Memorandum from the Office of the Inspector General

September 19, 2022

Jeremy P. Fisher

REQUEST FOR MANAGEMENT DECISION – AUDIT 2022-17370 – FEDERAL INFORMATION SECURITY MODERNIZATION ACT

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 audit objective was to determine the effectiveness of Tennessee Valley Authority's (TVA) ISP and practices as defined by the *Fiscal Year (FY) 2022 Core IG Metrics Implementation Analysis and Guidelines* (see Appendix B). Our audit scope was limited to answering the core IG metrics.

The FISMA methodology considers metrics at a level 4 (managed and measurable) or higher to be at an effective level of security. Based on our analysis of the core IG metrics and associated maturity models, we found 12 of the 20 core IG metrics were at a level 1 (ad-hoc), level 2 (defined), or level 3 (consistently implemented); therefore, TVA's ISP was not operating in an effective manner as defined by the *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*.

We made five recommendations to TVA management to improve the maturity of ineffective core IG metrics.

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

BACKGROUND

FISMA requires each agency's IG to conduct an annual independent evaluation to determine the effectiveness of the ISP and practices of its respective agency. As required by the Office of Management and Budget (OMB),[1] FISMA shifted to a continuous assessment process in FY 2022. As a result, OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) transitioned the IG metrics process to a multi-year cycle beginning in FY 2022. Specifically, a subset of the FY 2021 IG FISMA metrics[2] were selected as the 20 core IG metrics to be evaluated annually and the additional IG metrics will be evaluated on a two-year cycle.

[1] OMB Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*, December 6, 2021.

[2] *Fiscal Year 2021 Inspector General Federal Information Security Modernization Act Of 2014 Reporting Metrics Version 1.1*, May 12, 2021.

For FY 2022, IGs were required to test the 20 core IG metrics only. The *FY 2022 Core IG Metrics Implementation Analysis and Guidelines* (see Appendix B) were developed by OMB, the Department of Homeland Security (DHS), and CIGIE, in consultation with the Federal Chief Information Officer Council and other stakeholders. These 20 core IG metrics were chosen based on alignment with Executive Order 14028, *Improving the Nation's Cybersecurity*,[3] as well as recent OMB guidance to agencies in furtherance of the modernization of federal cybersecurity.

The results of our review were provided to OMB and DHS through the use of their online reporting tool on July 25, 2022.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our audit objective was to determine the effectiveness of TVA's ISP and practices as defined by the *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*. Our audit scope was limited to answering the 20 core IG metrics (defined in Appendix B); therefore, the results of this audit are based on assessing these 20 core IG metrics only. A complete discussion of our audit objective, scope, and methodology is included in Appendix A.

FINDINGS

The FISMA methodology considers metrics at a level 4 (managed and measurable) or higher to be at an effective level of security. Based on our analysis of the core IG metrics and associated maturity models, we found 12 of the 20 core IG metrics were at a level 1 (ad-hoc), level 2 (defined), or level 3 (consistently implemented); therefore, TVA's ISP was not operating in an effective manner as defined by the *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*. See Table 1 for metric ratings.

FY 2022 IG FISMA Metric Results	
Maturity Level	**Number of Metrics**
Level 1: *Ad-hoc*	3
Level 2: *Defined*	8
Level 3: *Consistently Implemented*	1
Level 4: *Managed and Measurable*	7
Level 5: *Optimized*	1

Table 1

Specifically for the 12 core IG metrics rated at a level 1, 2, or 3, we found:

- Five metrics had actions in progress to improve their maturity or had mitigating controls in place to reduce the risk.

[3] 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.

- Seven metrics had weaknesses that should be addressed by TVA management, including:
  - Information system inventory and system components.
  - Hardware asset management process.
  - Standard data elements for software assets.
  - Configuration management process.
  - Contingency plan testing.

The following provides a detailed discussion of our findings.

INFORMATION SYSTEM INVENTORY AND SYSTEM COMPONENTS

We found TVA has not defined policies, procedures, and processes for developing and maintaining a comprehensive and accurate inventory of TVA's information system and system interconnections. Without a comprehensive and accurate information system and system interconnections inventory, TVA cannot adequately (1) perform system control assessments that are used to grant system authorizations and (2) transition to ongoing control and system authorization through the implementation of its continuous monitoring policies and strategy, which are required in order for other core IG metrics to mature.

HARDWARE ASSET MANAGEMENT PROCESS

We found TVA has defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets. However, TVA does not utilize hardware asset standard data elements/taxonomy to inform which assets can or cannot be introduced into the network as part of the network authentication process. Without an accurate hardware asset inventory for network authentication, TVA cannot transition to ongoing monitoring of hardware assets inventory status, such as configurations, patching, etc., as part of TVA's information system continuous monitoring strategy.

STANDARD DATA ELEMENTS FOR SOFTWARE ASSETS

We found TVA 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 mobile applications. While we found TVA has a catalog for software services, employees may request items not in the catalog which creates a decentralized process that does not follow the standard data elements/taxonomy that are necessary for tracking and reporting. Without an accurate software asset and licenses inventory, TVA cannot inform what can or cannot be introduced to the network and transition to ongoing monitoring of software assets inventory status as part of TVA's information system continuous monitoring strategy.

CONFIGURATION MANAGEMENT PROCESS

We found TVA has defined policies and procedures for secure configurations, including documenting common secure configurations. However, TVA has not consistently

implemented secure configuration settings for all its information systems. Specifically, TVA has no tools or processes in place to maintain server configurations for one of its information systems and not maintained device configurations for another one of its information systems. A configuration management process provides a method to identify, monitor, and control information system configuration settings. This ensures common secure configuration settings are followed, which affects the security and privacy posture or functionality of the system.

CONTINGENCY PLAN TESTING

We found (1) TVA has defined policies, procedures and processes for information system contingency plan testing and (2) contingency plan exercises have been defined. TVA's Standard Program and Process 12.013, *Information Systems Contingency Planning*, states "business critical applications are reviewed annually." However, we found TVA has completed contingency plan testing on only one of the 16 business critical applications during the FISMA testing period. Therefore, TVA has not consistently implemented annual contingency plan testing and exercises. According to TVA personnel, this was due to staffing turnover. Contingency plan testing allows the opportunity to identify and address vulnerabilities to increase plan effectiveness and the organization's readiness to execute the plan. This is a repeat finding from the FY 2020 FISMA audit.[4]

RECOMMENDATIONS

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

1. Define policies, procedures, and processes for developing and maintaining a comprehensive and accurate inventory of its information system and system interconnections that can be used for system authorizations and monitor the inventory as part of TVA's information system continuous monitoring strategy.

2. Improve the hardware asset management processes to include standard data elements/taxonomy that are used to inform what assets can be or cannot be introduced into the network as part of network authentication process.

3. Define standard data elements/taxonomy for software assets that are used to (a) develop and maintain an up-to-date inventory of software assets and licenses, including mobile applications, and (b) inform what assets can or cannot be introduced to the network.

4. Ensure the configuration management process is consistently implemented for all information systems.

5. Ensure contingency plans are consistently tested as required by policy.

[4] Audit Report 2020-15709, *Federal Information Security Modernization Act*, December 21, 2020.

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

- - - - - -

This report is for your review and information. 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, please contact Melissa L. Conforti, Senior Auditor, at (865) 633-7383 or Sarah E. Huffman, Director, Information Technology Audits, 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
Andrea S. Brackett
Tammy C. Bramlett
Kenneth C. Carnes II
Sherri R. Collins
Melissa R. Crane
Buddy Eller
David B. Fountain
Jim R. Hopson
Gregory G. Jackson
Benjamin A. Jones
Melissa A. Livesey
Jeffrey J. Lyash
Jill M. Matthews
Todd E. McCarter
John M. Thomas III
Josh Thomas
Ben R. Wagner
OIG File No. 2022-17370

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 *Fiscal Year* (*FY) 2022 Core IG Metrics Implementation Analysis and Guidelines* (see Appendix B). Our audit scope was limited to answering the 20 core IG metrics (defined in Appendix B). Our fieldwork was completed between June 2022 and July 2022.

To accomplish our objective, we:

- Inquired with TVA Technology and Innovation (T&I) personnel and conducted walkthroughs as necessary to gain an understanding and clarification of the policies, processes, and current state.
- Reviewed documentation provided by T&I to corroborate our understanding and assess TVA's current state, including:
  - Relevant TVA agency-wide and business unit specific policies, procedures, and documents (such as Standard Programs and Processes and Work Instructions).
  - Configuration baselines.
- Reviewed previous Office of Inspector General audit reports on TVA's compliance with the (1) Federal Information Security Modernization Act of 2014 in 2020,[1] (2) Privacy Program,[2] and (3) Privileged Account Management[3] for relevant findings.
- Judgmentally selected five business critical applications based on auditor knowledge of TVA environment and judgment of critical and high-risk applications. For these applications, we reviewed the information system contingency plan and business impact analysis documentation for completeness and incorporation into strategy and plan development efforts. Since this was a judgmental sample, the results of the sample cannot be projected to the population.

---

1 Audit Report 2020-15709, *Federal Information Security Modernization Act*, December 21, 2020.

2 Audit Report 2021-15779, *TVA's Privacy Program*, September 20, 2021.

3 Audit Report 2021-15777, *Privileged Account Management*, September 22, 2021.

During the course of this audit, we determined the overall effectiveness of TVA's ISP by assessing the 20 core IG metrics (as detailed in Appendix B) on a maturity model spectrum. Table 1 details the five maturity model levels.

FY 2022 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

The maturity level was determined by answering the related core IG metrics and using a simple majority rule of the most frequent resulting maturity levels. The FISMA methodology considers metrics at a 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.

OMB Office of the Federal Chief Information Officer

FY22 Core IG Metrics Implementation Analysis and Guidelines

This document outlines the Office of Management and Budget's (OMB) guidance for implementing the requirements outlined in M-22-05, accompanying the Core Inspector General (IG) Metrics for FY22 provided in Appendix A. The guidance below and related metrics are based on coordinated discussions between (and the consensus opinion of) representatives from OMB, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), Federal Civilian Executive Branch (FCEB) Chief Information Security Officers (CISOs) and their staff, and the Intelligence Community (IC). Research, interviews and IG survey data provided quantitative and qualitative information to formulate these guidelines.

Overview and Background

The Federal Information Security Modernization Act of 2014 (FISMA) requires each agency IG, or an independent external auditor, to conduct an annual independent evaluation to determine the effectiveness of the information security program and practices of its respective agency. Accordingly, the fiscal year (FY) 2022 IG FISMA Reporting Metrics focus on key areas to ensure successful independent evaluations of agencies' information security programs.

The FY 2022 Core IG Metrics represent a continuation of work begun in FY 2016, when the IG metrics were aligned to 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. The Cybersecurity Framework provides agencies with a common structure for assessing cybersecurity capabilities and associated risks implemented across the enterprise and enables the IGs to have a framework for the communication of capabilities and the maturity of controls that support them.

The FY22 Core IG Metrics were chosen based on alignment with Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," as well as recent OMB guidance to agencies in furtherance of the modernization of federal cybersecurity, including:

- Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (M-22-09) – OMB and CISA solicited public feedback on strategic and technical guidance documents meant to move the U.S. government towards a zero trust architecture. The goal of OMB's Federal Zero Trust Strategy is to accelerate agencies towards a baseline of early zero trust maturity.

- Multifactor Authentication (MFA) and Encryption (EO 14028) – Per the EO, agencies were required to fully adopt MFA and encryption for data at rest and in transit by November 8, 2021. For agencies that were unable to meet these requirements within 180 days of the date of the order, the agency head was directed to provide a written rationale to the Secretary of Homeland Security through the Director of CISA, the Director of OMB, and the APNSA.

- Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents (M-21-31) – This memorandum provides specific requirements for log management. It includes a maturation model, prioritizing the most critical log types and requirements, to build a roadmap to success.

- Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response (M-22-01) – On October 8, 2021, this

memorandum was issued for agencies to focus on improving early detection capabilities, creating "enterprise-level visibility" across components and sub-agencies, and requires agencies to deploy an EDR solution.

- Software Supply Chain Security & Critical Software – Section 4 of EO 14028 tasks OMB, NIST, and other federal entities with developing new guidelines and frameworks to improve the security and integrity of the technology supply chain. In collaboration with industry and other partners, this effort is providing frameworks and guidelines on how to assess and build secure technology, including open source software.

Additionally, OMB Memorandum M-22-05 adjusts the timeline for the Inspectors General evaluation of agency effectiveness to align the results of the evaluation with the budget submission cycle. Historically, the evaluation of agency effectiveness by Inspectors General finished in October. This timing limited agency leadership's ability to request resources in the next Budget Year submissions to provide for remediations. The expectation is this change will reduce the time between issue identification, resource request and allocation. Outlined below is implementation guidance to support IGs as they manage this adjustment.

Determining Effectiveness with Core Metrics

IGs are required to assess the effectiveness of information security programs on a maturity model spectrum. Aligning with the Carnegie Mellon Cybersecurity Maturity Model Certification (CMMI), the foundational levels require agencies to develop sound policies and procedures, while advanced levels capture the extent to which agencies institutionalize those policies and procedures.

Representatives from OMB, FCEB CISO teams, CIGIE, and IC Community agreed that these 20 Core IG Metrics should provide sufficient data to determine the effectiveness of an Agency's information security program with a high level of confidence.

As with previous guidance on the use of the five-level maturity model, a Level 4, *Managed and Measurable*, information security program is still considered operating at an effective level of security. While the determination of effectiveness can be established based on the results of the IG metrics, IGs should continue to consider their own assessment of the unique missions, resources, and challenges faced by their agency when assessing the maturity of information security programs.

To that end, IGs are encouraged to leverage supplemental 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 this evaluation period (or past periods, as applicable). OMB requests that IGs consider results that deterministically demonstrate outcomes of security processes through ground truth testing[1] as supportive supplemental information when evaluating for effectiveness. Finally, consideration of agency mission, resources, and challenges should also be considered in the assessment, and be documented in the agency's assessment of risk as discussed in OMB Circular A-123, the U.S. Government Accountability Office's (GAO) Green Book, and NIST SP 800-37/800-39. Collectively, this data can provide IGs alternative methods to determine agencies' overall effectiveness ratings when their offices find contextual data to support an adjustment.

[1] Methods that empirically validate security and find weaknesses, such as manual and automated penetration testing and red team exercises. (Source: M-22-05 FISMA Guidance)

Execution of the FY22 IG Evaluation

OMB is requesting Agency IG teams submit Core IG Metrics data from agency evaluations via Cyberscope **no later than July 30, 2022**. Understanding the unique challenges of this transition year, qualitative data and other supplemental reports can be submitted before the end of FY22.

We understand that this transition may impact both existing resources and resource planning. IG teams that utilize contract resources should prioritize their assessment for submission on July 30, 2022. For the remaining period of performance, it is recommended that resources focus on contract modifications for FY23, followed by remediation efforts and closeout activities (prioritizing areas covered by Core Metrics).

IGs should utilize Cyberscope to submit the results of the Core IG Metrics evaluation. Cyberscope will be updated to accommodate the submission of the results, and will support the data entry for Core Metrics in July. Additionally, Cyberscope will provide supplementary fields to allow the IG to provide additional comments to the Core Metrics submission. IGs may use these fields to provide additional data supporting the Core Metrics evaluation results, and will ultimately provide their determination of effectiveness within the platform.

Extension requests can be submitted to the OFCIO Mailbox (ofcio@omb.eop.gov). Extension requests will be evaluated based on unique requirements presented by the agency IG.

Core IG Metrics Working Group

A working group will be chartered by June 30, 2022 to support the future of the Core IG Metrics process. The working group will be co-led by designees identified by OMB and CIGIE respectively. Working group membership will be comprised of representatives from CIGIE, FCEB, OMB, the IC, and others deemed appropriate by OMB and CIGIE. The group will focus on evaluating the Core and supplemental metrics, providing recommendations to the IG Community that align and harmonize evaluation practices, improve reporting processes, and reduce burden where practicable and mutually beneficial. By establishing this working group, we hope to ensure that evolving cybersecurity needs and practices are reflected in future metrics. This includes evaluation of the effectiveness rating methodology, and areas of potential enhancement.[2] Additional details will be shared with the IG Community about the working group proposal as it is developed.

Summary

OMB and the IG have a unique, parallel relationship in providing oversight of agencies' cybersecurity practices—ultimately improving the efficacy of our government services. It is our strong belief that building a foundation for greater information sharing and common evaluative toolsets among our offices will have exponential benefits.

Determining effectiveness is a complex activity that involves both common data points paired with environment-specific context. Focusing on these Core Metrics, IGs will be able to coalesce the most important data points and focus on outcomes that best posture agencies for successful security programs. IG-led supplemental data and analysis helps stakeholders obtain an essential perspective on the landscape

[2] This action aligns with Recommendation 2 in GAO-22-104364, "OMB Should Update Inspector General Reporting Guidance to Increase Rating Consistency and Precision."

of security and provide context to these core metrics. These guidelines for the FY22 Core IG Metrics will help facilitate the transition to the vision outlined in M-22-05.

Appendix A: Core IG Metrics

The table below shows the Core IG metrics for use in the FY22 IG evaluation period. These metrics were selected from the FY 21 IG metrics for their applicability to critical efforts emanating from EO 14028 and M-22-05.

Question	Metric	Mapping
1	**FY22 Core Metric:** 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 800-53, Rev. 5: CA-3 and PM-5; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2022 CIO FISMA Metrics: 1.1-1.1.5, 1.3; OMB A-130, NIST SP 800-37, Rev. 2: Task P-18; NIST 800-207, Section 7.3; EO 14028, Section 3; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B and D (5); CISA Cybersecurity & Incident Response Playbooks
2	**FY22 Core Metric:** 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 800-53, Rev. 5: CA-7 and CM-8; NIST SP 800-137; NIST IR 8011; NIST 800-207, 7.3.2; Federal Enterprise Architecture (FEA) Framework, v2; FY 2022 CIO FISMA Metrics: 1.2-1.2.3; CSF: ID.AM-1, ID.AM-5; NIST SP 800-37, Rev. 2: Task P-10 and P-16; NIST 800-207, Section 7.3; EO 14028, Section 3; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8: Control 1
3	**FY22 Core Metric:** To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting?	NIST SP 800-53, Rev. 5: CA-7, CM-8, CM-10, and CM-11; NIST SP 800-137; NIST IR 8011; FEA Framework, v2; FY 2022 CIO FISMA Metrics: 1.3 and 4.0; OMB M-21-30; EO 14028, Section 4; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B; CSF: ID.AM-2; NIST SP 800-37, Rev. 2: Task P-10 and P-16; NIST 800-207, Section 7.3; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8: Control 2
5	**FY22 Core Metric:** 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 800-39; NIST SP 800-53, Rev. 5: RA-3 and PM-9; NIST IR 8286; CSF: ID RM-1 – ID.RM-3; OMB A-123; OMB M-16-17; OMB M-17-25; NIST SP 800-37 (Rev. 2): Tasks P-2, P-3, P-14, R-2, and R-3
10	**FY22 Core Metric:** To what extent does the organization utilize 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; OMB A-123; NIST IR 8286; CISA Zero Trust Maturity Model, Pillars 2-4, NIST 800-207, Tenets 5 and 7; OMB M-22-09, Federal Zero Trust Strategy, Security Orchestration, Automation, and Response
14	**FY22 Core Metric:** 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 ()?	The Federal Acquisition Supply Chain Security Act of 2018, NIST SP 800-53, Rev. 5: SA-4, SR-3, SR-5 and SR-6 (as appropriate); NIST SP 800-152; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4, NIST IR 8276, NIST 800-218, Task PO.1.3; FY 2022 CIO FISMA Metrics: 7.4.2; CIS Top 18 Security Controls v.8: Control 15

20	**FY22 Core Metric:** To what extent does the organization utilize settings/common secure configurations for its information systems?	NIST SP 800-53, Rev. 5: CM-6, CM-7, and RA-5; NIST SP 800-70, Rev. 4; FY 2022 CIO FISMA Metrics, Section 7, Ground Truth Testing; EO 14028, Section 4, 6, and 7; OMB M-22-09, Federal Zero Trust Strategy, Section D; OMB M-22-05; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8, Controls 4 and 7; CSF: ID.RA-1 and DE.CM-8
21	**FY22 Core Metric:** To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities?	EO 14028, Sections 3 and 4; NIST SP 800-53, Rev. 5: CM-3, RA-5, SI-2, and SI-3; NIST SP 800-40, Rev. 3; NIST 800-207, section 2.1; CIS Top 18 Security Controls v.8, Controls 4 and 7; FY 2022 CIO FISMA Metrics: Section 8; CSF: ID.RA-1; DHS Binding Operational Directives (BOD) 18-02, 19-02, and 22-01; OMB M-22-09, Federal Zero Trust Strategy, Section D; CISA Cybersecurity Incident and Vulnerability Response Playbooks
30	**FY22 Core Metric:** To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for non-privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access?	EO 14028, Section 3; HSPD-12; NIST SP 800-53, Rev. 5: AC-17, IA-2, IA-5, IA-8, and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63, 800-157; FY 2022 CIO FISMA Metrics: Section 2; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section A (2); CSF: PR.AC-1 and 6; OMB M-19-17, NIST SP 800-157; NIST 800-207 Tenet 6; CIS Top 18 Security Controls v.8: Control 6
31	**FY22 Core Metric:** To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access?	EO 14028, Section 3; HSPD-12; NIST SP 800-53, Rev. 5: AC-17 and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63 and 800-157; OMB M-19-17; FY 2022 CIO FISMA Metrics: Section 2; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section A (2); CSF: PR.AC-1 and 6; DHS ED 19-01; NIST 800-207 Tenet 6; CIS Top 18 Security Controls v.8: Control 6
32	**FY22 Core Metric:**: 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?	EO 14028, Section 8; FY 2022 CIO FISMA Metrics: 3.1; OMB M-21-31; OMB M-19-17; 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; DHS ED 19-01; CSF: PR.AC-4; CIS Top 18 Security Controls v.8: Controls 5, 6, and 8
36	**FY22 Core Metric:** To what extent has the organization implemented the encryption of data rest, in transit, limitation of transference of data by removable media, and sanitization of digital media prior to disposal or reuse to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle?	EO 14028, Section 3(d); OMB M-22-09, Federal Zero Trust Strategy; NIST 800-207; NIST SP 800-53, Rev. 5; SC-8, SC-28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2022 CIO FISMA Metrics: 2.1, 2.2, 2.12, 2.13; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6; CIS Top 18 Security Controls v. 8: Control 3
37	**FY22 Core Metric:**: To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses?	FY 2022 CIO FISMA Metrics, 5.1; NIST SP 800-53, Rev. 5: SI-3, SI-7, SI-4, SC-7, and SC-18; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5, OMB M-21-07; CIS Top 18 Security Controls v.8: Controls 9 and 10
42	**FY22 Core Metric:** To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover?	FY 2022 CIO FISMA Metrics, Section 6; NIST SP 800-53, Rev. 5: AT-2, AT-3, and PM-13; NIST SP 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181; and CIS Top 18 Security Controls v.8: Control 14
47	**FY22 Core Metric:**: To what extent does the organization utilize information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier?	NIST SP 800-53, Rev. 5: CA-7, PM-6, PM-14, and PM-31; NIST SP 800-37 (Rev. 2) Task P-7; NIST SP 800-137: Sections 3.1 and 3.6; CIS Top 18 Security Controls v.8: Control 13

49	**FY22 Core Metric:** 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?	OMB A-130; NIST SP 800-137: Section 2.2; NIST SP 800-53, Rev. 5: CA-2, CA-5, CA-6, CA-7, PL-2, and PM-10; NIST Supplemental Guidance on Ongoing Authorization; NIST SP 800-37 (Rev. 2) Task S-5; NIST SP 800-18, Rev. 1, NIST IR 8011; OMB M-14-03; OMB M-19-03
54	**FY22 Core Metric:**: How mature are the organization's processes for incident detection and analysis?	EO 14028, Section 6; OMB M-22-05, Section I; CISA Cybersecurity Incident and Vulnerability Response Playbooks; FY 2022 CIO FISMA Metrics: 10.6; NIST 800-53, Rev. 5: IR-4, IR-5, and IR-6; NIST SP 800-61 Rev. 2; OMB M-20-04; CSF: DE.AE-1, DE.AE-2 -5, PR.DS-6, RS.AN-1 and 4, and PR.DS-8; and CIS Top 18 Security Controls v.8: Control 17
55	**FY22 Core Metric:**: How mature are the organization's processes for incident handling?	EO 14028, Section 6; OMB M-22-05, Section I; CISA Cybersecurity Incident and Vulnerability Response Playbooks; FY 2022 CIO FISMA Metrics: 10.6; NIST 800-53, Rev. 5: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 2
61	**FY22 Core Metric:** To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts?	FY 2022 CIO FISMA Metrics: 10.1.4; NIST SP 800-53, Rev. 5: CP-2, and RA-9; NIST SP 800-34, Rev. 1, 3.2; NIST IR 8286; FIPS 199; FCD-1; OMB M-19-03; CSF:ID.RA-4
63	**FY22 Core Metric:** To what extent does the organization perform tests/exercises of its information system contingency planning processes?	FY 2022 CIO FISMA Metrics: 10.1; NIST SP 800-34; NIST SP 800-53, Rev. 5: CP-3 and CP-4; CSF: ID.SC-5 and CSF: PR.IP-10; CIS Top 18 Security Controls v.8: Control 11

September 13, 2022

David P. Wheeler, WT 2C-K

RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2022-17370 – FEDERAL INFORMATION SECURITY MODERNIZATION ACT

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

We would like to thank 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.

Jeremy Fisher
Vice President and Chief Information Officer
Technology and Innovation
SP 3A-C

ASB:BAA
cc (Attachment): Response to Request
Andrea Brackett, WT 5D-K
Faisal Bhatti
Kenneth C. Carnes II
Sherri R. Collins
Melissa R. Crane, SP 3A-C
David B. Fountain
Melissa A. Livesey WT 5B-K
Gregory Jackson
Tammy Bramlett, SP 2A-C
Ben Jones, SP 3L-C
Todd McCarter, MP 2C-C
John Thomas, MR 6D-C
Joshua Thomas
OIG File No. 2022-17370

Audit 2022-17370
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: Define policies, procedures, and processes for developing and maintaining a comprehensive and accurate inventory of its information system and system interconnections that can be used for system authorization and monitor the inventory as part of TVA's information system continuous monitoring strategy.	Management agrees.
2	We recommend the Vice President and Chief Information and Digital Officer, T&I: Improve the hardware asset management processes to include standard data elements/taxonomy that are used to inform what assets can be or cannot be introduced into the network as part of network authentication process.	Management agrees.
3	We recommend the Vice President and Chief Information and Digital Officer, T&I: Define standard data elements/taxonomy for software assets that are used to (a) develop and maintain an up-to-date inventory of software assets and licenses, including mobile applications, and (b) inform what assets can or cannot be introduced to the network.	Management agrees.
4	We recommend the Vice President and Chief Information and Digital Officer, T&I: Ensure the configuration management process is consistently implemented for all information systems.	Management agrees.

Audit 2022-17370
Federal Information Security Modernization Act
Response to Request for Comments

ATTACHMENT A
Page 2 of 1

Recommendation		Comments
5	We recommend the Vice President and Chief Information and Digital Officer, T&I: Ensure contingency plans are consistently tested as required by policy.	Management agrees.