegations of authority (NIST 800-53: CP-1 and CP-2; NIST 800-34; NIST 800-84; FCD-1: Annex B)?	Roles and responsibilities have not been fully defined and communicated across the organization, including appropriate delegations of authority.	Roles and responsibilities of stakeholders have been fully defined and communicated across the organization, including appropriate delegations of authority. In addition, the organization has designated appropriate teams to implement its contingency planning strategies.	Roles and responsibilities of stakeholders involved in information system contingency planning have been fully defined and communicated across the organization. In addition, the organization has established appropriate teams that are ready to implement its information system contingency planning strategies. Stakeholders and teams have adequate resources (people, processes, and technology) to effectively implement system contingency planning activities.	The organization has assigned responsibility for monitoring and tracking the effectiveness of information systems contingency planning activities. Staff is consistently collecting, monitoring, and analyzing qualitative and quantitative performance measures on the effectiveness of information system contingency planning program activities, including validating the operability of an IT system or system component to support essential functions during a continuity event.	



Final FY 2017 Inspector General FISMA Metrics v1.0
Recover Function Area (Contingency Planning)

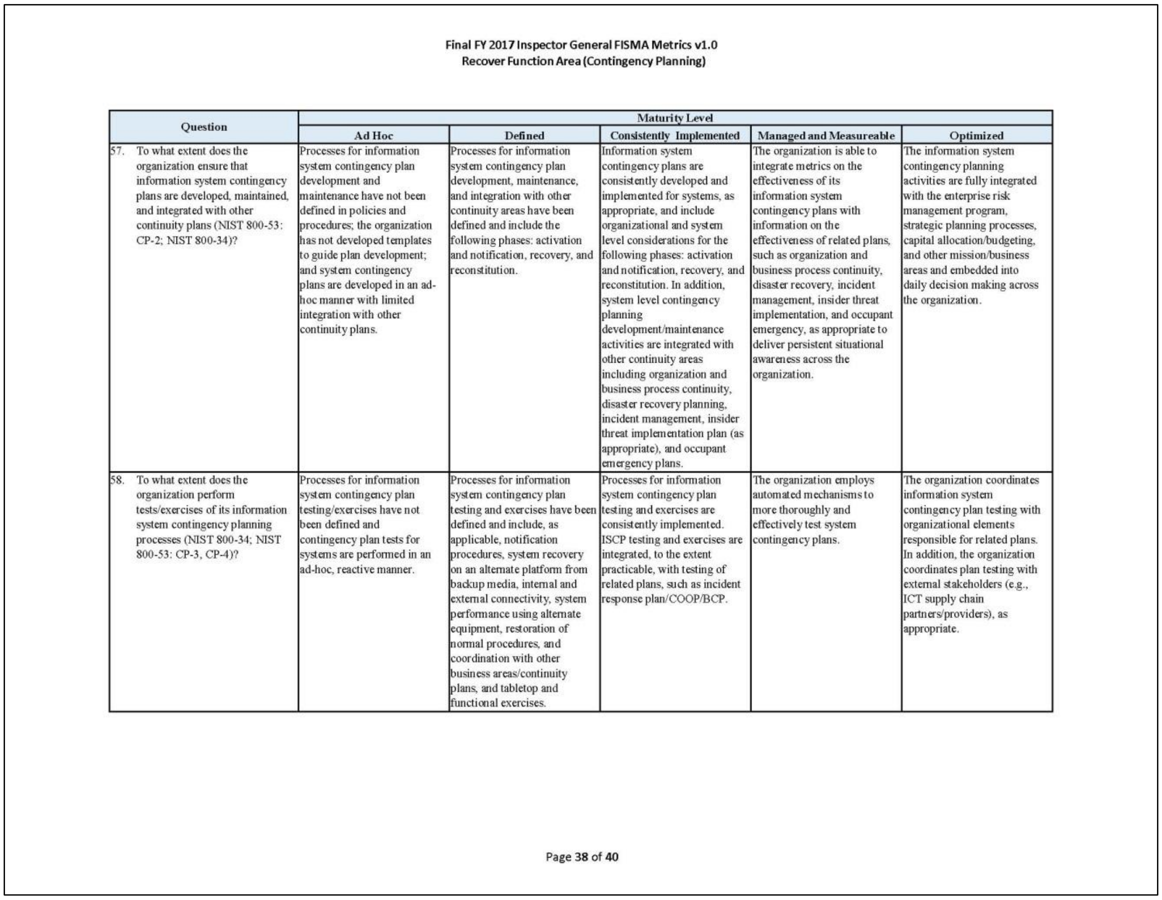
Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
55. To what extent has the organization defined and implemented its information system contingency planning program through policies, procedures, and strategies, as appropriate (Note: Assignment of an overall maturity level should take into consideration the maturity of questions 56-60) (NIST SP 800-34; NIST SP 800-161).	The organization has not defined its policies, procedures, and strategies, as appropriate, for information system contingency planning. Policies/procedures/strategies do not sufficiently address, at a minimum, the following areas: roles and responsibilities, scope, resource requirements, training, exercise and testing schedules, plan maintenance, technical contingency planning considerations for specific types of systems, schedules, backups and storage, and use of alternate processing and storage sites.	The organization has defined its policies, procedures, and strategies, as appropriate, for information system contingency planning, including technical contingency planning considerations for specific types of systems, such as cloud-based systems, client/server, telecommunications, and mainframe based systems. Areas covered include, at a minimum, roles and responsibilities, scope, resource requirements, training, exercise and testing schedules, plan maintenance schedules, backups and storage, and use of alternate processing and storage sites.	The organization consistently implements its defined information system contingency planning policies, procedures, and strategies. In addition, the organization consistently implements technical contingency planning considerations for specific types of systems, including but not limited to methods such as server clustering and disk mirroring. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of information system contingency planning policies, procedures, strategy, and processes to update the program.	The organization understands and manages its information and communications technology (ICT) supply chain risks related to contingency planning activities. As appropriate, the organization: integrates ICT supply chain concerns into its contingency planning policies and procedures, defines and implements a contingency plan for its ICT supply chain infrastructure, applies appropriate ICT supply chain controls to alternate storage and processing sites, considers alternate telecommunication service providers for its ICT supply chain infrastructure and to support critical information systems.	The information system contingency planning program is fully integrated with the enterprise risk management program, strategic planning processes, capital allocation/budgeting, and other mission/business areas and embedded into daily decision making across the organization.

Page 36 of 40



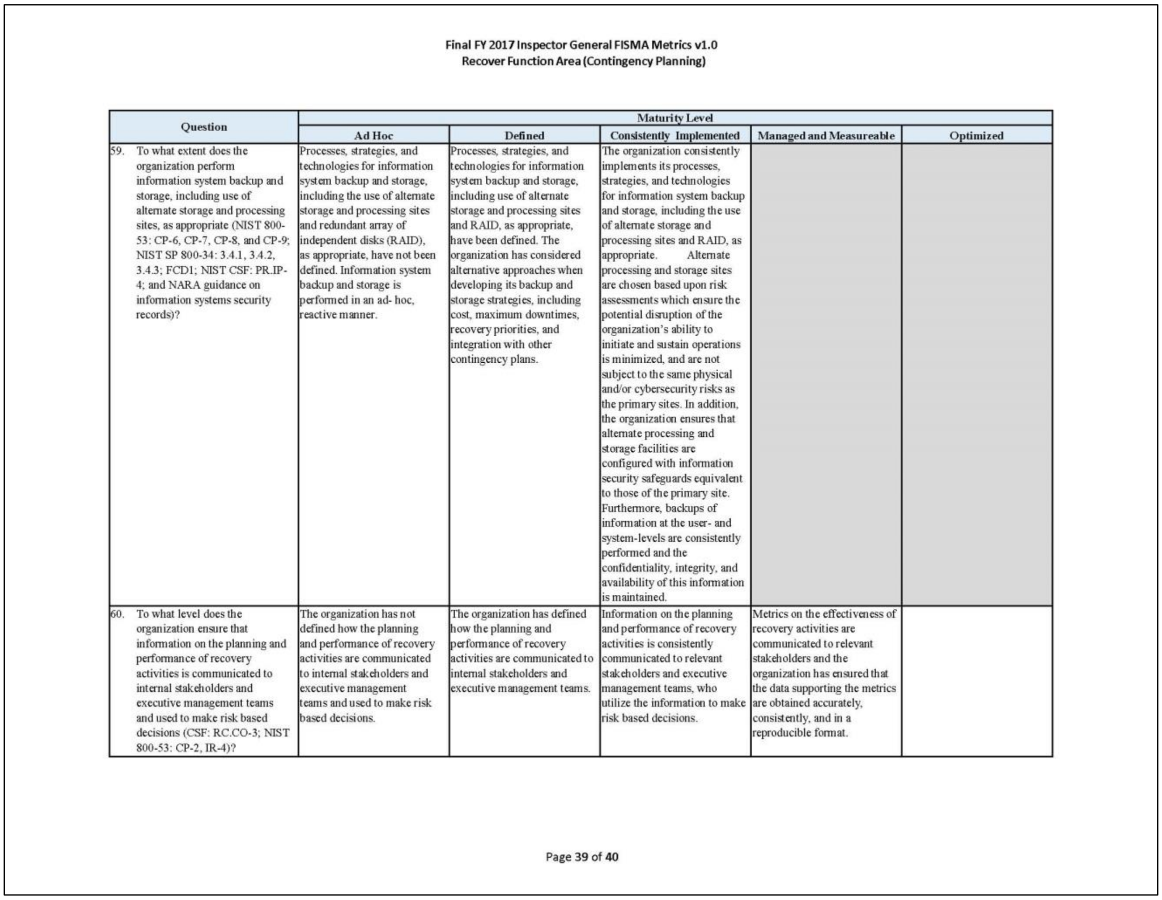
Final FY 2017 Inspector General FISMA Metrics v1.0
Recover Function Area (Contingency Planning)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
56. To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST 800-53: CP-2; NIST 800-34, Rev. 1, 3.2, FIPS 199, FCD-1, OMB M-17-09)?	Processes for conducting organizational and system-level BIAs and for incorporating the results into strategy and plan development efforts have not been defined in policies and procedures and are performed in an ad-hoc, reactive manner.	Processes for conducting organizational and system-level BIAs and for incorporating the results into strategy and plan development efforts have been defined.	The organization incorporates the results of organizational and system level BIAs into strategy and plan development efforts consistently. System level BIAs are integrated with the organizational level BIA and include: characterization of all system components, determination of missions/business processes and recovery criticality, identification of resource requirements, and identification of recovery priorities for system resources. The results of the BIA are consistently used to determine contingency planning requirements and priorities, including mission essential functions/high-value assets.		



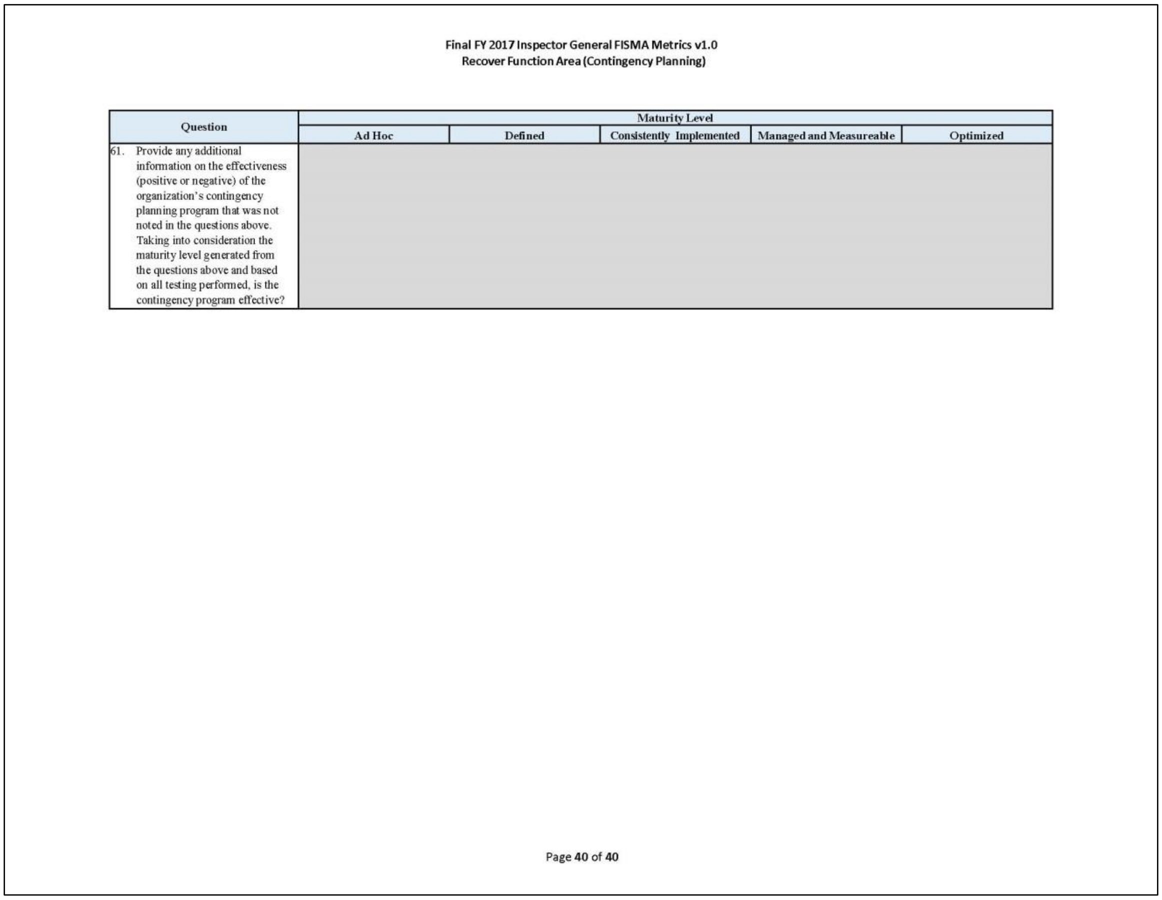
Final FY 2017 Inspector General FISMA Metrics v1.0
Recover Function Area (Contingency Planning)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
57. To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST 800-53: CP-2; NIST 800-34)?	Processes for information system contingency plan development and maintenance have not been defined in policies and procedures; the organization has not developed templates to guide plan development; and system contingency plans are developed in an ad-hoc manner with limited integration with other continuity plans.	Processes for information system contingency plan development, maintenance, and integration with other continuity areas have been defined and include the following phases: activation and notification, recovery, and reconstitution.	Information system contingency plans are consistently developed and implemented for systems, as appropriate, and include organizational and system level considerations for the following phases: activation and notification, recovery, and reconstitution. In addition, system level contingency planning development/maintenance activities are integrated with other continuity areas including organization and business process continuity, disaster recovery planning, incident management, insider threat implementation plan (as appropriate), and occupant emergency plans.	The organization is able to integrate metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related plans, such as organization and business process continuity, disaster recovery, incident management, insider threat implementation, and occupant emergency, as appropriate to deliver persistent situational awareness across the organization.	The information system contingency planning activities are fully integrated with the enterprise risk management program, strategic planning processes, capital allocation/budgeting, and other mission/business areas and embedded into daily decision making across the organization.
58. To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST 800-34; NIST 800-53: CP-3, CP-4)?	Processes for information system contingency plan testing/exercises have not been defined and contingency plan tests for systems are performed in an ad-hoc, reactive manner.	Processes for information system contingency plan testing and exercises have been defined and include, as applicable, notification procedures, system recovery on an alternate platform from backup media, internal and external connectivity, system performance using alternate equipment, restoration of normal procedures, and coordination with other business areas/continuity plans, and tabletop and functional exercises.	Processes for information system contingency plan testing and exercises are consistently implemented. ISCP testing and exercises are integrated, to the extent practicable, with testing of related plans, such as incident response plan/COOP/BCP.	The organization employs automated mechanisms to more thoroughly and effectively test system contingency plans.	The organization coordinates information system contingency plan testing with organizational elements responsible for related plans. In addition, the organization coordinates plan testing with external stakeholders (e.g., ICT supply chain partners/providers), as appropriate.



Final FY 2017 Inspector General FISMA Metrics v1.0
Recover Function Area (Contingency Planning)

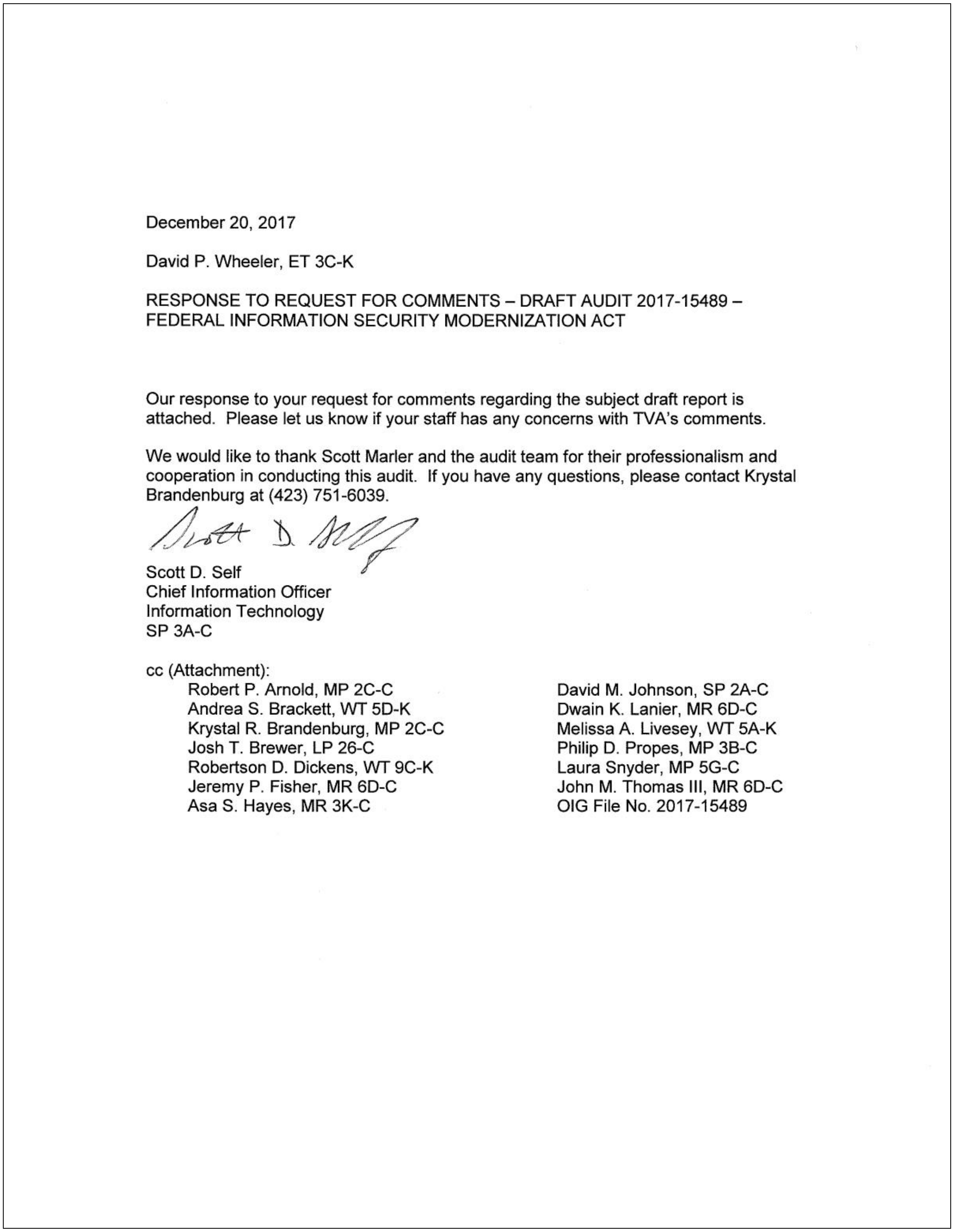
Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
59. To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST 800-53: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD1; NIST CSF: PR.IP-4; and NARA guidance on information systems security records)?	Processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites and redundant array of independent disks (RAID), as appropriate, have not been defined. Information system backup and storage is performed in an ad- hoc, reactive manner.	Processes, strategies, and technologies for information system backup and storage, including use of alternate storage and processing sites and RAID, as appropriate, have been defined. The organization has considered alternative approaches when developing its backup and storage strategies, including cost, maximum downtimes, recovery priorities, and integration with other contingency plans.	The organization consistently implements its processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites and RAID, as appropriate. Alternate processing and storage sites are chosen 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. In addition, the organization ensures that alternate processing and storage facilities are configured with information security safeguards equivalent to those of the primary site. Furthermore, backups of information at the user- and system-levels are consistently performed and the confidentiality, integrity, and availability of this information is maintained.		
60. To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk based decisions (CSF: RC.CO-3; NIST 800-53: CP-2, IR-4)?	The organization has not defined how the planning and performance of recovery activities are communicated to internal stakeholders and executive management teams and used to make risk based decisions.	The organization has defined how the planning and performance of recovery activities are communicated to internal stakeholders and executive management teams.	Information on the planning and performance of recovery activities is consistently communicated to relevant stakeholders and executive management teams, who utilize the information to make risk based decisions.	Metrics on the effectiveness of recovery activities are communicated to relevant stakeholders and the organization has ensured that the data supporting the metrics are obtained accurately, consistently, and in a reproducible format.	



Final FY 2017 Inspector General FISMA Metrics v1.0
Recover Function Area (Contingency Planning)

Question	Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
61. 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. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the contingency program effective?					

APPENDIX B
Page 1 of 2



December 20, 2017

David P. Wheeler, ET 3C-K

RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2017-15489 –
FEDERAL INFORMATION SECURITY MODERNIZATION ACT

Our response to your request for comments regarding the subject draft report is attached. Please let us know if your staff has any concerns with TVA's comments.

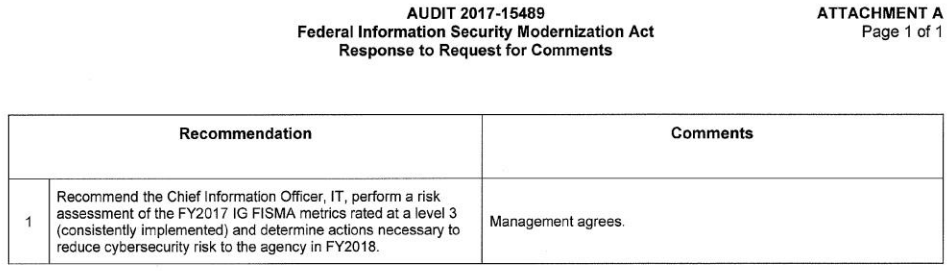
We would like to thank Scott Marler and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact Krystal Brandenburg at (423) 751-6039.

Scott D. Self

Scott D. Self
Chief Information Officer
Information Technology
SP 3A-C

cc (Attachment):

Robert P. Arnold, MP 2C-C
Andrea S. Brackett, WT 5D-K
Krystal R. Brandenburg, MP 2C-C
Josh T. Brewer, LP 26-C
Robertson D. Dickens, WT 9C-K
Jeremy P. Fisher, MR 6D-C
Asa S. Hayes, MR 3K-C
David M. Johnson, SP 2A-C
Dwain K. Lanier, MR 6D-C
Melissa A. Livesey, WT 5A-K
Philip D. Propes, MP 3B-C
Laura Snyder, MP 5G-C
John M. Thomas III, MR 6D-C
OIG File No. 2017-15489



AUDIT 2017-15489
Federal Information Security Modernization Act
Response to Request for Comments

Recommendation		Comments
1	Recommend the Chief Information Officer, IT, perform a risk assessment of the FY2017 IG FISMA metrics rated at a level 3 (consistently implemented) and determine actions necessary to reduce cybersecurity risk to the agency in FY2018.	Management agrees.