Memorandum from the Office of the Inspector General

September 26, 2023

Tammy W. Wilson

REQUEST FOR MANAGEMENT DECISION – AUDIT 2023-17423 – FEDERAL INFORMATION SECURITY MANAGEMENT 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. In accordance with the Inspector General Act of 1978, as amended, the Office of the Inspector General is required to report to Congress semiannually regarding audits that remain unresolved after 6 months from the date of report issuance.

If you have any questions or wish to discuss our findings, please contact Melissa L. Conforti, Senior Auditor, at (865) 633-7383 or Sarah E. Huffman, Director, at (865) 633-7345. We appreciate the courtesy and cooperation received from your staff during the audit.

David P. Wheeler
Assistant Inspector General
(Audits and Evaluations)

MLC:KDS
Attachment
cc (Attachment):

TVA Board of Directors
Brett A. Atkins
Brandy A. Barbee
Faisal Bhatti
Andrea S. Brackett
Tammy C. Bramlett
Kenneth C. Carnes II
Sherri R. Collins
Buddy Eller
David B. Fountain
Gregory G. Jackson
Melissa A. Livesey
Jeffrey J. Lyash
Jill M. Matthews
Todd E. McCarter
Kevin L. Tarver
John M. Thomas, III
Josh Thomas
Ben R. Wagner
OIG File No. 2023-17423

Office of the Inspector General

Audit Report

To the Vice President and Chief Information and Digital Officer, Technology and Innovation

FEDERAL INFORMATION SECURITY MODERNIZATION ACT

Auditor
Melissa L. Conforti

Audit 2023-17423
September 26, 2023

ABBREVIATIONS

BIA	Business Impact Analysis
DHS	Department of Homeland Security
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IG	Inspector General
ISP	Information Security Program
OMB	Office of Management and Budget
TVA	Tennessee Valley Authority
VDP	Vulnerability Disclosure Policy

TABLE OF CONTENTS

APPENDICES

Audit 2023-17423 – 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 practices of its respective agency.

Our objective was to determine the effectiveness of the Tennessee Valley Authority's (TVA) ISP and practices as defined by the *FY 2023 – 2024 IG FISMA Reporting Metrics*. Our audit scope was limited to answering the fiscal year (FY) 2023 IG metrics, which include 20 core IG metrics and 20 supplemental IG metrics (Appendix B). The 20 core IG metrics were chosen based on alignment with Executive Order 14028, *Improving the Nation's Cybersecurity*,[i] as well as recent Office of Management and Budget guidance to agencies in furtherance of the modernization of federal cybersecurity.

What the OIG Found

During the course of this audit, we utilized the methodology and metrics in the FY 2023 IG metrics (Appendix B) in our annual independent evaluation to determine the effectiveness of TVA's ISP and practices. The FISMA methodology considers metrics at a maturity level 4 (managed and measurable) or higher to be at an effective level of security. Each metric was assessed to determine its maturity level, as described in Table 1 below.

FY 2023 IG FISMA Maturity Definitions	
Maturity Level	**Maturity Level Description**
Level 1: *Ad-hoc*	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: *Defined*	Policies, procedures, and strategies are formalized and documented, but not consistently implemented.
Level 3: *Consistently Implemented*	Policies, procedures, and strategies 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 strategies are collected across the organization and used to assess them and make necessary changes.
Level 5: *Optimized*	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Table 1

[i] United States, Executive Order of the President [Joseph Biden] Compilation of Presidential Documents, *Executive Order 14028 - Improving the Nation's Cybersecurity*, May 17, 2021, < https:// www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity>, accessed on July 25, 2022.

EXECUTIVE SUMMARY

For FY 2023, IGs were required to test 20 core and 20 supplemental IG metrics that were aligned with the following five function areas in the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity: Identify, Protect, Detect, Respond, and Recover. Our analysis of the metric results was used to determine the overall function maturity levels in Table 2 below.

FY 2023 IG FISMA Function Average Results				
Function	**Core Assessed Maturity Level**	**Supplemental Assessed Maturity Level**	**Overall Assessed Maturity Level**	**Rating**
Identify	2.83	4.00	3.36	Not Effective
Protect	2.50	3.40	3.00	Not Effective
Detect	2.50	5.00	3.33	Not Effective
Respond	3.50	4.50	4.00	Effective
Recover	2.50	2.50	2.50	Not Effective

Table 2

Based on our analysis of the FY 2023 IG (20 core and 20 supplemental) metrics and associated maturity models, we found TVA's ISP and practices were not operating in an effective manner as defined by the *FY 2023 – 2024 IG FISMA Reporting Metrics*.

What the OIG Recommends

We made five recommendations to TVA management to increase the effectiveness of TVA's ISP and practices as defined by the FISMA reporting metrics. Our specific recommendations are included within the report.

TVA Management's Comments

In response to our draft audit report, TVA management agreed with the recommendations. See Appendix C 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 practices of its respective agency. As required by the Office of Management and Budget (OMB), FISMA shifted to a continuous assessment process in fiscal year (FY) 2022.[1] As a result, OMB and the Council of the Inspectors General on Integrity and Efficiency transitioned the IG metrics process to a multi-year cycle beginning in FY 2022. Specifically, a subset of the FY 2021 IG FISMA metrics (Appendix B) were selected as the 20 core IG metrics to be evaluated annually and remaining IG metrics will be evaluated on a two-year cycle. The 20 core IG metrics were chosen based on alignment with Executive Order 14028, *Improving the Nation's Cybersecurity*,[2] as well as recent OMB guidance to agencies in furtherance of the modernization of federal cybersecurity.

The IG metrics were organized into nine domains and aligned with the following five function areas in the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity: Identify, Protect, Detect, Respond, and Recover. This 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 2023 – 2024 IG FISMA Reporting Metrics* (Appendix B) were developed by 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 and other stakeholders. For FY 2023, IGs were required to test 20 core and 20 supplemental IG metrics.

The results of our review were provided to OMB and DHS through the use of their online reporting tool on August 1, 2023.

---

1 OMB Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*, December 2, 2022.

2 United States, Executive Order of the President [Joseph Biden] Compilation of Presidential Documents, *Executive Order 14028 - Improving the Nation's Cybersecurity*, May 17, 2021, <https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity>, accessed on July 25, 2022.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine the effectiveness of the Tennessee Valley Authority's (TVA) ISP and practices as defined by the *FY 2023 – 2024 IG FISMA Reporting Metrics*. Our audit scope was limited to answering the FY 2023 IG metrics, which included the 20 core and 20 supplemental IG metrics (Appendix B); therefore, the results of this audit are based on assessing these 40 IG metrics only. A complete discussion of our objective, scope, and methodology is included in Appendix A.

FINDINGS

The FISMA methodology considers metrics at a maturity level 4 (managed and measurable) or higher to be at an effective level of security. Based on our analysis of the FY 2023 IG metrics and associated maturity models, we found TVA's ISP and practices were not operating in an effective manner as defined by the *FY 2023 – 2024 IG FISMA Reporting Metrics*. See Table 1 for individual function averages and ratings.

FY 2023 IG FISMA Function Average Results				
Function	**Core Assessed Maturity Level**	**Supplemental Assessed Maturity Level**	**Overall Assessed Maturity Level**	**Rating**
Identify	2.83	4.00	3.36	Not Effective
Protect	2.50	3.40	3.00	Not Effective
Detect	2.50	5.00	3.33	Not Effective
Respond	3.50	4.50	4.00	Effective
Recover	2.50	2.50	2.50	Not Effective

Table 1

Specifically, we found 21 of the 40 IG metrics were ineffective. For the 21 ineffective IG metrics, we found:

- Fifteen metrics had actions in progress to improve their maturity, which included open Office of the Inspector General audit recommendations[3] and Executive Order 14028 requirements. One metric had mitigating controls in place to reduce cybersecurity risk. Completion of these actions in progress could improve the effectiveness of TVA's ISP and practices, specifically in the Identify, Protect, Detect, and Respond functions.
- Two core IG metrics had weaknesses that should be addressed by TVA management, including:
  - Security workforce assessment.
  - Business impact analysis (BIA).

[3] Audit 2022-17370, *Federal Information Security Modernization Act*, September 19, 2022, and Audit 2022-17390, *Remote Application and Desktop Virtualization Client*, June 21, 2023.

- Three supplemental metrics had weaknesses that should be addressed by TVA management, including:
  - Vulnerability disclosure policy (VDP).
  - Contingency planning.
  - Recovery activities communication.

The following provides a detailed discussion of our findings.

CORE INSPECTOR GENERAL METRICS

Based on our analysis of the 20 core IG metrics, we identified weaknesses in two metrics that could be addressed to improve the effectiveness of TVA's ISP and practices. Specifically, the weaknesses include security workforce assessment in the Protect function and BIA in the Recover function.

Security Workforce Assessment
TVA has defined processes for assessing the knowledge, skills, and abilities of its cybersecurity workforce to determine awareness and specialized training needs and periodically updating its assessment to account for a changing risk environment. However, TVA has not assessed the knowledge, skills, and abilities of the cybersecurity workforce; therefore, TVA has not tailored awareness and specialized training or fully identified skill gaps. Without implementing and leveraging a skills assessment, TVA cannot address identified knowledge, skills, and abilities gaps through training or talent acquisition.

Business Impact Analysis
TVA has defined and consistently implemented policies, procedures, and processes for conducting organizational and system-level BIA and incorporating the results into strategy and planning development efforts. However, TVA has not ensured the results of BIAs are (1) integrated with the enterprise risk management process and (2) used in conjunction with the risk register to calculate potential overall risk and inform senior level decision-making. Therefore, TVA cannot (1) consistently evaluate, record, and monitor the criticality and sensitivity of enterprise assets and (2) adequately calculate potential overall risk at an enterprise-wide level.

SUPPLEMENTAL INSPECTOR GENERAL METRICS

Based on our analysis of the 20 FY 2023 supplemental IG metrics, we identified weaknesses in three metrics that could be addressed to improve the effectiveness of TVA's ISP and practices. Specifically, the weaknesses include VDP in the Protect function and contingency planning and recovery activities communication in the Recover function.

Vulnerability Disclosure Policy

TVA has developed, documented, and publicly disseminated a comprehensive VDP. However, TVA has not included all internet accessible federal systems in the scope of the VDP. According to DHS Binding Operational Directive 20-01,[4] a VDP includes federal information systems "accessible over the internet, which encompasses those systems directly managed by an agency as well as those operated on an agency's behalf." Without including all internet accessible federal systems in its VDP, TVA (1) may not be aware of security risks that need to be mitigated and (2) cannot properly monitor, analyze, and report on the qualitative and quantitative performance measures used to gauge the effectiveness of its VDP and disclosure handling procedures.

Contingency Planning

TVA has defined, communicated, and implemented contingency planning policies and procedures, including roles and responsibilities for test, training and exercise activities across the organization. In addition, TVA has designated appropriate teams to implement contingency planning strategies. However, we determined (1) TVA's contingency plans did not include the detailed contact information for the individuals required to perform the roles and responsibilities and (2) not all contingency plans have been tested annually as required by TVA policy; therefore, the training could not be conducted for the untested plans. Without detailed contact information and consistently implementing its contingency plan testing and training, TVA cannot ensure (1) resources are allocated in a risk-based manner for stakeholders to effectively implement system contingency planning activities, and (2) stakeholders are held accountable for carrying out their roles and responsibilities effectively.

Recovery Activities Communication

TVA has defined and consistently communicated information on the planning and performance of recovery activities for completed business critical applications to relevant stakeholders and executive management teams. However, TVA has not (1) communicated metrics on the effectiveness of recovery activities to relevant stakeholders and (2) ensured that the data supporting the metrics are obtained accurately, consistently, and in a reproducible format. Without qualitative and quantitative metrics, TVA cannot communicate risk and contingency plan changes and improve coordination of recovery activities in the event of an incident.

[4] Binding Operational Directive 20-01, *Develop and Publish a Vulnerability Disclosure Policy*, September 2, 2020.

RECOMMENDATIONS

We recommend the Vice President and Chief Information and Digital Officer, Technology and Innovation:

1. Implement a knowledge, skills, and abilities assessment to tailor cybersecurity awareness and specialized training, identify gaps in TVA's cybersecurity workforce, and subsequently address the identified gaps through training or talent acquisition.

2. Update processes to ensure that the results of BIAs are consistently (a) integrated with the enterprise risk management process and (b) used in conjunction with the risk register to calculate potential overall risk and inform senior level decision-making.

3. Update TVA's VDP to include all internet-accessible federal systems in the scope of the policy and create performance measures to gauge the effectiveness of its VDP and disclosure handling procedures.

4. Perform annual test, training, and exercise activities of each business critical application as required by TVA policy to ensure (a) contingency training is provided consistently with the roles and responsibilities to identify and include the appropriate content and level of detail, and (b) resources are allocated in a risk-based manner and stakeholders are held accountable.

5. Implement and communicate accurate, consistent, and reproducible metrics on the effectiveness of recovery activities to relevant stakeholders.

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

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine the effectiveness of the Tennessee Valley Authority's (TVA) information security program (ISP) and practices as defined by the *FY 2023 – 2024 IG Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (Appendix B). Our audit scope was limited to answering the FY 2023 IG metrics, which included 20 core and 20 supplemental IG metrics (Appendix B). The security controls significant to the objective were incorporated into the FY 2023 IG metrics and associated maturity models.

Our fieldwork was completed between February 2023 and August 2023.

To accomplish our objective, we:

- Inquired with TVA Technology and Innovation personnel and conducted walkthroughs as necessary to gain an understanding and clarification of the policies, processes, and current state of TVA's ISP.
- Reviewed TVA documentation to corroborate our understanding and assess the current state of TVA's ISP, including:
  - Relevant TVA agency-wide and business unit specific policies, procedures, and documents (such as Standard Programs and Processes and Work Instructions).
  - Technology and Innovation organizational chart.
  - Vulnerability Disclosure Policy.
- Reviewed previous Office of Inspector General audit reports on TVA's (1) compliance with the FISMA in FY 2022,[1] and (2) remote application and desktop virtualization client in FY 2023[2] for relevant findings.
- Reviewed the contingency plan and after action report for one business critical application that was completed in 2023 and performed a walkthrough to determine if appropriate content and level of detail was included.
- Assessed the maturity level for 20 core metrics and 20 supplemental metrics contained in the *FY 2023-2024 IG FISMA Reporting Metrics.*
- Calculated an average of the FY 2023 metrics for each function and corresponding domains included in Table 1 on the following page.

[1] Audit Report 2022-17370, *Federal Information Security Modernization Act*, September 19, 2022.
[2] Audit Report 2022-17390, *Remote Application and Desktop Virtualization Client*, June 21, 2023.

FY 2023 FISMA Functions and Corresponding Domains	
Function	**Domain**
Identify	Risk Management Supply Chain Risk Management
Protect	Configuration Management Identity and Access Management Data Protection and Privacy Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

Table 1

During the course of this audit, we determined the overall effectiveness of TVA's ISP and practices by assessing the 40 IG metrics (Appendix B) on a maturity model spectrum. Table 2 below details the five maturity model levels.

FY 2023 IG FISMA Maturity Definitions	
Maturity Level	**Maturity Level Description**
Level 1: *Ad-hoc*	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: *Defined*	Policies, procedures, and strategies are formalized and documented, but not consistently implemented.
Level 3: *Consistently Implemented*	Policies, procedures, and strategies 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 strategies are collected across the organization and used to assess them and make necessary changes.
Level 5: *Optimized*	Policies, procedures, and strategies 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

The maturity level was determined by answering the related FY 2023 IG metrics, which included 20 core and 20 supplemental IG metrics and using the average of the metrics in a particular domain to determine the effectiveness of individual function areas and the overall program. The FISMA methodology considers metrics at a maturity level 4 (managed and measurable) or higher to be at an effective level of security.

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 objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics

February 10, 2023

Document History

Version	Date	Comments	Sec/Page
1.0	1/6/2023	Initial draft sent to stakeholders for comment	All
1.1	2/10/2023	Final version	All

Contents

GENERAL INSTRUCTIONS

Overview

This document outlines the Office of Management and Budget's (OMB) guidance for implementing the requirements outlined in OMB Memorandum M-23-03, Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements. The guidance below and related metrics were developed in coordination amongst representatives from the OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), with review and feedback provided by several stakeholders, including the Federal CIO and CISO councils. As noted in OMB M-23-03, IGs are required to provide their responses to the FY 2023 FISMA metrics outlined in this document in the CyberScope reporting tool by July 31, 2023.

Background and Methodology

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. OMB, CIGIE, and other stakeholders worked collaboratively to develop the *FY 2023-2024 IG FISMA Reporting Metrics*. The *FY 2023-2024 IG FISMA Reporting Metrics* represent a continuation of the work started in FY 2022, when the IG metrics reporting process was transitioned to a multi-year cycle.

The Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements (M-22-05) encouraged agencies to shift towards a continuous assessment process for their annual independent assessment. To help facilitate this, the memo also announced that OMB and CIGIE are transitioning the IG FISMA metrics to a multi-year cycle—with a set of core metrics that must be evaluated annually and the remaining metrics that will be evaluated on a two-year cycle, beginning in FY 2023.[1]

The core metrics represent a combination of Administration priorities and other highly valuable controls that must be evaluated annually. Specifically, these core metrics align with the Executive Order on Improving the Nation's Cybersecurity (EO 14028), and guidance from OMB to agencies to improve federal cybersecurity, including:

- Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (M-22-09), sets forth a plan for migrating the federal government to a new cybersecurity paradigm that does not presume that any person or device inside an organization's perimeter is trusted, and focuses agencies on strengthening their capability to limit, and continuously verify, the access those people and devices have to government data.
- Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents (M-21-31), sets detailed requirements for log management, configuration, and enterprise-level centralization. It also provides a maturity model that prioritizes the most critical software types and requirements.
- Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response (M-22-01), directs agencies to coordinate

[1] These changes do not in any way limit the scope of IG authority to evaluate information systems on an as-needed or ad-hoc basis.

with the Cybersecurity and Infrastructure Security Agency (CISA) to accelerate their adoption of robust EDR solutions, an essential component for zero trust architecture that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.

- Enhancing the Security of the Software Supply Chain through Secure Software Development Practices (M-22-18), initiates a government-wide shift towards requiring agencies to use software developed in a secure manner. This will minimize the risks associated with running unvetted technologies on agency networks, increasing the resilience of Federal technology against cyber threats.

The IG FISMA metrics are aligned with the five function areas in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): *identify*, *protect*, *detect*, *respond*, and *recover* (table 1). 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.

Table 1: IG Metrics and NIST Cybersecurity Framework Function Areas and Categories

IG Metric Function Area and Related Domains[a]	Related Cybersecurity Framework Categories
Identify (Risk Management)	Asset Management (ID.AM), Business Environment (ID.BE), Governance (ID.GV), Risk Assessment (ID.RA), and Risk Management Strategy (ID.RM)
Identify (Supply Chain Risk Management)	Supply Chain Risk Management (ID.SC)
Protect (Configuration Management)	Information Protection Processes and Procedures (PR.IP)
Protect (Identity and Access Management)	Identity Management and Access Control (PR.AC)
Protect (Data Protection and Privacy)	Data Security (PR.DS)
Protect (Security Training)	Awareness and Training (PR.AT)
Detect (Information Security Continuous Monitoring)	Security Continuous Monitoring (DE.CM)
Respond (Incident Response)	Response Planning (RS.RP), Communications (RS.CO), Analysis (RS.AN), Mitigation (RS.MI), and Improvements (RS.IM)
Recover (Contingency Planning)	Recovery Planning (RC.RP), Improvements (RC.IM), and Communications (RC.CO)

[a] Refer to the NIST glossary for definitions of the function areas and domains.

Key Changes to the FY 2023 – 2024 IG FISMA Metrics

One of the goals of the annual FISMA evaluations is to assess agencies' progress toward achieving outcomes that strengthen Federal cybersecurity. The FY 2023 – 2024 FISMA IG metrics have been updated to determine agency progress in implementing these requirements, as follows:

- OMB M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements* – By the end of FY 2023, agencies are required to report at least 80% of government-furnished equipment through the DHS' CDM program. As such, metric #2 regarding hardware asset management has been updated to reflect this new requirement.
- DHS Binding Operational Directive 23-01, *Improving Asset Visibility and Vulnerability Detection on Federal Networks* – By April 3, 2023, agencies are required to take specific actions for asset discovery, vulnerability enumeration, and automated reporting. Metrics #2, #20, and #21 regarding hardware asset management, configuration settings, and flaw remediation, respectively, have been updated accordingly.
- OMB M-21-30, *Protecting Critical Software through Enhanced Security Measures* – This memorandum provides guidance on the implementation of security measures for EO-critical software. As such, metric #3 regarding software asset management has been updated.
- OMB M-22-18, *Enhancing the Security of the Software Supply Chain Through Secure Software Development Practices* – This memorandum requires agencies to comply with NIST guidance and any subsequent updates related to software supply chain security. Metric #14 regarding third-party security has been updated to reflect requirements regarding software producer self-attestations.
- OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* – This memorandum directs agencies to take action to strengthen audit logging, log retention, and log management capabilities. As such, Metrics #32 and #54 regarding privileged account management and incident detection and analysis, respectively, have been updated to reflect these requirements.
- OMB M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* – This memorandum directs agencies to take action to strengthen their endpoint detection and response solutions and capabilities. As such, metric #37 regarding data exfiltration and enhanced network defenses has been updated to reflect these requirements.

FISMA Metric Ratings

IGs are required to assess the effectiveness of information security programs on a maturity model spectrum, in which the foundational levels ensure that agencies develop sound policies and procedures and the advanced levels capture the extent that agencies institutionalize those policies and procedures. The five maturity model levels are *ad hoc*, *defined*, *consistently implemented*, *managed and measurable*, and *optimized* (table 2). Within the context of the maturity model, OMB believes that achieving a Level 4 (*managed and measurable*) or above represents an effective level of security. NIST provides additional

guidance for determining the effectiveness of security controls.[2] IGs should consider both their and the agency's assessment of unique missions, resources, and challenges when determining information security program effectiveness. IGs have the discretion to determine whether an agency is effective in each of the Cybersecurity Framework Function (*e.g., protect, detect*) and whether the agency's overall information security program is effective based on the results of the determinations of effectiveness in each function and the overall assessment. Therefore, an IG has the discretion to determine that an agency's information security program is effective even if the agency does not achieve a Level 4 *(managed and measurable)*.

Table 2: IG Evaluation Maturity Levels

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

Reflecting OMB's shift in emphasis away from compliance in favor of risk management-based security outcomes, IGs are encouraged to evaluate the IG metrics based on the risk tolerance and threat model of their agency and to focus on the practical security impact of weak control implementations, rather than strictly evaluating from a view of compliance or the mere presence or absence of controls.

In response to the threat environment and technology ecosystem which continue to evolve and change at a faster pace each year, OMB implemented a new framework regarding the timing and focus of assessments in FY2022. The goal of this new framework was to provide a more flexible but continued focus on annual assessments for the federal community. This effort yielded two distinct groups of metrics: Core and Supplemental.

Core Metrics – Metrics that are assessed annually and represent a combination of Administration priorities, high impact security processes, and essential functions necessary to determine security program effectiveness.

[1] NIST Special Publication (SP) 800-53, Rev. 5, Security and Privacy Controls for 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.

Supplemental Metrics – Metrics that are assessed at least once every two years and represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.

IGs should leverage the core metrics to gain a clear picture of where agencies stand as it relates to the priority objectives outlined above. However, those priorities do not account for the totality of efforts made by agencies to secure their environments. IGs are encouraged to leverage supplemental metric scores, additional reports (including past evaluations where results have had little variance year over year), and any additional evidence of information security program effectiveness to provide context within the evaluation period (or past periods, as applicable). These additional considerations should be documented in Cyberscope to justify the effectiveness determinations made by IGs.

Scoring Methodology

In previous years, IGs have been directed to utilize a mode-based scoring approach to assess agency maturity levels. Under this approach, ratings throughout the reporting domains were determined by a simple majority, where the most frequent level (i.e., the mode) across the questions served as the domain rating. The same logic was applied at the function and overall information security program level. However, in FY 2021, OMB and CIGIE conducted a pilot to score agencies based on a weighted average for certain priority metrics. One purpose of this pilot was to help evaluate the impacts of these priority metrics and prepare agencies for the possibility of changing the maturity calculation process in the future.

Through analyses of the data obtained through this pilot and the FY2020 – FY2022 governmentwide IG FISMA reporting, OMB and CIGIE determined that a non-weighted (e.g., calculated) average more closely aligned with the OIG's assessed maturity levels expressed in a numeric format. This result highlights that maturity levels assigned by IGs at the domain, function, and information security program levels align more closely to an approach based on a calculated average than one based on the mode. Further, with the introduction of Core metrics in FY 2022, a mode-based scoring approach, where all metrics are weighted equally, may not provide an accurate assessment of maturity in cases where specific domains and function areas may not have a large number of metrics. Therefore, ratings in FY 2023 will focus on a calculated average approach, wherein the average of the metrics in a particular domain will be used by IGs to determine the effectiveness of individual function areas (*identify, protect, detect, respond*, and *recover*) and the overall program.

To provide IGs with additional flexibility and encourage evaluations that are based on agencies' risk tolerance and threat models, calculated averages will not be automatically rounded to a particular maturity level. In determining maturity levels and the overall effectiveness of the agency's information security program, OMB strongly encourages IGs to focus on the results of the core metrics, as these tie directly to Administration priorities and other high-risk areas. IGs should use the calculated averages of the supplemental metrics as a data point to support their risk-based determination of overall program and function level effectiveness. Other data points that IGs may consider include:

- The results of cybersecurity evaluations, including system security control reviews, vulnerability scanning, and penetration testing conducted during the review period;
- The progress made by agencies in address outstanding IG recommendations; and,
- Reported security incidents reported during the review period.

As in previous years, IGs should provide comments in Cyberscope to explain the rationale for their overall effectiveness ratings at the domain, function, and information security program levels. Additionally, for any metrics rated lower than level 4, IGs will be required to provide comments. Comments in Cyberscope should reference how the agency's risk appetite and tolerance level with respect to adequate security, including compensating controls, were factored into the IGs maturity level determinations.

IGs continue to retain the discretion to determine the overall effectiveness of their respective agency's information security program, in accordance with Cybersecurity Framework function effectiveness (e.g., *identify*, *protect*), and the individual domain ratings (e.g., *risk management*, *configuration management*) at the maturity level based on their evaluations. Using this approach, IGs may determine that a particular domain, function area, and/or the agency's information security program is effective at a calculated maturity level lower than Level 4.

To that end, this document introduces a calculated average scoring model for FY 2023 and FY 2024. As part of this approach, Core metrics and Supplemental metrics will be averaged independently to determine a domain's maturity calculation and provide data points for the assessed program and function effectiveness. For example, if the calculated Core metric maturity of two of the function areas is Level 3 (*consistently implemented)* and the calculated Core metric maturity of the remaining three function areas is Level 4 (*managed and measurable*), then the information security program rating would average a 3.60. A hypothetical example of an IG evaluation for Core and Supplemental metrics in the *risk management* domain and the overall program evaluation is shown in the tables below.[1]

Table 3: Example of Calculated Average for Core Metrics Maturity Calculation in FY 2023

Core Metrics				
Metric Number	**Function**	**Metric Descriptor**	**Review Cycle**	**FY23 IG Rating**
1	Identify	System inventory	Core Metric	Level 4
2	Identify	Hardware asset management	Core Metric	Level 4
3	Identify	Software asset management	Core Metric	Level 3
5	Identify	Cybersecurity risk management and ERM integration	Core Metric	Level 3
10	Identify	Automated view of risk	Core Metric	Level 4
TOTAL			**5 core metrics in FY23**	**18**

[1] This example does not take into consideration the ratings of the *supply chain risk management* domain metrics, which Cyberscope will include in the calculation for the *identify* function area.

Table 4: Example of Calculated Average for Supplemental Metrics Maturity Calculation in FY23

FY23 Supplemental Metrics				
Metric Number	**Function**	**Metric Descriptor**	**Review Cycle**	**FY23 IG Rating**
7	Identify	Roles and responsibilities	FY23	Level 3
8	Identify	Plan of action and milestones	FY23	Level 4
9	Identify	Risk communication	FY23	Level 3
TOTAL			**3 supplemental metrics in FY23**	**10**

Table 5: Example of Calculated Average FY24 Supplemental Metrics Maturity Calculation in FY24

FY24 Supplemental Metrics				
Metric Number	**Function**	**Metric Descriptor**	**Review Cycle**	**FY24 IG Rating**
4	Identify	System categorization	FY24	Level 4
6	Identify	Information security architecture	FY24	Level 3
TOTAL			**2 supplemental metrics in FY24**	**7**

Table 6: Example of Overall Calculated Averages Maturity Calculation in FY23

FY23 Summary					
Function	**Core Metrics**	**FY23 Supp. Metrics**	**FY24 Supp. Metrics**	**FY23 Assessed Maturity**	**FY23 Justification**
Identify	3.6	3.3	N/A	Effective	Ipsum lorem.
Protect	4.0	3.7	N/A	Effective	Ipsum lorem.
Detect	3.0	3.1	N/A	Not Effective	Ipsum lorem.
Respond	4.0	4.0	N/A	Effective	Ipsum lorem.
Recover	3.4	3.1	N/A	Not Effective	Ipsum lorem.
Overall Maturity	**3.6**	**3.4**	**N/A**	**Not Effective**	**Ipsum lorem.**

Table 7: Example of Overall Calculated Averages Maturity Calculation in FY24

FY24 Summary					
Function	**Core Metrics**	**FY23 Supp. Metrics**	**FY24 Supp. Metrics**	**FY24 Assessed Maturity**	**FY24 Justification**
Identify	3.7	3.3	3.5	Effective	Ipsum lorem.
Protect	4.0	3.7	3.6	Effective	Ipsum lorem.
Detect	3.2	3.1	3.2	Not Effective	Ipsum lorem.
Respond	4.0	4.0	3.9	Effective	Ipsum lorem.
Recover	3.4	3.1	3.2	Not Effective	Ipsum lorem.
Overall Maturity	**3.7**	**3.4**	**3.5**	**Not Effective**	**Ipsum lorem.**

Table 6 shows that this agency's information security program is struggling to mature their detection capability in FY23 and the IG believes that the *detect* and *recover* capabilities are not effective based on the combination of OMB's recommendation for a *Level 4 – Managed and Measurable* rating, relevant OMB Memoranda, additional reports and tests conducted during the period, results demonstrated during the evaluation period, and have taken the agency's unique missions, resources, and challenges into consideration. However, the IG has determined that the agency is effective in the *identify* domain based the same criteria and based on professional judgment has determined that the agency is operating effectively in this area.

Tables 5 and 7 show a potential agency result in FY24 and while the agency has improved in some areas, the IG has reassessed and reached the same conclusion as the previous year. Variation will occur from the examples above, however, the justification provided by the IG will outline the judgments made in a particular agency's evaluation.

These examples are intended to be illustrative and, while demonstrating a potential outcome, should only be used as a reference point to understand the lines between the evaluation of the maturity of an organization and the relationship to the IG's professional judgment of the security program's effectiveness and the program's effectiveness in the respective function areas. Each agency will have different missions and implementations of such missions and the IG should take that into account when comparing against the desired level outlined by OMB.

Submission Deadline

Historically, the evaluation of agency effectiveness by IGs finished in October; however, this timing limited agency leadership's ability to request resources in the next budget year to provide for remediations. As such, OMB M-22-05 adjusted the timeline for the IG evaluation of agency information security effectiveness to better align with the budget submission cycle. OMB is requesting that agency IGs submit FY23 FISMA metric data from agency evaluations via Cyberscope **no later than July 31, 2023**.

Cyberscope will also provide supplementary fields to allow the IG to provide additional comments and data supporting their evaluation results.

FISMA Metrics Evaluation Guide

To promote consistency in IG annual FISMA evaluations, an evaluation guide will be developed for IGs to use in their FY 2023 and FY 2024 FISMA evaluations. This guide provides a baseline of suggested sources of evidence and test steps/objectives that can be used by IGs as a part of their FISMA evaluations. The guide, which is a companion document to the *FY 2023-2024 IG FISMA Reporting Metrics*, also includes suggested types of analysis that IGs may perform to assess capabilities in given areas. As in previous years, the FISMA evaluation guidance will be published on DHS' FISMA website.

IDENTIFY FUNCTION AREA

Table 8: Risk Management

Question	Criteria	Review Cycle	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
1. To what extent 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 800-37 (Rev. 2) • NIST SP 800-53 (Rev. 5): CA-3, PM-5, and CM-8 • NIST Cybersecurity Framework (CSF): ID.AM-1 – 4 • FY 2023 CIO FISMA Metrics: 1.1 and 1.5 • OMB A-130 • OMB M-23-03	Core Metric	The organization has not defined its policies, procedures, and processes for developing and maintaining a comprehensive and accurate inventory of its information systems and system interconnections.	The organization has defined its policies, procedures, and processes for developing and maintaining a comprehensive and accurate inventory of its information systems and system interconnections.	The organization consistently implements its policies, procedures, and processes to maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public-facing websites, and third-party systems), and system interconnections.	The organization ensures that the information systems included in its inventory are subject to the monitoring processes defined within the organization's ISCM strategy.	The organization uses automation to develop and maintain a centralized information system inventory that includes hardware and software components from all organizational information systems. The centralized inventory is updated in a near-real time basis.
2. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including GFE and Bring Your Own Device (BYOD) mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting?	• NIST SP 800-37 (Rev. 2): Tasks P-10 and P-16 • NIST SP 800-53 (Rev. 5): CA-7 and CM-8 • NIST SP 800-137 • NIST SP 800-207 • NIST 1800-5 • NIST IR 8011 • NIST CSF: ID.AM-1 • Federal Enterprise Architecture (FEA) Framework • FY 2023 CIO FISMA Metrics: 1.2, 1.3, and 10.8 • CIS Top 18 Security Controls: Control 1 • OMB M-23-03 • DHS Binding Operational Directive (BOD) 23-01 • BOD 23-01 Implementation Guidance	Core Metric	The organization has not defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network (including through automated asset discovery) with the detailed information necessary for tracking and reporting.	The organization has defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network (including through automated asset discovery) with the detailed information necessary for tracking and reporting.	The organization consistently uses its standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network (including through automated asset discovery) and uses this taxonomy to inform which assets can/cannot be introduced into the network. The organization is making sufficient progress towards reporting at least 80% of its GFEs through DHS' CDM program.	The organization ensures that the hardware assets connected to the network are covered by an organization-wide hardware asset management capability and are subject to the monitoring processes defined within the organization's ISCM strategy. For mobile devices, the agency enforces the capability to deny access to agency enterprise services when security and operating system updates have not been applied within a given period based on agency policy or guidance.	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.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Review Cycle	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
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 800-37 (Rev. 2): Task P-10 • NIST SP 800-53 (Rev. 5): CA-7, CM-8, CM-10, and CM-11 • NIST SP 800-137 • NIST SP 800-207: Section 7.3 • NIST 1800-5 • NIST IR 8011 • NIST Security Measures for EO-Critical Software Use • NIST CSF: ID.AM-2 • FEA Framework • FY 2023 CIO FISMA Metrics: 1.4 and 4.1 • OMB M-21-30 • OMB M-22-09 • OMB M-22-18 • OMB M-23-03 • CIS Top 18 Security Controls: Control 2 • CISA Cybersecurity Incident Response Playbooks	Core Metric	The organization has not defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses, including for EO-critical software and mobile applications, used in the organization's environment with the detailed information necessary for tracking and reporting.	The organization has defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses, including for EO-critical software and mobile applications, used in the organization's environment with the detailed information necessary for tracking and reporting.	The organization consistently uses its standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses, including for EO-critical software and mobile applications, used in the organization's environment and uses this taxonomy to inform which assets can/cannot be introduced into the network. The organization establishes and maintains a software inventory for all platforms running EO-critical software and all software (both EO-critical and non-EO-critical) deployed to each platform.	The organization ensures that the software assets, including EO-critical software and mobile applications as appropriate, on the network (and their associated licenses), are covered by an organization-wide software asset management (or Mobile Device Management) capability and are subject to the monitoring processes defined within the organization's ISCM strategy. For mobile devices, the agency enforces the capability to prevent the execution of unauthorized software (e.g., blacklist, whitelist, or cryptographic containerization).	The organization employs automation to track the life cycle of the organization's software assets (and their associated licenses), including for EO-critical software and mobile applications, 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.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Review Cycle	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
4. To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets?	• NIST SP 800-37 (Rev. 2): Tasks C-2, C-3, P-4, P-12, P-13, S-1 – S-3 • NIST SP 800-53 (Rev. 5): RA-2, PM-7, and PM-11 • NIST SP 800-60 • NIST IR 8170 • NIST CSF: ID.BE-3, ID.AM-5, and ID.SC-2 • FIPS 199 • FY 2023 CIO FISMA Metrics: 1.1 • OMB M-19-03	FY24	The organization has not defined policies, procedures, and processes for categorizing, reviewing, and communicating the importance/priority of information systems in enabling its missions and business functions, including for high value assets, as appropriate. In addition, the organization has not defined its policies, procedures, and processes for controls allocation, selection, and tailoring based on the importance/ priority of its information systems.	The organization has defined policies, procedures, and processes for categorizing, reviewing, and communicating the importance/priority of information systems in enabling its missions and business functions, including for high value assets, as appropriate. In addition, the organization has defined policies, procedures, and processes for controls allocation, selection and tailoring based on the importance/ priority of its information systems.	The organization consistently implements its policies, procedures, and processes for system categorization, review, and communication, including for high value assets, as appropriate. Security categorizations consider potential adverse impacts to organization operations, organizational assets, individuals, other organizations, and the Nation. System categorization levels are used to guide risk management decisions, such as the allocation, selection, and implementation of appropriate control baselines.	The organization ensures the risk-based allocation of resources based on system categorization, including for the protection of high value assets, as appropriate, through collaboration and data-driven prioritization.	The organization uses impact-level prioritization for additional granularity, and cybersecurity framework profiles, as appropriate, to support risk-based decision-making.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Review Cycle	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
5. To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels?	• NIST SP 800-37 (Rev. 2): Tasks P-2, P-3, P-14, R-2, and R-3 • NIST SP 800-39 • NIST SP 800-53 (Rev. 5): RA-3 and PM-9 • NIST IR 8286 • NIST IR 8286A • NIST IR 8286B • NIST IR 8286C • NIST IR 8286D • NIST CSF: ID.RM-1 – ID.RM-3 • OMB A-123 • OMB M-16-17 • OMB M-23-03	Core Metric	The organization has not defined and communicated the policies, procedures and processes it uses to manage the cybersecurity risks associated with operating and maintaining its information systems. At a minimum, the policies, procedures, and processes do not cover the following areas from a cybersecurity perspective: • Risk framing • Risk assessment • Risk response • Risk monitoring	The organization has defined and communicated the policies, procedures and processes it uses to manage the cybersecurity risks associated with operating and maintaining its information systems. The policies, procedures, and processes cover cybersecurity risk management at the organizational, mission/business process, and information system levels and address the following components • Risk framing • Risk assessment • Risk response • Risk monitoring	The organization consistently implements its policies, procedures, and processes to manage the cybersecurity risks associated with operating and maintaining its information systems. The organization ensures that decisions to manage cybersecurity risk at the information system level are informed and guided by risk decisions made at the organizational and mission/business levels. System risk assessments are performed [according to organizational defined time frames] and appropriate security controls to mitigate risks identified are implemented on a consistent basis. The organization uses the common vulnerability scoring system, or similar approach, to communicate the characteristics and severity of software vulnerabilities. Further, the organization uses a cybersecurity risk register to manage risks, as appropriate, and is consistently capturing and sharing lessons learned on the effectiveness of cybersecurity risk management processes and updating the program accordingly.	The organization uses the results of its system level risk assessments, along with other inputs, to perform and maintain an organization-wide cybersecurity and privacy risk assessment. The result of this assessment is documented in a cybersecurity risk register and serve as an input into the organization's enterprise risk management program. The organization consistently monitors the effectiveness of risk responses to ensure that risk tolerances are maintained at an appropriate level. The organization ensures that information in cybersecurity risk registers is obtained accurately, consistently, and in a reproducible format and is used to (i) quantify and aggregate security risks, (ii) normalize cybersecurity risk information across organizational units, and (iii) prioritize operational risk response.	The cybersecurity risk management program is fully integrated at the organizational, mission/business process, and information system levels, as well as with the entity's enterprise risk management program. Further, the organization's cybersecurity risk management program is embedded into daily decision making across the organization and provides for continuous identification and monitoring to ensure that risk remains within organizationally-defined acceptable levels. The organization uses Cybersecurity Framework profiles and enterprise risk profiles to align cybersecurity outcomes with mission or business requirements, risk tolerance, and resources of the organization.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Review Cycle	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
6. To what extent does the organization use an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain?	• NIST SP 800-37 (Rev. 2): Task P-16 • NIST SP 800-39 • NIST SP 800-53 (Rev. 5): PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9 • NIST SP 800-160 • NIST SP 800-163, (Rev. 1) • NIST SP 800-218 • NIST CSF: ID.SC-1 and PR.IP-2 • FEA Framework • OMB M-15-14 • OMB M-19-03 • OMB M-22-18 • SECURE Technology Act: s. 1326 • Federal Information Technology Acquisition Reform Act (FITARA)	FY24	The organization has not defined an information security architecture and its processes for ensuring that new/acquired hardware/software, including mobile apps, 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. In addition, the organization has defined how it implements system security engineering principles and software assurance processes for mobile applications, within its system development life cycle (SDLC).	The organization has consistently implemented its security architecture across the enterprise, business process, and system levels. System security engineering principles are followed and include assessing the impacts to the organizations information security architecture prior to introducing information system changes into the organization's environment. In addition, the organization employs a software assurance process for mobile applications.	The organization's information security architecture is integrated with its systems development lifecycle and defines and directs implementation of security methods, mechanisms, and capabilities to both the Information and Communications Technology (ICT) supply chain and the organization's information systems.	The organization uses advanced technologies and techniques for managing supply chain risks. To the extent practicable, the organization can quickly adapt its information security and enterprise architectures to mitigate supply chain risks.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Review Cycle	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
7. To what extent have the roles and responsibilities of internal and external stakeholders involved in cybersecurity risk management processes been defined, communicated, implemented, and appropriately resourced across the organization?	• NIST SP 800-37 (Rev. 2): Section 2.8 and Task P-1 • NIST SP 800-39: Sections 2.3.1, 2.3.2, and Appendix D • NIST SP 800-53 (Rev. 5): RA-1 • NIST CSF: ID.AM-6, ID.RM-1, and ID.GV-2 • NIST IR 8286: Section 3.1.1 • OMB A-123 • OMB M-19-03 • OMB M-16-15	FY23	Roles and responsibilities for cybersecurity risk management have not been defined and communicated across the organization. Further, the organization has not defined the relevant work roles for stages in the cybersecurity risk management process and which roles are responsible, accountable, consulted, or informed about various activities, as appropriate. In addition, the organization has not defined the relationships between cybersecurity risk management roles and those roles involved with enterprise risk management.	Roles and responsibilities of stakeholders involved in cybersecurity risk management processes have been defined and communicated across the organization. This includes the relevant work roles for stages in the cybersecurity risk management process and which roles are responsible, accountable, consulted, or informed about various activities, as appropriate. In addition, the organization has defined and clearly communicated the relationships between cybersecurity risk management roles and those roles involved with enterprise risk management.	Individuals are consistently performing the cybersecurity risk management roles and responsibilities that have been defined across the organization. This includes roles and responsibilities related to integration with enterprise risk management processes, as appropriate.	Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement cybersecurity risk management activities and integrate those activities with enterprise risk management processes, as appropriate. Further, stakeholders involved in cybersecurity risk management are held accountable for carrying out their roles and responsibilities effectively.	The organization uses an integrated governance structure, in accordance with A-123, and associated review processes (e.g., ERM councils or IT investment review boards) to support the integration of roles and responsibilities for cybersecurity risk management and ERM.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Review Cycle	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
8. To what extent has the organization ensured that plans of action and milestones (POA&Ms) are used for effectively mitigating security weaknesses?	• NIST SP 800-37 (Rev. 2): Tasks A-6, R-3 • NIST SP 800-53 (Rev. 5): CA-5 and PM-4 • NIST CSF: ID.RA-6 • OMB M-14-04 • OMB M-19-03 • OMB A-130	FY23	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, monitoring and maintenance, and independent validation of POA&M activities.	The organization consistently uses POA&Ms to effectively mitigate security weaknesses. The organization uses a prioritized and consistent approach to POA&Ms that considers: • Security categorizations • Security, privacy, and supply chain risk assessments • Specific control deficiencies and their criticality • Rationale for accepting certain deficiencies in controls • Required POA&M attributes, in accordance with OMB M-04-14 (e.g., severity and brief description of the weakness, remediation tasks and milestones for meeting those tasks, and estimated funding resources required to resolve the weakness) Further, the organization uses lessons learned in implementation to review and update its POA&M processes.	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 in a near real-time basis. Further, processes are in place to identify and manage emerging risks, in addition to known security weaknesses.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Review Cycle	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
9. To what extent does the organization ensure that information about cybersecurity risks is communicated in a timely and effective manner to appropriate internal and external stakeholders?	• NIST SP 800-37 (Rev. 2): Task M-5 • NIST CSF: Section 3.3 • NIST IR 8170 • NIST IR 8286 • OMB A-123 • OMB Circular A-11 • OMB M-19-03 • SECURE Technology Act: s. 1326	FY23	The organization has not defined how cybersecurity risk information is communicated in a timely and effective manner to appropriate internal and external stakeholders.	The organization has defined how cybersecurity risks are identified, documented, and communicated in a timely and effective manner to appropriate internal and external stakeholders. This includes the organizations policies, procedures, and processes for using cybersecurity risk registers, or other comparable mechanisms, to share and coordinate cybersecurity risk activities.	The organization consistently uses a cybersecurity risk register, or other comparable mechanism to ensure that information about risks is communicated in a timely and effective manner to appropriate 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. Further, processes to share cybersecurity risk information are integrated with the organization's ISCM processes.	The organization employs robust diagnostic and reporting frameworks, including dashboards that facilitate a portfolio view of cybersecurity risks across the organization. The dashboard presents qualitative and quantitative metrics that provide indicators of cybersecurity risk. Cybersecurity risks are integrated into enterprise level dashboards and reporting frameworks. The organization ensures that data supporting the cybersecurity risk register, or other comparable mechanism, are obtained accurately, consistently, and in a reproducible format and is used to: • Quantify and aggregate security risks • Normalize information across organizational units • Prioritize operational risk response activities	Using risk profiles and dynamic reporting mechanisms, cybersecurity risk information is incorporated into the organization's enterprise risk management program and used to provide a fully integrated, prioritized, enterprise-wide near real-time view of organizational risks to drive strategic and business decisions. Cyber risks are normalized and translated at the organizational level to support a fully integrated, prioritized, enterprise-wide view of organizational risks to drive strategic and business decisions.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Review Cycle	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
10. To what extent does the organization use technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?	• NIST SP 800-39 • NIST SP 800-207, Tenets 5 and 7 • NIST IR 8286 • OMB A-123 • OMB M-22-09 • CISA Zero Trust Maturity Model: Pillars 2-4 • FY 2023 CIO FISMA Metrics: 7.4.2	Core Metric	The organization has not identified and defined its requirements for an automated solution to provide a centralized, enterprise wide (portfolio) view of cybersecurity 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 cybersecurity 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 cybersecurity risks, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards. All necessary sources of cybersecurity risk information are integrated into the solution.	In addition, the organization ensures that cybersecurity risk management information is integrated into ERM reporting tools (such as a governance, risk management, and compliance tool), as appropriate.	The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its cybersecurity risk management program. Examples include scenario analysis and modeling, the incorporation of technical indicators from threat intelligence, and the ability to consume open security control assessments language (OSCAL) into its GRC processes.
11. 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?							

FY 2023-2024 Inspector General FISMA Reporting Metrics

Table 9: Supply Chain Risk Management (SCRM)

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
12. To what extent does the organization use an organization wide SCRM strategy to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services?	• NIST SP 800-53 (Rev. 5): PM-30, SR-1, and SR-2 • NIST SP 800-161 (Rev. 1) • NIST IR 8276 • The Federal Acquisition Supply Chain Security Act of 2018 (H.R. 7327, 41 USC Chap. 13, Sub chap. III and Chap. 47, P.L. 115-390) • National Counterintelligence Strategy • OMB M-22-18	FY23	The organization has not defined and communicated an organization wide SCRM strategy.	The organization has defined and communicated an organization wide SCRM strategy. The strategy addresses: • SCRM risk appetite and tolerance • SCRM strategies or controls • Processes for consistently evaluating and monitoring supply chain risk • Approaches for implementing and communicating the SCRM strategy • Associated roles and responsibilities	The organization consistently implements its SCRM strategy across the organization and uses the strategy to guide supply chain analyses, communication with internal and external partners and stakeholders, and in building consensus regarding the appropriate resources for SCRM. Further, the organization uses lessons learned in implementation to review and update its SCRM strategy in an organization defined timeframe.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its SCRM 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 SCRM strategy is fully integrated with its enterprise risk management strategy and program. On a near real-time basis, the organization actively adapts its SCRM strategy to respond to evolving and sophisticated threats.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
13. To what extent does the organization use SCRM policies and procedures to manage SCRM activities at all organizational tiers?	• NIST SP 800-53 (Rev. 5): SR-1 • NIST SP 800-161 (Rev. 1) • NIST CSF: ID.SC-1 and ID.SC-5 • NIST IR 7622 • NIST IR 8276 • NIST IR 8419 • The Federal Acquisition Supply Chain Security Act of 2018 • DHS's ICT Supply Chain Library • Securing the Software Supply Chain • OMB M-22-18	FY23	The organization has not defined and communicated its SCRM policies, procedures, and processes.	The organization has defined and communicated its SCRM policies, procedures, and processes. As appropriate, the policies and procedures are guided by the organization wide SCRM strategy (metric #11). At a minimum, the following areas are addressed: • Procedures to facilitate the implementation of the policy and the associated baseline supply chain risk management controls as well as baseline supply chain related controls in other families. • Purpose, scope, SCRM roles and responsibilities, management commitment, and coordination amongst organization entities.	The organization consistently implements its policies, procedures, and processes for managing supply chain risks for [organizationally-defined] products, systems, and services provided by third parties. Further, the organization uses lessons learned in implementation to review and update its SCRM policies, procedures, and processes in an organization defined timeframe.	The organization monitors, analyzes, and reports on the qualitative and quantitative performance measures used to gauge the effectiveness of its SCRM policies and procedures and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format. The organization has integrated SCRM processes across its enterprise, including personnel security and physical security programs, hardware, software, and firmware development processes, configuration management tools, techniques, and measures to maintain provenance (as appropriate); shipping and handling procedures; and programs, processes, or procedures associated with the production and distribution of supply chain elements.	In a near real-time basis, the organization can update its SCRM policies, procedures, and processes, as appropriate, to respond to evolving and sophisticated threats.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
14. To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements?	• NIST SP 800-53 (Rev. 5): SA-4, SR-3, SR-5, and SR-6 • NIST SP 800-152 • NIST SP 800-161 (Rev. 1) • NIST SP 800-218: Task PO.1.3 • NIST IR 8276 • NIST CSF: ID.SC-2 through ID.SC-4 • OMB A-130 • OMB M-19-03 • OMB M-22-18 • CIS Top 18 Security Controls: Control 15 • The Federal Acquisition Supply Chain Security Act of 2018 • FedRAMP standard contract clauses • Cloud computing contract best practices • DHS's ICT Supply Chain Library	Core Metric	The organization has not defined and communicated policies, procedures, and processes to ensure that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and supply chain risk management requirements.	The organization has defined and communicated policies and procedures to ensure that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and supply chain risk management requirements. The following components, at a minimum, are defined • The identification and prioritization of externally provided systems, system components, and services as well how the organization maintains awareness of its upstream suppliers. • Integration of acquisition processes, including the use of contractual agreements that stipulate appropriate cyber and SCRM measures for external providers. • Tools and techniques to use the acquisition process to protect the supply chain, including, risk-based processes for evaluating cyber supply chain risks associated with third party providers, as appropriate. • Contract tools or procurement methods to confirm contractors are meeting their contractual SCRM obligations.	The organization ensures that its policies, procedures, and processes are consistently implemented for assessing and reviewing the supply chain-related risks associated with suppliers or contractors and the system, system component. In addition, the organization obtains sufficient assurance, through audits, test results, software producer self-attestation (in accordance with M-22-18), or other forms of evaluation, that the security and supply chain 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. Furthermore, the organization maintains visibility into its upstream suppliers and can consistently track changes in suppliers.	The organization uses qualitative and quantitative performance metrics (e.g., those defined within SLAs) to measure, report on, and monitor the information security and SCRM performance of organizationally defined products, systems, and services provided by external providers. In addition, the organization has incorporated supplier risk evaluations, based on criticality, into its continuous monitoring practices to maintain situational awareness into the supply chain risks.	The organization analyzes, in a near-real time basis, the impact of material changes to security and SCRM assurance requirements on its relationships with external providers and ensures that acquisition tools, methods, and processes are updated as soon as possible.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
15. To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization's systems?	• NIST SP 800-53 (Rev. 5): SR-11 (1)(2) • NIST SP 800-161 (Rev. 1) • OMB M-22-18 • NIST SP 800-218	FY24	The organization has not defined and communicated its component authenticity policies and procedures.	The organization has defined and communicated its component authenticity policies and procedures. At a minimum the following areas are addressed: • Procedures to detect and prevent counterfeit components from entering the system. • Procedures to maintain configuration control over organizationally defined system components that are awaiting repair and service or repaired components awaiting return to service. • Requirements and procedures for reporting counterfeit system components.	The organization consistently implements its component authenticity policies and procedures. Further, the organization: • Provides component authenticity/anti-counterfeit training for designated personnel. • Maintains configuration control over organizationally defined system components that are awaiting repair and service or repaired components awaiting return to service.	The organization monitors, analyzes, and reports on the qualitative and quantitative performance measures used to gauge the effectiveness of its component authenticity policies and procedures and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format. In addition, the organization has incorporated component authenticity controls into its continuous monitoring practices.	In a near real-time basis, the organization can update its supply chain risk management policies and procedures, as appropriate, to respond to evolving and sophisticated threats.
16. Provide any additional information on the effectiveness (positive or negative) of the organization's supply chain 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 supply chain risk management program effective?							
16.1 Please provide an IG self-assessment rating (Effective/Not Effective) for the agency's *identify* function.							

PROTECT FUNCTION AREA

Table 10: Configuration Management

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
17. To what extent have the roles and responsibilities of configuration management stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?	• NIST SP 800-53 (Rev. 5): CM-1 • NIST SP 800-128: Section 2.4 • Green Book: Principles 3, 4, and 5	FY24	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.	Individuals are performing the roles and responsibilities that have been defined across the organization.	Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively perform information system configuration management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.	The organization continuously evaluates and adapts its configuration management-based roles and responsibilities to account for a changing cybersecurity landscape.
18. To what extent does the organization use 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 phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems?	• NIST SP 800-53 (Rev. 5): CM-9 • NIST SP 800-128: Section 2.3.2	FY24	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 uses 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 uses 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).

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
19. To what extent does the organization use 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 (Rev. 5): CM-2 and CM-8 • NIST CSF: DE.CM-7 and PR.IP-1 • BOD 23-01 • CIS Top 18 Security Controls: Control 4	FY23	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. Further, the organization uses lessons learned in implementation to make improvements to its baseline configuration policies and procedures.	The organization employs automated mechanisms (such as application whitelisting and network management tools) to detect unauthorized hardware, software, and firmware and unauthorized changes to hardware, software, and firmware.	The organization uses 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.
20. To what extent does the organization use configuration settings/common secure configurations for its information systems?	• NIST SP 800-53 (Rev. 5): CM-6, CM-7, RA-5, and SI-2 • NIST SP 800-70 (Rev. 4) • NIST CSF: ID.RA-1 and DE.CM-8 • NIST Security Measures for EO-Critical Software Use: SM 3.3 • OMB M-22-09 • OMB M-23-03 • BOD 23-01 • CIS Top 18 Security Controls: Controls 4 and 7 • CISA Cybersecurity Incident Response Playbooks	Core Metric	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 for configuration settings/common secure configurations. In addition, the organization has developed, documented, and disseminated 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 the principle of least functionality. Further, the organization consistently uses SCAP-validated software assessing (scanning) capabilities against all systems on the network (in accordance with BOD 23-01) to assess and manage both code-based and configuration-based vulnerabilities. The organization uses lessons learned in implementation to make improvements to its secure configuration policies and procedures.	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 and makes appropriate modifications in accordance with organization-defined timelines.	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.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
21. To what extent does the organization use flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management, to manage software vulnerabilities on all network addressable IP-assets?	• NIST SP 800-40 (Rev. 4) • NIST SP 800-53 (Rev. 5): CM-3, RA-5, SI-2, and SI-3 • NIST SP 800-207: Section 2.1 • NIST CSF: ID.RA-1 • NIST Security Measures for EO-Critical Software Use: SM 3.2 • OMB M-22-09 • FY 2023 CIO FISMA Metrics: 1.4, 8.1 and 8.2 • CIS Top 18 Security Controls: Controls 4 and 7 • BOD 18-02 • BOD 19-02 • BOD 22-01 • BOD 23-01 • BOD 23-01 Implementation Guidance • CISA Cybersecurity Incident Response Playbooks	Core Metric	The organization has not developed, documented, and disseminated its policies and procedures for flaw remediation, including for mobile devices (GFE and non-GFE).	The organization has developed, documented, and disseminated its policies and procedures for flaw remediation, including for mobile devices. 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 and uses lessons learned in implementation to make improvements to its flaw remediation policies and procedures. Further, for EO-critical software platforms and all software deployed to those platforms, the organization uses supported software versions.	The organization centrally manages its flaw remediation process and uses automated patch management and software update tools for operating systems, where such tools are available and safe. The organization monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of flaw remediation processes and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.	The organization uses automated patch management and software update tools for all applications and network devices (including mobile devices), as appropriate, where such tools are available and safe. As part its flaw remediation processes, the organization performs deeper analysis of software code, such as through patch sourcing and testing.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
22. To what extent has the organization adopted the Trusted Internet Connection (TIC) 3.0 program to assist in protecting its network?	• NIST SP 800-207 • OMB M-19-26 • DHS-CISA TIC 3.0 Core Guidance Documents • NCPS Cloud Interface Reference Architecture	FY23	The organization has not prepared and planned to meet the goals of the TIC initiative, consistent with OMB M-19-26. Specifically, the agency has not defined and customized, as appropriate, its policies, procedures, and processes to implement TIC 3.0, including updating its network and system boundary policies, in accordance with OMB M-19-26. This includes, as appropriate, the TIC security capabilities catalog, TIC use cases, and TIC overlays. The agency has not defined processes to develop and maintain an accurate inventory of its network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection.	The organization has prepared and planned to meet the goals of the TIC initiative, consistent with OMB M-19-26. Specifically, the agency has defined and customized, as appropriate, its policies, procedures, and processes to implement TIC 3.0, including updating its network and system boundary policies, in accordance with OMB M-19-26. This includes, as appropriate, incorporation of TIC security capabilities catalog, TIC use cases, and TIC overlays. The agency has defined processes to develop and maintain an accurate inventory of its network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection.	The organization consistently implements TIC requirements based on OMB M-19-26. This includes consistent implementation of defined TIC security controls, as appropriate, and ensuring that that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. The agency develops and maintains an accurate inventory of agency network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection.	The organization, in accordance with OMB M-19-26, DHS guidance, and its cloud strategy is ensuring that its TIC implementation remains flexible and that its policies, procedures, and information security program are adapting to meet the security capabilities outlined in the TIC initiative, consistent with OMB M-19-26. The organization monitors and reviews the implemented TIC 3.0 use cases to determine effectiveness and incorporates new/different use cases, as appropriate.	The organization integrates its implementation of TIC 3.0 with the organization's zero trust architecture strategy. Further, for cloud-based environments, the organization provides telemetry on its cloud-based traffic to CISA via the National Cybersecurity Protection System.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
23. 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 SP 800-53 (Rev. 5): CM-2, CM-3, and CM-4 • NIST CSF: PR.IP-3	FY24	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, 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 explicit consideration of security impacts prior to change implementation. The organization uses lessons learned in implementation to make improvements to its change control policies and procedures.	The organization monitors, analyzes, and reports 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. In addition, the organization implements [organizationally defined security responses] if baseline configurations are changed in an unauthorized manner.	The organization uses automation to improve the accuracy, consistency, and availability of configuration change control and configuration baseline information. Automation is also used to provide data aggregation and correlation capabilities, alerting mechanisms, and dashboards on change control activities to support risk-based decision making across the organization.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
24. To what extent does the organization use a vulnerability disclosure policy (VDP) as part of its vulnerability management program for internet-accessible federal systems?	• NIST SP 800-53 (Rev. 5): RA-5(11) • OMB M-20-32 • DHS BOD 20-01 • FY 2023 CIO FISMA Metrics: 9.1, 9.2, and 9.3	FY23	The organization has not developed, documented, and disseminated a comprehensive VDP.	The organization has developed, documented, and publicly disseminated a comprehensive VDP. The following elements are addressed: • The systems in scope • Types of testing allowed • Reporting mechanisms • Timely feedback • Remediation In addition, the organization has updated its vulnerability disclosure handling procedures to support the implementation of its VDP.	The organization consistently implements its VDP. In addition, the organization: • Has updated the relevant fields at the .gov registrar to ensure appropriate reporting by the public. • Ensures that all internet-accessible systems are included in the scope of its VDP. • Increases the scope of systems covered by its VDP, in accordance with DHS BOD 20-01.	The organization monitors, analyzes, and reports on the qualitative and quantitative performance measures used to gauge the effectiveness of its vulnerability disclosure policy and disclosure handing procedures.	On a near real-time basis, the organization actively adapts its vulnerability disclosure policies and procedures and provides information to stakeholders and partners. Within the context of its enterprise risk management program, the organization considers the use of a Bug Bounty program. As appropriate, Bug Bounty programs are implemented in accordance with OMB M-20-32.
25. 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 overall maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?							

FY 2023-2024 Inspector General FISMA Reporting Metrics

Table 11: Identity and Access Management

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
26. To what extent have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?	• NIST SP 800-53 (Rev. 5): AC-1, IA-1, IA-2, PL-4, and PS-1 • NIST SP 800-63-3 • NIST SP 800-63A, B, and C • OMB M-19-17 • Federal Identity, Credential, and Access Management (FICAM) playbooks and guidance • HSPD 12	FY23	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, monitor programs, and ensuring awareness and understanding.	Individuals are performing the roles and responsibilities that have been defined across the organization. The organization ensures that there is consistent coordination amongst organization leaders and mission owners to implement, manage, and maintain the organization's ICAM policy, strategy, process, and technology solution roadmap.	Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement identity, credential, and access management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.	In accordance with OMB M-19-17, the agency has implemented an integrated agency-wide ICAM office, team, or other governance structure in support of its ERM capability to effectively govern and enforce ICAM efforts.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
27. To what extent does the organization use a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities?	• NIST SP 800-53 (Rev. 5): AC-1 and IA-1 • NIST SP 800-207 • NIST CSF: PR.AC-4 and PR.AC-5 • OMB M-19-17 • OMB M-22-09 • DHS ED 19-01 • FICAM • CIS Top 18 Security Controls: Controls 5 and 6	FY23	The organization has not developed a comprehensive ICAM policy, strategy, process, and technology solution road map to guide its ICAM processes and activities. In addition, the organization has not performed a review of current practices, identified gaps, and developed a transition plan to serve as an input to the ICAM policy, strategy, and technology solution road map.	The organization has developed a comprehensive ICAM policy, strategy, process, and technology solution road map to guide its ICAM processes and activities. The organization has developed milestones for how it plans to align with Federal initiatives, including strong authentication, the Federal ICAM architecture and OMB M-19-17, and phase 2 of DHS's Continuous Diagnostics and Mitigation (CDM) program, as appropriate.	The organization is consistently implementing its ICAM policy, strategy, process, and technology solution road map and is on track to meet milestones. The strategy encompasses the entire organization, aligns with the FICAM and CDM requirements, and incorporates applicable Federal policies, standards, playbooks, and guidelines. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its ICAM policy, strategy, and road map and making updates as needed.	The organization integrates its ICAM strategy and activities with its enterprise architecture and the Federal ICAM architecture. The organization uses automated mechanisms (e.g., machine-based, or user-based enforcement), where appropriate, to manage the effective implementation of its ICAM policies, procedures, and strategy. Examples of automated mechanisms include network segmentation based on the label/classification of information stored; automatic removal/disabling of temporary/emergency/ inactive accounts; and use of automated tools to inventory and manage accounts and perform segregation of duties/least privilege reviews.	On a near real-time basis, the organization actively adapts its ICAM policy, strategy, and related processes and activities to a changing cybersecurity landscape to respond to evolving and sophisticated threats. 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.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
28. To what extent has the organization developed and implemented processes for assigning position risk designations and performing appropriate personnel screening prior to granting access to its systems?	• NIST SP 800-53 (Rev. 5): PS-2 and PS-3 • NIST CSF: PR.IP-11 • OMB M-19-17 • National Insider Threat Policy • FY 2023 CIO FISMA Metrics: 7.4.3	FY24	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.	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.
29. 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 (Rev. 5): AC-8, AC-21, CA-3, PL-4, and PS-6	FY23	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 that access its systems.	The organization ensures that access agreements for individuals are completed prior to access being granted to systems and are consistently maintained thereafter. The organization uses more specific/detailed agreements for privileged users or those with access to sensitive information, as appropriate.	The organization uses automation to manage and review user access agreements for privileged and non-privileged users. To the extent practical, this process is centralized.	On a near real-time basis, the organization ensures that access agreements for privileged and non-privileged users are maintained, as necessary.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
30. To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO2, or web authentication) for non-privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access?	• NIST SP 800-53 (Rev. 5): AC-17, IA-2, IA-5, IA-8, and PE-3 • NIST SP 800-63 • NIST SP 800-128 • NIST SP 800-157 • NIST SP 800-207: Tenet 6 • NIST CSF: PR.AC-1 and PR.AC-6 • NIST Security Measures for EO-Critical Software Use: SM 1.1 • FIPS 201-2 • HSPD-12 • OMB M-19-17 • OMB M-22-09 • OMB M-23-03 • CIS Top 18 Security Controls: Control 6 • CISA Capacity Enhancement Guide • FY 2023 CIO FISMA Metrics: 2.3, 2.3.1, 2.3.2, 2.4, 2.9, 2.10, and 2.10.2	Core Metric	The organization has not planned for the use of strong authentication mechanisms for non-privileged users of the organization's facilities [organization-defined entry/exit points], systems, and networks, including for remote access. In addition, the organization has not performed digital identity 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 [organization-defined entry/exit points], systems, and networks, including the completion of digital identity risk assessments.	The organization has consistently implemented strong authentication mechanisms for non-privileged users of the organization's facilities [organization-defined entry/exit points] and networks, including for remote access, in accordance with Federal targets. For instances where it would be impracticable to use the PIV card, the organization uses an alternative token (derived PIV credential) which can be implemented and deployed with mobile devices. Further, for public-facing systems that support multifactor authentication, users are provided the option of using phishing-resistant multifactor authentication.	All non-privileged users use strong authentication mechanisms to authenticate to applicable organizational systems and facilities [organization-defined entry/exit points]. To the extent possible, the organization centrally implements support for non-PIV authentication mechanisms in their enterprise identity management system.	The organization has implemented an enterprise-wide single sign on solution and all 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 near real-time basis.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
31. To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO2, or web authentication) for privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access?	• NIST SP 800-53 (Rev. 5): AC-17 and PE-3 • NIST SP 800-63 • NIST SP 800-128 • NIST SP 800-157 • NIST SP 800-207: Tenet 6 • NIST CSF: PR.AC-1 and PR.AC-6 • NIST Security Measures for EO-Critical Software Use: SM 1.1 • FIPS 201-2 • HSPD-12 • OMB M-19-17 • OMB M-22-09 • OMB M-23-03 • DHS ED 19-01 • CIS Top 18 Security Controls: Control 6 • FY 2023 CIO FISMA Metrics: 2.3, 2.4, 2.9, and 2.10	Core Metric	The organization has not planned for the use of strong authentication mechanisms for privileged users of the organization's facilities [organization-defined entry/exit points], systems, and networks, including for remote access. In addition, the organization has not performed digital identity 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 [organization-defined entry/exit points], systems, and networks, including the completion of digital identity risk assessments.	The organization has consistently implemented strong authentication mechanisms for privileged users of the organization's facilities [organization-defined entry/exit points], and networks, including for remote access, in accordance with Federal targets. For instances where it would be impracticable to use the PIV card, the organization uses an alternative token (derived PIV credential) which can be implemented and deployed with mobile devices.	All privileged users, including those who can make changes to DNS records, use strong authentication mechanisms to authenticate to applicable organizational systems.	The organization has implemented an enterprise-wide single sign on solution and all 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 near real-time basis.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
32. 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?	• NIST SP 800-53 (Rev. 5): AC-1, AC-2, AC-5, AC-6, AC-17, AU-2, AU-3, AU-6, and IA-4 • NIST CSF: PR.AC-4 • NIST Security Measures for EO-Critical Software Use: SM 2.2 • FY 2023 CIO FISMA Metrics: 3.1 • OMB M-19-17 • OMB M-21-31 • DHS ED 19-01 • CIS Top 18 Security Controls: Controls 5, 6, and 8	Core Metric	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; 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. Further, the organization is meeting privileged identity and credential management logging requirements at maturity EL2, in accordance with M-21-31.	The organization is making demonstrated progress towards implementing EL3's advanced requirements for user behavior monitoring to detect and alert on privileged user compromise.
33. 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 800-46 (Rev. 2) • NIST SP 800-53 (Rev. 5): AC-11, AC-12, AC-17, AC-19, AU-2, IA-7, SC-10, SC-13, and SI-4 • NIST CSF: PR.AC-3 • OMB M-22-09	FY23	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.	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.
34. 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 overall maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?							

FY 2023-2024 Inspector General FISMA Reporting Metrics

Table 12: Data Protection and Privacy

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
35. To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems?	• NIST SP 800-37 (Rev. 2): Section 2.3 and Task P-1 • NIST SP 800-53 (Rev. 5): CA-2, RA-3, RA-8, SA-8(33), PM-5(1), PM-20, PM-27, PT-5, PT-6, and SI-12(1) • NIST SP 800-122 • NIST CSF: ID.GV-3 • NIST Privacy Framework • OMB M-19-03 • OMB M-20-04 • OMB A-130: Appendix I • FY 2022 SAOP FISMA Metrics: Sections 1, 4, and 5(b)	FY23	The organization has not established a privacy program and related plans, policies, and procedures as appropriate for the protection of PII collected, used, maintained, shared, and disposed of by information systems. Additionally, roles and responsibilities for the effective implementation of the organization's privacy program have not been defined.	The organization has defined and communicated its privacy program plan and related policies and procedures for the protection of PII that is collected, used, maintained, shared, and/or disposed of by its information systems. In addition, roles and responsibilities for the effective implementation of the organization's privacy program have been defined and the organization has determined the resources and optimal governance structure needed to effectively implement its privacy program.	The organization consistently implements its privacy program by: • Dedicating appropriate resources to the program • Maintaining an inventory of the collection and use of PII • Conducting and maintaining privacy impact assessments and system of records notices for all applicable systems • Reviewing and removing unnecessary PII collections on a regular basis (i.e., SSNs) • Using effective communications channels for disseminating privacy policies and procedures • Ensuring that individuals are consistently performing the privacy roles and responsibilities that have been defined across the organization.	The organization monitors and analyses quantitative and qualitative performance measures on the effectiveness of its privacy activities and uses that information to make needed adjustments. The organization conducts an independent review of its privacy program and makes necessary improvements.	The privacy program is fully integrated with other security areas, such as ISCM, and other business processes, such as strategic planning and risk management. Further, the organization's privacy program is embedded into daily decision making across the organization and provides for continuous identification of privacy risks.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
36. To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle? • Encryption of data at rest • Encryption of data in transit • Limitation of transfer to removable media • Sanitization of digital media prior to disposal or reuse	• NIST SP 800-37 (Rev. 2) • NIST SP 800-53 (Rev. 5): SC-8, SC-28, MP-3, MP-6, and SI-12(3) • NIST SP 800-207 • NIST CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6 • NIST Security Measures for EO-Critical Software Use: SM 2.3 and SM 2.4 • OMB M-22-09 • DHS BOD 18-02 • FY 2023 CIO FISMA Metrics: 2.1, 2.1.1 and 2.2 • CIS Top 18 Security Controls: Control 3	Core Metric	The organization has not defined its policies and procedures in one or more of the specified areas.	The organization's 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 considerations based on data classification and sensitivity.	The organization's policies and procedures have been consistently implemented for the specified areas, including (i) use of FIPS-validated encryption of PII and other agency sensitive data, as appropriate, both at rest and in transit, (ii) prevention and detection of untrusted removable media, and (iii) destruction or reuse of media containing PII or other sensitive agency data.	The organization ensures that the security controls for protecting PII and other agency sensitive data, as appropriate, throughout the data lifecycle are subject to the monitoring processes defined within the organization's ISCM strategy.	The organization employs advanced capabilities to enhance protective controls, including: • Remote wiping • Dual authorization for sanitization of media devices • Exemption of media marking as long as the media remains within organizationally-defined control areas • Configuring systems to record the date the PII was collected, created, or updated and when the data is to be deleted or destroyed according to an approved data retention schedule.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
37. To what extent has the organization implemented security controls (e.g., EDR) to prevent data exfiltration and enhance network defenses?	• NIST SP 800-53 (Rev. 5): SI-3, SI-7(8), SI-4(4)(18), SC-7(10), and SC-18 • NIST CSF: PR.DS-5 • NIST Security Measures for EO-Critical Software Use: SM 4.3 • OMB M-21-07 • OMB M-22-01 • CIS Top 18 Security Controls: Controls 9 and 10 • DHS BOD 18-01 • DHS ED 19-01	Core Metric	The organization has not defined its policies and procedures related to data exfiltration, endpoint detection and response, enhanced network defenses, email authentication processes, and mitigation against DNS infrastructure tampering.	The organization has defined and communicated it policies and procedures for data exfiltration, endpoint detection and response, enhanced network defenses, email authentication processes, and mitigation against DNS infrastructure tampering.	The organization consistently monitors inbound and outbound network traffic, ensuring that all traffic passes through a web content filter that protects against phishing, malware, and blocks against known malicious sites. Additionally, the organization checks outbound communications traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of PII. Also, suspected malicious traffic is quarantined or blocked. In addition, the organization uses email authentication technology and ensures the use of valid encryption certificates for its domains. The organization consistently implements EDR capabilities to support host-level visibility, attribution, and response for its information systems.	The organization analyzes qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses. The organization also conducts exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses. Further, the organization monitors its DNS infrastructure for potential tampering, in accordance with its ISCM strategy. In addition, the organization audits its DNS records. Further, the organization has assessed its current EDR capabilities, identified any gaps, and is coordinating with CISA for future EDR solution deployments.	The organization's data exfiltration and enhanced network defenses are fully integrated into the ISCM and incident response programs to provide near real-time monitoring of the data that is entering and exiting the network, and other suspicious inbound and outbound communications. The organization continuously runs device posture assessments (e.g., using EDR tools) to maintain visibility and analytics capabilities related to data exfiltration.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
38. To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events?	• NIST SP 800-53 (Rev. 5): IR-8 and IR-8(1) • NIST SP 800-122 • OMB M-17-12 • OMB M-23-03 • FY 2022 SAOP FISMA Metrics: Section 12	FY24	The organization has not developed a Data Breach Response Plan that includes the agency's policies and procedures for reporting, investigating, and managing a privacy-related breach. Further, the organization has not established a breach response team that includes the appropriate agency officials.	The organization has defined and communicated its Data Breach Response Plan, including its processes and procedures for data breach notification. Further, a breach response team has been established that includes the appropriate agency officials.	The organization consistently implements its Data Breach Response plan. Additionally, the breach response team participates in table-top exercises and uses lessons learned to make improvements to the plan as appropriate. Further, the organization can identify the specific individuals affected by a breach, send notice to the affected individuals, and provide those individuals with credit monitoring and repair services, as necessary.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization's Data Breach Response plan is fully integrated with incident response, risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. Further the organization employs automation to monitor for potential privacy incidents and takes immediate action to mitigate the incident and provide protection to the affected individuals.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
39. To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements)	• NIST SP 800-53 (Rev. 5): AT-1, AT-2, AT-3, and PL-4 • FY 2022 SAOP FISMA Metrics: Section 9, 10, and 11	FY24	The organization has not defined its privacy awareness training program based on organizational requirements, its mission, and the types of PII that its users have access to. In addition, the organization has not developed role-based privacy training for individuals having responsibility for PII or activities involving PII.	The organization has defined and communicated its privacy awareness training program, including requirements for role-based privacy awareness training. Further, training has been tailored to the organization's mission and risk environment.	The organization ensures that all individuals receive basic privacy awareness training and individuals having responsibilities for PII or activities involving PII receive role-based privacy training at least annually. Additionally, the organization ensures that individuals certify acceptance of responsibilities for privacy requirements at least annually.	The organization measures the effectiveness of its privacy awareness training program by obtaining feedback on the content of the training and conducting targeted phishing exercises for those with responsibility for PII. Additionally, the organization make updates to its program based on statutory, regulatory, mission, program, business process, information system requirements, and/or results from monitoring and auditing.	The organization has institutionalized a process of continuous improvement incorporating advanced privacy training practices and technologies.
40. Provide any additional information on the effectiveness (positive or negative) of the organization's data protection and privacy 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 data protection and privacy program effective?							

FY 2023-2024 Inspector General FISMA Reporting Metrics

Table 13: Security Training

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
41. To what extent have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated, and implemented 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 SP 800-50 • NIST SP 800-53 (Rev. 5): AT-1 • Green Book: Principles 3, 4, and 5	FY23	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.	Individuals are performing the roles and responsibilities that have been defined across the organization.	Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to consistently implement security awareness and training responsibilities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.	The organization continuously evaluates and adapts its security training roles and responsibilities to account for a changing cybersecurity landscape.
42. To what extent does the organization use 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 SP 800-50: Section 3.2 • NIST SP 800-53 (Rev. 5): AT-2, AT-3, and PM-13 • NIST SP 800-181 • Federal Cybersecurity Workforce Assessment Act of 2015 • National Cybersecurity Workforce Framework • CIS Top 18 Security Controls: Control 14 • FY 2023 CIO FISMA Metrics: 6.1 • EO 13870	Core Metric	The organization has not defined its processes for assessing the knowledge, skills, and abilities of its workforce.	The organization has defined its processes for assessing 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 assessed the knowledge, skills, and abilities of its workforce; tailored 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 its identified knowledge, skills, and abilities gaps through training or talent acquisition.	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.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
43. To what extent does the organization use a security awareness and training strategy/plan that leverages its skills assessment and is adapted to its mission and risk environment? 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 • Deployment methods	• NIST SP 800-50: Section 3 • NIST SP 800-53 (Rev. 5): AT-1 • NIST CSF: PR.AT-1 • OMB M-16-15	FY23	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.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
44. To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, 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 SP 800-50: 6.2 • NIST SP 800-53 (Rev. 5): AT-1 and AT-2 • NIST CSF: PR.AT-2 • CIS Top 18 Security Controls: Control 14	FY24	The organization has not defined its security awareness policies, procedures, and related material based on its mission, risk environment, 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 [within organizationally defined timeframes] 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 policies, procedures, and related material and delivery methods based on FISMA requirements, its, 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 [within organizationally defined timeframes] and periodically thereafter. Furthermore, 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 its security awareness policies and procedures are consistently implemented. The organization ensures that all appropriate users complete the organization's security awareness training (or a comparable awareness training for contractors) [within organizationally defined timeframes] 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 program by, for example, conducting phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate. The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness policies, procedures, and practices. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization has institutionalized a process of continuous improvement incorporating advanced security awareness practices and technologies. On a near real-time basis (as determined by the agency given its threat environment), the organization actively adapts its security awareness policies, procedures, processes to a changing cybersecurity landscape and provides awareness and training, as appropriate, on evolving and sophisticated threats.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
45. To what extent does the organization ensure that specialized security training is provided to individuals with significant security responsibilities (as defined in the organization's security policies and procedures and in accordance with 5 Code of Federal Regulation 930.301)?	• NIST SP 800-53 (Rev. 5): AT-3 and AT-4 • EO 13870 • 5 Code of Federal Regulation 930.301	FY24	The organization has not defined its security training policies, procedures, and related materials based on its mission, risk environment, and the types of roles with significant security responsibilities. In addition, the organization has not defined its processes for ensuring that personnel with significant security roles and responsibilities are provided specialized security training [within organizationally defined timeframes] and periodically thereafter.	The organization has defined its security training policies, procedures, and related material based on FISMA requirements, its mission and risk environment, and the types of roles with significant security responsibilities. In addition, the organization has defined its processes for ensuring that personnel with assigned security roles and responsibilities are provided specialized security training [within organizationally defined time frames] and periodically thereafter.	The organization ensures that its security training policies and procedures are consistently implemented. The organization ensures that individuals with significant security responsibilities complete the organization's defined specialized security training (or comparable training for contractors) [within organizationally defined timeframes] and periodically thereafter. The organization also maintains completion records for specialized training taken by individuals with significant security responsibilities. The organization obtains feedback on its security training program and uses that information to make improvements.	The organization obtains feedback on its specialized security training content and processes 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 targeted phishing exercises and following up with additional training, and/or disciplinary action, as appropriate. The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security training policies, procedures, and practices. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization has institutionalized a process of continuous improvement incorporating advanced security training practices and technologies. On a near real-time basis, the organization actively adapts its security training policies, procedures, processes to a changing cybersecurity landscape and provides awareness and training, as appropriate, on evolving and sophisticated threats.
46. 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 overall maturity level generated from the questions above and based on all testing performed, is the security training program effective?							
46.1 Please provide an IG self-assessment rating (Effective/Not Effective) for the agency's *protect* function.							

DETECT FUNCTION AREA

Table 14: Information Security Continuous Monitoring (ISCM)

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
47. To what extent does the organization use information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier?	• NIST SP 800-37 (Rev. 2): Task P-7 • NIST SP 800-53 (Rev. 5): CA-7, PM-6, PM-14, and PM-31 • NIST SP 800-137: Sections 3.1 and 3.6 • NIST Security Measures for EO-Critical Software Use: SM 4.2 • CIS Top 18 Security Controls: Control 13	Core Metric	The organization has not developed, tailored, and communicated its ISCM policies and an organization wide ISCM strategy.	The organization has developed, tailored, and communicated its ISCM policies and strategy. The following areas are included: • Monitoring requirements at each organizational tier • The minimum monitoring frequencies for implemented controls across the organization (The criteria for determining minimum frequencies is established in coordination with organizational officials [e.g., senior accountable official for risk management, system owners, and common control providers] and in accordance with organizational risk tolerance). • The organization's ongoing control assessment approach • How ongoing assessments are to be conducted • Analyzing ISCM data, reporting findings, and reviewing and updating the ISCM policies, procedures, and strategy	The organization's ISCM policies and strategy are 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 policies and strategy.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM policies and strategy and makes updates, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. The organization has transitioned to ongoing control and system authorization through the implementation of its continuous monitoring policies and strategy.	The organization's ISCM policies and strategy are fully integrated with its enterprise and supply chain risk management, configuration management, incident response, and business continuity programs. The organization can demonstrate that it is using its ISCM policies and strategy to reduce the cost and increase the efficiency of security and privacy programs.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
48. To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization?	• NIST SP 800-37 (Rev. 2): Tasks P-7 and S-5 • NIST SP 800-53 (Rev. 5): CA-1 • NIST SP 800-137 • NIST CSF: DE.DP-1 • Green Book: Principles 3, 4, and 5	FY23	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.	Individuals are performing the roles and responsibilities that have been defined across the organization.	Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement ISCM activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.	The organization continuously evaluates and adapts its ISCM-based roles and responsibilities to account for a changing cybersecurity landscape.
49. How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls?	• NIST SP 800-18 (Rev. 1) • NIST SP 800-37 (Rev. 2): Task S-5 • NIST SP 800-53 (Rev. 5): CA-2, CA-5, CA-6, CA-7, PL-2, and PM-10 • NIST SP 800-137: Section 2.2 • NIST IR 8011 • NIST IR 8397 • OMB A-130 • OMB M-14-03 • OMB M-19-03 • OMB M-22-09 • FY 2023 CIO FISMA Metrics: 7.1	Core Metric	The organization has not developed system level continuous monitoring strategies/policies that define its processes for performing ongoing security control assessments, granting system authorizations, including developing and maintaining system security plans, monitoring security controls for individual systems, and time-based triggers for ongoing authorization.	The organization has developed system level continuous monitoring strategies/policies that define its processes for performing ongoing security control assessments, granting system authorizations, including developing and maintaining system security plans, monitoring security controls for individual systems, and time-based triggers for ongoing authorization. The system level strategy/policies address the monitoring of those controls that are not addressed by the organizational level strategy, as well as how changes to the system are monitored and reported.	The organization consistently implements its system level continuous monitoring strategies and related processes, including performing ongoing security control assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring security controls to provide a view of the organizational security posture, as well as each system's contribution to said security posture. In conjunction with the overall ISCM strategy, all security control classes (management, operational, and technical) and types (common, hybrid, and system-specific) are assessed and monitored, and their status updated regularly (as defined in the agency's information security policy) in security plans.	The organization uses the results of security control assessments and monitoring to maintain ongoing authorizations of information systems, including the maintenance of system security plans. Organization authorization processes include automated analysis tools and manual expert analysis, as appropriate.	The organization's system level ISCM policies and strategies are fully integrated with its enterprise and supply chain risk management, configuration management, incident response, and business continuity programs. The organization can demonstrate that it is using its system level ISCM policies and strategy to reduce the cost and increase the efficiency of security and privacy programs.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
50. How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings?	• NIST SP 800-137	FY24	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 can 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.
51. 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 overall maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?							
51.1 Please provide an IG self-assessment rating (Effective/Not Effective) for the agency's *detect* function.							

RESPOND FUNCTION AREA

Table 15: Incident Response

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
52. To what extent does the organization use an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents?	• NIST SP 800-53 (Rev. 5): IR-8 • NIST SP 800-61 (Rev. 2): Section 2.3.2 • NIST CSF: RS.RP-1 • Presidential Policy Directive (PPD) 8 – National Preparedness • FY 2023 CIO FISMA Metrics: 10.1.1 • FY 2022 CIO FISMA Metrics: 10.6	FY24	The organization has not developed an incident response plan to provide a roadmap for implementing its incident response capability.	The organization has developed a tailored incident response plan that addresses: • Structure and organization of the incident response capability • High-level approach for how the incident response capability fits into the overall organization • Defines reportable incidents, including major incidents • Metrics for measuring the incident response capability • Resources and management support	The organization consistently implements its incident response plan. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident response plan and making updates as necessary.	The organization monitors and analyzes the qualitative and quantitative performance measures that have been defined in its incident response plan to monitor and maintain the effectiveness of its overall incident response capability. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization's incident response plan is fully integrated with risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. In addition, the organization make near real-time updates to its incident response plan based on changing risk environments and threat information. The organization participates in DHS's Cyber Storm national level exercise, as appropriate, or other exercises, to assess, cybersecurity preparedness, and examine incident response processes.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
53. To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization?	• NIST SP 800-53 (Rev. 5) IR-7 • NIST SP 800-61 (Rev. 2) • NIST SP 800-83 • NIST CSF: RS.CO-1 • OMB M-20-04 • US-CERT Federal Incident Notification Guidelines • Green Book: Principles 3, 4, and 5	FY24	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.	Individuals are performing the roles and responsibilities that have been defined across the organization.	Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement incident response activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.	The organization continuously evaluates and adapts its incident response-based roles and responsibilities to account for a changing cybersecurity landscape.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
54. How mature are the organization's processes for incident detection and analysis?	• NIST SP 800-53 (Rev. 5): IR-4, IR-5, and IR-6 • NIST SP 800-61 (Rev. 2) • NIST CSF: DE.AE-1 -5, PR.DS-6, RS.AN-1, RS.AN-4, and PR.DS-8 • OMB M-20-04 • OMB M-21-31 • OMB M-22-01 • OMB M-23-03 • CISA Cybersecurity Incident Response Playbooks • CIS Top 18 Security Controls: Control 17 • US-CERT Federal Incident Notification Guidelines • FY 2023 CIO FISMA Metrics: 3.1, 10.4, 10.5, and 10.6	Core Metric	The organization has not defined and communicated its policies, procedures, and processes for incident detection and analysis. In addition, 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 and communicated its policies, procedures, and processes for incident detection and analysis. In addition, 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 implements its policies, procedures, and processes for incident detection and analysis. In addition, the organization consistently uses 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. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident detection policies and procedures and making updates as necessary. In addition, the organization is meeting logging requirements at maturity EL1 (basic), in accordance with M-21-31.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident detection and analysis policies and procedures. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. The organization uses 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. In addition, the organization is meeting logging requirements at maturity EL2 (intermediate), in accordance with M-21-31.	The organization is making demonstrated progress towards implementing EL3's (advanced) requirements for its logging capabilities.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
55. How mature are the organization's processes for incident handling?	• NIST SP 800-53 (Rev. 5): IR-4 • NIST SP 800-61 (Rev. 2) • NIST IR 8374 • NIST CSF: RS.MI-1 and RS.MI-2 • OMB M-21-31 • OMB M-23-03 • CISA Cybersecurity Incident Response Playbooks • FY 2023 CIO FISMA Metrics: 10.4, 10.5, and 10.6	Core Metric	The organization has not defined its policies, procedures, and 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 defined its policies, procedures, and processes for incident handling to include containment strategies for each key 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 incident handling policies, procedures, containment strategies, and incident eradication processes. In addition, the organization consistently implements processes to remediate vulnerabilities that may have been exploited on the target system(s) and recovers system operations. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident handling policies and procedures and making updates as necessary.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident handling policies and procedures. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. The organization manages and measures the impact of successful incidents and can quickly mitigate related vulnerabilities on other systems so that they are not subject to exploitation of the same vulnerability.	The organization uses 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.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
56. 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 • NIST SP 800-53 (Rev. 5): IR-6 • NIST CSF: RS.CO-2 through RS.CO-5 • OMB M-20-04 • US-CERT Federal Incident Notification Guidelines • PPD-41 • DHS Cyber Incident Reporting Unified Message	FY24	The organization has not defined its policies, procedures, and processes to share incident response information with individuals with significant security responsibilities or its processes for reporting security incidents, including major 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 policies, procedures, and processes 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, including for major incidents, to US-CERT, law enforcement, the Congress 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. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident reporting policies and procedures and making updates as necessary.	Incident response metrics are used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization receives, retains, uses, and disseminates cyber threat indicators in accordance with the Cybersecurity Information Sharing Act of 2015.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
57. 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, including through contracts/agreements, as appropriate, for incident response support?	• NIST SP 800-53 (Rev. 5): IR-4 • NIST SP 800-86 • OMB M-20-04 • PPD-41 • NCPS Cloud Interface Reference Architecture	FY23	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 use 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 use DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving the organization's networks.	The organization consistently uses 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 contractual relationships in support of incident response processes (e.g., for forensic support), as needed. The organization has fully deployed DHS' Einstein 1 and 2 to screen all traffic entering and leaving its network through a TIC.	The organization uses Einstein 3 Accelerated, and/or other comparable tools or services, to detect and proactively block cyber-attacks or prevent potential compromises.	The organization is making progress in implementing information sharing and reporting patterns to provide telemetry information to CISA for its cloud-based environments not covered by Einstein 3 Accelerated.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
58. To what extent does the organization use 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 800-44 • NIST SP 800-61 (Rev. 2) • NIST SP 800-137 • OMB M-22-01 • OMB M-22-09	FY23	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 use 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 used 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 evaluates the effectiveness of its incident response technologies and makes adjustments to configurations and toolsets, as appropriate.	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.
59. 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 overall maturity level generated from the questions above and based on all testing performed, is the incident response program effective?							
59.1 Please provide an IG self-assessment rating (Effective/Not Effective) for the agency's *respond* function.							

RECOVER FUNCTION AREA

Table 16: Contingency Planning

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
60. To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined, communicated, and implemented across the organization, including appropriate delegations of authority?	• NIST SP 800-34 • NIST SP 800-53 (Rev. 5): CP-1, CP-2, and CP-3 • NIST SP 800-84 • FCD-1: Annex B	FY23	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. Further, the organization has defined its policies and procedures for providing contingency training consistent with roles and responsibilities.	Individuals are performing the roles and responsibilities that have been defined across the organization. The organization ensures that contingency training is provided consistent with roles and responsibilities to ensure that the appropriate content and level of detail is included.	Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement system contingency planning activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.	The organization incorporates simulated events into contingency training to facilitate effective response by stakeholders (internal and external) involved in information systems contingency planning and to measure the extent to which individuals are equipped to perform their roles and responsibilities.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
61. To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts?	• NIST SP 800-34 (Rev. 1): Section 3.2 • NIST SP 800-53 (Rev. 5): CP-2 and RA-9 • NIST IR 8179 • NIST IR 8286 • NIST IR 8286D • NIST CSF: ID.RA-4 • FIPS 199 • FCD-1 • FCD-2 • OMB M-19-03	Core Metric	The organization has not defined its policies, procedures, and processes for conducting organizational and system-level BIAs and for incorporating the results into strategy and plan development efforts.	The organization has defined its policies, procedures, and processes for conducting organizational and system-level BIAs and for incorporating the results into strategy and plan development efforts.	The organization consistently incorporates the results of organizational and system level BIAs into strategy and plan development efforts. 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 • 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.	The organization ensures that the results of organizational and system level BIAs are integrated with enterprise risk management processes, for consistently evaluating, recording, and monitoring the criticality and sensitivity of enterprise assets. As appropriate, the organization uses the results of its BIA in conjunction with its risk register to calculate potential losses and inform senior level decision making.	The organization integrates its BIA and asset management processes to improve risk identification, accurate exposure consideration (based on realistic calculations of harmful impacts), and effective risk response.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
62. To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans?	• NIST SP 800-34 • NIST SP 800-53 (Rev. 5) CP-2 • NIST CSF: PR.IP-9 • FY 2023 CIO FISMA Metrics: 10.1.2, 10.2, and 10.3 • OMB M-19-03	FY24	The organization has not defined its policies, procedures, and processes for information system contingency plan (ISCP) development and maintenance. In addition, 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.	The organization has defined its policies, procedure, and processes for information system contingency plan development, maintenance, and integration with other continuity areas. The policies, procedures, and processes for ISCP 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 can 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 organization coordinates the development of ISCP's with the contingency plans of external service providers.	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.
63. To what extent does the organization perform tests/exercises of its information system contingency planning processes?	• NIST SP 800-34 • NIST SP 800-53 (Rev. 5): CP-3 and CP-4 • NIST CSF: ID.SC-5 and PR.IP-10 • CIS Top 18 Security Controls: Control 11	Core Metric	The organization has not defined its policies, procedures, and processes for information system contingency plan testing/exercises. ISCP tests are performed in an ad-hoc, reactive manner.	Policies, procedures, and 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.	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 test system contingency plans more thoroughly and effectively. In addition, the organization coordinates plan testing with external stakeholders (e.g., ICT supply chain partners/providers), as appropriate.	Based on risk, the organization performs a full recovery and reconstitution of systems to a known state. In addition, the organization proactively employs [organization defined mechanisms] to disrupt or adversely affect the system or system component and test the effectiveness of contingency planning processes.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
64. To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate?	• NIST SP 800-34: Sections 3.4.1 through 3.4.3 • NIST SP 800-53 (Rev. 5): CP-6, CP-7, CP-8, CP-9, and CP-10 • NIST SP 800-209 • NIST CSF: PR.IP-4 • FCD-1 • FY 2023 CIO FISMA Metrics: 10.3.1 and 10.3.2 • NIST Security Measures for EO-Critical Software Use: SM 2.5	FY24	The organization has not defined its policies, procedures, 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. Information system backup and storage is performed in an ad-hoc, reactive manner.	The organization has defined its policies, procedures, processes, strategies, and technologies for information system backup and storage, including use of alternate storage and processing sites and RAID, as appropriate. The organization has considered alternative approaches when developing its backup and storage strategies, including cost, environment (e.g., cloud model deployed), maximum downtimes, recovery priorities, and integration with other contingency plans.	The organization consistently implements its policies, procedures, 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 that ensure the potential disruption of the organization's ability to initiate and sustain operations is minimized. In addition, the organization ensures that these sites and are not subject to the same risks as the primary site. Furthermore, the organization ensures that alternate processing and storage facilities are configured with information security safeguards equivalent to those of the primary site, including applicable ICT supply chain controls. Furthermore, backups of information at the user- and system-levels are consistently performed, and the confidentiality, integrity, and availability of this information is maintained.	The organization ensures that its information system backup and storage processes, including use of alternate storage and processing sties, and related supply chain controls, are assessed, as appropriate, as part of its continuous monitoring program. As part of its continuous monitoring processes, the organization demonstrates that its system backup and storage and alternate storage and processing sites are configured to facilitate recovery operations in accordance with recovery time and recover point objectives.	The organization takes appropriate steps to protect against infection or other compromise of its backup data. Further, on a near real-time basis, for sensitive data and EO-critical software, the organization maintains an up-to-date recovery catalog for each backup that records which anti-malware tool the backups have been scanned with. In addition, for sensitive data, the organization periodically scans a subset of past backups with current anti-malware tools to identify poisoned backups.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Question	Criteria	Core Metric or FY	Maturity Level				
			Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
65. 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?	• NIST SP 800-53 (Rev. 5): CP-2 and IR-4 • NIST CSF: RC.CO-3	FY23	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 use 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.	The organization ensures that information on the planning and performance of recovery activities for its ICT supply chain providers is integrated into its communication processes on a near real-time basis.
66. 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 overall maturity level generated from the questions above and based on all testing performed, is the contingency planning program effective?							
66.1 Please provide an IG self-assessment rating (Effective/Not Effective) for the agency's recover function.							

September 22, 2023

David P. Wheeler

RESPONSE TO REQUEST FOR COMMENTS – AUDIT 2023-17423 –
Federal Information Security Modernization Act

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

We would like to thank Sarah Huffman, Melissa Conforti, and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact Brett Atkins.

Tammy Wilson
Vice President and Chief Information and Digital Officer
Technology and Innovation

ASB:BAA
cc (Attachment): Response to Request
KC Carnes
Andrea Brackett
Melissa Crane
Joshua Linville
Tammy Bramlett
Faisal Bhatti
Melissa Livesey
Kevin Tarver
Gregory Jackson
Todd McCarter
John Thomas
Joshua Thomas
David Harrison
Dustin Pate
OIG File No. 2023-17423

Audit 2023-17423
Federal Information Security Modernization Act
Response to Request for Comments

ATTACHMENT A
Page 1 of 1

	Recommendation	Comments
1	We recommend the Vice President and Chief Information and Digital Officer, T&I: Implement a knowledge, skills, and abilities assessment to tailor cybersecurity awareness and specialized training, identify gaps in TVA's cybersecurity workforce, and subsequently address the identified gaps through training or talent acquisition.	Management agrees.
2	Update processes to ensure that the results of BIAs are consistently (a) integrated with the enterprise risk management process and (b) used in conjunction with the risk register to calculate potential overall risk and inform senior level decision-making.	Management agrees.
3	Update TVA's VDP to include all internet-accessible federal systems in the scope of the policy and create performance measures to gauge the effectiveness of its VDP and disclosure handling procedures.	Management agrees.
4	Perform annual test, training, and exercise activities of each business critical application as required by TVA policy to ensure (a) contingency training is provided consistently with the roles and responsibilities to identify and include the appropriate content and level of detail, and (b) resources are allocated in a risk-based manner and stakeholders are held accountable.	Management agrees.
5	Implement and communicate accurate, consistent, and reproducible metrics on the effectiveness of recovery activities to relevant stakeholders.	Management agrees.