Evaluation Report

OIG-CA-23-036

CYBERSECURITY/INFORMATION TECHNOLOGY

The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2023

July 27, 2023

Office of Inspector General
Department of the Treasury

This Page Intentionally Left Blank

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

July 27, 2023

Mary Walker, Executive Director
Gulf Coast Ecosystem Restoration Council
500 Poydras Street
Suite 1117
New Orleans, LA 70130

Re: Evaluation Report – The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2023 (OIG-CA-23-036)

Dear Ms. Walker:

We hereby transmit the attached report, *The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2023*, dated July 27, 2023. The Federal Information Security Modernization Act of 2014 (FISMA) requires that Federal agencies have an annual independent evaluation performed of their information security programs and practices to determine the effectiveness of such programs and practices, and to report the results to the Office of Management and Budget (OMB). OMB delegated its responsibility to the Department of Homeland Security for the collection of annual FISMA responses. FISMA also requires that the agency Inspector General (IG) or an independent external auditor perform the annual evaluation as determined by the IG.

To meet our FISMA requirements, we contracted with RMA Associates, LLC (RMA), an independent certified public accounting firm, to perform this year's annual FISMA evaluation of the Gulf Coast Ecosystem Restoration Council's (Council) security program and practices for the period April 1, 2022 through March 31, 2023. RMA conducted its evaluation in accordance with *Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation*. In connection with our contract with RMA, we reviewed its report and related documentation and inquired of its representatives. Our review, as differentiated from an evaluation performed in accordance with inspection and evaluation standards, was not intended to enable us to conclude on the effectiveness of the Council's information security program and practices or its compliance with FISMA. RMA is responsible for its report and the conclusions expressed therein.

In brief, RMA reported that consistent with applicable FISMA requirements, OMB policy and guidance, and the National Institute of Standards and Technology standards and guidelines, the Council's information security program and practices were established and have been maintained for the five Cybersecurity Function areas and nine FISMA Metric Domains. RMA found that the Council's information security program and practices were effective for the period April 1, 2022 through March 31, 2023.

Appendix I of the attached RMA report includes the *Fiscal Year 2023 – 2024 IG FISMA Reporting Metrics*.

If you have any questions or require further information, you may contact me at (202) 927 0361.

Sincerely,

/s/

Larissa Klimpel
Director, Cyber/Information Technology Audits

Attachment

RMA | Associates
Auditors. Consultants. Advisors.

The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2023

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

July 27, 2023

Richard K. Delmar
Acting Inspector General
Department of the Treasury
1500 Pennsylvania Avenue NW
Room 4436
Washington, DC 20220

Re: The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2023

Dear Mr. Delmar:

RMA Associates, LLC is pleased to submit the Gulf Coast Ecosystem Restoration Council (Council) Federal Information Security Modernization Act of 2014 (FISMA) Evaluation Report for fiscal year (FY) 2023. We conducted the evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* issued in December 2020. The objective of this evaluation was to evaluate the effectiveness of the Council's information security program and practices for the period April 1, 2022, through March 31, 2023.

For FY 2023, the Office of Management and Budget (OMB) identified 20 core and 20 supplemental Inspector General (IG) FISMA Reporting Metrics to evaluate. These metrics are outlined in OMB's *FY 2023 – 2024 IG FISMA Reporting Metrics* Version 1.1, dated February 10, 2023. The IG was required to assess the maturity levels of those metrics. As part of our evaluation, we conducted an assessment of FY 2023 core and supplemental IG Metrics on behalf of the Department of the Treasury's Office of Inspector General. The results of this assessment are presented in Appendix I: FY 2023 – 2024 IG FISMA Reporting Metrics.

In summary, we found the Council's information security program and practices were effective for the period April 1, 2022, through March 31, 2023.

We very much appreciate the opportunity to serve you and will be pleased to discuss any questions you may have.

Sincerely,

RMA Associates

RMA Associates, LLC
Arlington, VA

Table of Contents

Abbreviations

AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
ARC	Administrative Resource Center
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BOD	Binding Operational Directive
BYOD	Bring Your Own Device
CA	Assessment, Authorization, and Monitoring
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CM	Configuration Management
COOP	Continuity of Operations Plan
Council	Gulf Coast Ecosystem Restoration Council
CP	Contingency Planning
CSF	Cybersecurity Framework
DOA	Delegation Option Authority
DE.AE	Detect – Anomalies and Events
DE.CM	Detect – Security Continuous Monitoring
DHS	Department of Homeland Security
DNS	Domain Name System
ED	Emergency Directive
EL	Event Logging
EO	Executive Order
EPA	United States Environmental Protection Agency
ERM	Enterprise Risk Management
FCD	Federal Continuity Directive
FEA	Federal Enterprise Architecture
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAO	Government Accountability Office
GFE	Government Furnished Equipment
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
H.R	House of Representatives
IA	Identification and Authentication
ICT	Information and Communications Technology

ID.AM	Identify – Asset Management
ID.GV	Identify – Governance
ID.RA	Identify – Risk Assessment
ID.RM	Identify – Risk Management Strategy
ID.SC	Identify – Supply Chain Risk Management
IG	Inspector General
IT	Information Technology
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Planning
IR	Incident Response
IT	Information Technology
NIST	National Institute of Standards and Technology
NIST IR	National Institute of Standards and Technology Interagency or Internal Report
MP	Media Protection
NOAA	National Oceanic and Atmospheric Administration
OIG	Office of Inspector General
OMB	Office of Management and Budget
OS	Operating System
OSN	Office Support Network
PE	Physical and Environment Protection
PII	Personally Identifiable Information
PIV	Personal Identity Verification
P.L.	Public Law
PL	Planning
PM	Program Management
POA&M	Plan of Action and Milestones
PPD	Presidential Policy Directive
PR.AC	Protect – Identity Management and Access Control
PR.DS	Protect – Data Security
PR.IP	Protect – Information Protection Processes and Procedures
PR.PT	Protect – Protective Technology
PS	Personnel Security
RA	Risk Assessment
RC.CO	Recover – Communications
RESTORE Act	Resources and Ecosystems Sustainability, Tourist Opportunities, and Revived Economies of the Gulf Coast States Act of 2012
RMA	RMA Associates, LLC
ROB	Rules of Behavior
RS.AN	Respond – Analysis
RS.MI	Respond – Mitigation
SA	System and Service Acquisition
SAOP	Senior Agency Official for Privacy
SCRM	Supply Chain Risk Management
SCAP	Security Content Automation Protocol

SI	System and Information Integrity
SC	System and Communication Protection
SOC	Security Operations Center
SP	Special Publication
SR	Supply Chain Risk Management
TIC	Trusted Internet Connection
Treasury	Department of the Treasury
USC	U.S. Code
VDP	Vulnerability Disclosure Policy
VPN	Virtual Private Network

Introduction

This report presents the results of our independent evaluation of the Gulf Coast Ecosystem Restoration Council's (Council) information security program and practices. The *Federal Information Security Modernization Act of 2014* (FISMA)[1] requires Federal agencies to have an annual independent evaluation of their information security program and practices to determine the effectiveness of such programs and practices and to report the evaluation results to the Office of Management and Budget (OMB). OMB delegated its responsibility to the Department of Homeland Security (DHS) for the collection of annual FISMA responses.

The Department of the Treasury's (Treasury) Office of Inspector General (OIG) engaged RMA Associates, LLC (RMA) to conduct the Fiscal Year (FY) 2023 FISMA evaluation of the Council's information security program and practices. The objective of this evaluation was to evaluate the effectiveness of the Council's information security program and practices for the period April 1, 2022, through March 31, 2023.

As part of our evaluation, we responded to the FY 2023 20 core and 20 supplemental metrics from OMB's *FY 2023-2024 Inspector General (IG) FISMA Reporting Metrics,* Version 1.1, dated February 10, 2023.[2] For FY 2023, 20 supplemental metrics were evaluated in addition to the 20 core metrics that were evaluated in FY 2022. These metrics 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. 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. This evaluation was performed in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) *Quality Standards for Inspection and Evaluation*, issued in December 2020.

Summary Evaluation Results

We concluded that consistent with FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, the Council's information security program and practices were established and maintained for the five Cybersecurity Function areas[3] and nine FISMA Metric Domains.[4] The overall maturity of the Council's information security program was determined to be Level 3, Consistently Implemented, as described in this report. That said, we found the Council's information security program and practices were effective for the period April 1, 2022, through March 31, 2023. Although within the context of the maturity model, Level 4, Managed and

[1] Public Law (P.L.) 113-283, Federal Information Security Modernization Act of 2014 (Dec. 18, 2014).

[2] OMB, DHS, and CIGIE developed the IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officers Council.

[3]The five Cybersecurity Functions as defined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* are: (1) identify, (2) protect, (3) detect, (4) respond, and (5) recover.

[4] As described in the FISMA Reporting Metrics, the nine FISMA Metric Domains, which are aligned with the five Cybersecurity Functions are: (1) risk management, (2) supply chain risk management, (3) configuration management, (4) identity and access management, (5) data protection and privacy, (6) security training, (7) information security continuous monitoring, (8) incident response, and (9) contingency planning.

Measurable, represents an effective level of security; based on the Council's overall implementation of security controls and considering the unique mission, resources, and challenges of the Council, we found the Council's information security program and practices were appropriate and effective.

We provided the Council with a draft of this report for comment. In a written response, management agreed with the results of our evaluation. See *Management Response* in Appendix II for the Council's response in its entirety.

Background

Gulf Coast Ecosystem Restoration Council

Spurred by the Deepwater Horizon oil spill, the Resources and Ecosystems Sustainability, Tourist Opportunities, and Revived Economies of the Gulf Coast States Act (RESTORE Act) was signed into law by President Obama on July 6, 2012. The RESTORE Act calls for a regional approach to restoring the long-term health of the valuable natural ecosystem and economy of the Gulf Coast region. The RESTORE Act dedicates 80 percent of civil and administrative penalties paid under the Clean Water Act, after the date of enactment, by responsible parties in connection with the Deepwater Horizon oil spill to the Gulf Coast Restoration Trust Fund for ecosystem restoration, economic recovery, and tourism promotion in the Gulf Coast region.

In addition to creating the Trust Fund, the RESTORE Act established the Council. The Council is comprised of the following Federal agencies: the U.S Departments of Agriculture, the Army, Commerce, Homeland Security, the Interior, and the U.S Environmental Protection Agency (EPA). Additionally, the Council includes the Governors of the States of Alabama, Florida, Louisiana, Mississippi, and Texas, as well as the EPA Administrator and Secretaries or designees of the other Agencies.

The Council's information system infrastructure consists of an Office Support Network (OSN) and eight system service providers. OSN is technically not a computer network as it includes no network servers. OSN is a stand-alone group of laptops connected to a leased wireless access point that provides a leased virtual private network connection to the Trusted Internet Connection portal.

Federal Information Security Modernization Act of 2014

On December 18, 2014, the President signed FISMA, which amended *FISMA 2002* and provided several modifications that modernized Federal security practices to address evolving security concerns. These changes resulted in strengthening the use of continuous monitoring in systems, increasing focus on the agencies' compliance, and producing reports that focused on issues caused by security incidents.

FISMA requires Federal agencies to have an annual, independent assessment performed of their information security programs and practices to determine the effectiveness of such programs and practices and report the assessment's results to OMB. In addition to the annual review and reporting requirements, FISMA included new provisions that further strengthened the federal government's data and information systems security, such as requiring the development of minimum control standards for agencies' systems.

FISMA extends to OMB oversight authority of agency security policies and practices and provides authority for implementing agency policies and practices for information systems to the DHS.[5]

FISMA requires the Secretary of DHS to develop and oversee the implementation of operational directives requiring agencies to implement OMB's standards and guidelines for safeguarding Federal information and systems from a known or reasonably suspected information security threat, vulnerability, or risk. It authorizes the Director of OMB to revise or repeal operational directives not in accordance with the Director's policies.[6]

FISMA "directs the Secretary to consult with and consider guidance developed by the National Institute of Standards and Technology (NIST) to ensure operational directives do not conflict with NIST information security standards."[7]

Additionally, FISMA directs Federal agencies to submit an annual report regarding major incidents to OMB, DHS, Congress, and the Comptroller General of the Government Accountability Office (GAO). Reports are required to include: (1) threats and threat factors, vulnerabilities, and impacts; (2) risk assessments of affected systems before and the status of compliance of the systems at the time of major incidents; (3) detection, response, and remediation actions; (4) the total number of incidents; and (5) a description of the number of individuals affected by, and the information exposed by, major incidents involving a breach of personally identifiable information.[8]

Further, FISMA requires OMB to ensure the development of guidance for evaluating the effectiveness of information security programs and practices.[9] As part of the NIST's statutory role in providing technical guidance to Federal agencies, NIST works with agencies in developing information security standards and guidelines. NIST developed an integrated Risk Management Framework that effectively brings together all the FISMA-related security standards and guidance to promote the development of comprehensive and balanced information security programs for all Federal agencies.

FISMA requires the head of each agency to be responsible for:

- Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;
- Complying with the requirements of NIST's related policies, procedures, and standards;
- Ensuring information security management processes are integrated with agency

[5] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 2014). https://www.congress.gov/bill/113th-congress/senate-bill/2251.

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] Ibid.

strategic, operational, and budgetary planning processes; and

- Ensuring senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including assessing risk, determining the levels of information security, implementing policies to reduce risks cost-effectively, and periodically testing and evaluating security controls.

FISMA requires the IG to conduct an annual independent assessment to determine the effectiveness of the information security program and practices of its respective agency. These assessments (a) test the effectiveness of information security policies, procedures, and practices of a subset of agency information systems and (b) assess the effectiveness of an agency's information security policies, procedures, and practices.[10]

FY 2023 Core and Supplemental IG Metrics

OMB's *FY 2023 – 2024 IG FISMA Reporting Metrics* Version 1.1, dated February 10, 2023 specified the FY 2023 20 Core and 20 Supplemental IG Metrics (refer to Appendix I). It directed IGs to report the assessed maturity levels of these metrics in CyberScope no later than July 31, 2023. The FY 2023 FISMA IG Metrics were aligned with the five Cybersecurity Framework security function areas (key performance areas) as follows:

- Identify, which includes questions pertaining to Risk Management and Supply Chain Risk Management (SCRM);
- Protect, which includes questions pertaining to Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training;
- Detect, which includes questions pertaining to Information Security Continuous Monitoring (ISCM);
- Respond, which includes questions pertaining to Incident Response; and
- Recover, which includes questions pertaining to Contingency Planning.

We evaluated the effectiveness of the Council's information security programs and practices on a maturity model spectrum, in which the foundation levels ensure the development of sound policies and procedures. The FY 2023 – 2024 IG Reporting Metrics classify information security programs and practices into five maturity model levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized (**Table 1**). Within the context of the maturity model, Level 4, Managed and Measurable, represents an effective level of security. However, for FY 2023, 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.

[10] NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (December 2020).

Table 1: IG Evaluation Maturity Levels

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

The scope of our evaluation was conducted for the period between April 1, 2022, and March 31, 2023. It consisted of testing the 20 Core and 20 Supplemental Metrics as shown in Appendix I, which reflects the results of our assessment of the Council's information security program and practices.

Evaluation Results

In previous years, IGs were directed to use 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. In FY 2023, a calculated average scoring model was used, where core and supplemental metrics were 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 was Level 3 (*consistently implemented)* (i.e., 3.0) and the computed Core metric maturity of the remaining three function areas was Level 4 (*managed and measurable*) (i.e., 4.0), the information security program rating would average a 3.60 (3+3+4+4+4)/5).

Core and Supplemental metrics were averaged independently to determine a domain's maturity calculation and provide data points for the assessed program and function effectiveness. An overall program calculation is shown in **Table 2**. The Council's FY 2023 corresponding maturity levels for the five function areas and the overall level are presented in **Table 3**.

Table 2: Overall Calculated Averages Maturity Calculation in FY 2023

Function	Core Metrics	FY 2023 Supplemental Metrics	FY 2023 Assessed Maturity Average[11]	FY 2023 Assessed Maturity
Identify	3.67	3.60	3.63	Consistently Implemented

[11] The FY 2023 Assessed Maturity Average was calculated by averaging the core and supplemental metrics. The calculated averages were truncated to determine the maturity level. In determining maturity levels and the overall effectiveness of Council's information security program, RMA focused on the results of the core metric and made a risk-based determination of overall program and function level effectiveness.

Function	Core Metrics	FY 2023 Supplemental Metrics	FY 2023 Assessed Maturity Average[11]	FY 2023 Assessed Maturity
Protect	3.88	3.70	3.79	Consistently Implemented
Detect	4.00	4.00	4.00	Managed and Measurable
Respond	3.50	4.00	3.75	Consistently Implemented
Recover	3.50	4.50	4.00	Managed and Measurable
Overall Maturity	**3.71**	**3.96**	**3.83**	**Consistently Implemented**

Table 3: The Council's FY 2023 Maturity Levels

Function	Core Metrics	FY 2023 Supplemental Metrics	FY 2023 Assessed Maturity	RMA's FY 2023 Assessed Maturity Level[12]
Identify	Consistently Implemented	Consistently Implemented	Consistently Implemented	Effective
Protect	Consistently Implemented	Consistently Implemented	Consistently Implemented	Effective
Detect	Managed and Measurable	Managed and Measurable	Managed and Measurable	Effective
Respond	Consistently Implemented	Managed and Measurable	Consistently Implemented	Effective
Recover	Consistently Implemented	Managed and Measurable	Managed and Measurable	Effective
Overall Maturity	**Consistently Implemented**	**Consistently Implemented**	**Consistently Implemented**	**Effective**

RMA focused on the results of the core metrics to determine the maturity level and used the calculated averages of the supplemental metrics as a data point to support our risk-based determination of overall program and function level effectiveness. The overall maturity level of the information security program was determined as Consistently Implemented and, as such, was effective for the period April 1, 2022, through March 31, 2023.

NOTE: No significant operation change for the Council occurred from the previous year; however, DHS adopted a new scoring model for FY 2023 that resulted in the Council achieving a maturity level of Consistently Implemented. Based on Council's risk tolerance and threat models, RMA used discretion to determine the overall effectiveness of Council'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 our assessments. Using this approach, RMA determined that a particular domain, function areas, and/or the Council's information security program is effective at a calculated maturity level lower than Level 4.

[12] Based on the Council's overall implementation of security controls and considering the unique mission, resources, and challenges of the Council, we found the Council's information security program and practices were effective.

The Chief Information Officer (CIO) was required to monitor and evaluate the performance of information system programs and practices based on performance measurements. The following paragraphs provide more details on each functional area's assessed maturity level.

The overall maturity level of the Council's information security program was determined as Consistently Implemented based upon calculated average scores for each domain's maturity level, and due to the CIO's direct involvement in every information technology (IT) security decision, his direct oversight of security controls, and the simple IT structure of stand-alone laptops and service vendors. Our tests of effectiveness found no exceptions.

Below is the maturity level for each domain.

Risk Management: We determined the Council's overall maturity level for the Risk Management domain was Consistently Implemented. The Council did not perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting implications. Given the Council uses third party service providers for their information system needs, the Council did not need the level of sophistication to protect its assets. Our testing found no exceptions for risk management, and the controls were operating as intended. The Council implemented its security architecture across the enterprise, business process, and system levels to help leadership make informed risk management decisions. Those risk management decisions helped improve and update the Council's risk management policies, procedures, and strategy, including methodologies for categorizing risk, developing a risk profile, assessing risk, determining risk appetite/tolerance levels, responding to risk, and monitoring risk. Consequently, based on the Council's overall implementation of security controls and considering the unique mission and resources, we concluded the Council's Risk Management controls in place were effective overall.

Supply Chain Risk Management: We determined the Council's overall maturity level for the SCRM domain was Consistently Implemented. Although the Council defined supply chain policies and procedures, the Council did not define qualitative and quantitative performance metrics as required by Questions 12-14 of the *FY 2023-2024 IG Reporting Metrics* (see Appendix I). The Council managed its supply chain risks by purchasing products from trusted and approved manufacturers. The Council's OSN was considered a server-less network with a *Federal Information Processing Standards* (FIPS) Publication 199' low rating.[13] Although the maturity level of this domain was Consistently Implemented, our testing found no exceptions, and the controls were operating as intended. The Council only had a single IT vendor with a small number of machines to maintain. Hence, the Council had limited SCRM risks. We concluded the Council's SCRM controls in place were effective.

Configuration Management: We determined the Council's overall maturity level for the Configuration Management domain was Consistently Implemented. The Council did not own or

[13] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, states that a potential impact on organizations or individuals was considered low if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

host its own systems. The Council website was hosted by U.S. Geological Survey Data Center which falls under the Department of the Interior's Vulnerability Disclosure Policy (VDP). As such, the Council was not responsible for managing VDP. In addition, the Council's laptops were connected to a local network and its primary configuration management considerations were related to the standard configuration of their laptops. Our testing found no exceptions, and the controls were operating as intended. We concluded the Council's Configuration Management controls in place were effective.

Identity and Access Management: We determined the Council's overall maturity level for the Identity and Access Management domain was Consistently Implemented. The Council managed the Identity and Access Management protocols for its employees and contractors. Due to the Council's size and structure with all systems, except the OSN, being cloud-based and housed by third parties, account changes could only be made on local machines. All accounts are local accounts that were not shared and could only be modified by a privileged user logging into each machine. The Council did not use automated tools to inventory and manage accounts and perform segregation of duties/least privilege reviews. Since there is only one privileged user, their CIO, it would not have been cost-effective to use automated tools to inventory and manage accounts. Our testing found no exceptions, and controls were operating as intended. We concluded the Council's Identity and Access Management controls in place were effective.

Data Protection and Privacy: We determined the Council's overall maturity level for the Data Protection and the Privacy program was Consistently Implemented. The Council did not process Personally Identifiable Information (PII) data. PII needed for human resources and payroll were handled through agreements with third parties, which have systems approved to collect and process PII. Controls over PII were the responsibility of the Council's outsourced service providers. Our testing found no exceptions, and controls were operating as intended. We concluded the Council's Data Protection and Privacy controls in place were effective.

Security Training: We determined the Council's overall maturity level for the Security Training program was Managed and Measurable. The Council effectively allocated resources in a risk-based manner for stakeholders to implement security awareness training consistently. The Council also was able to demonstrate the ability to monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. In addition, the Council addressed its identified knowledge, skills, and abilities gaps through talent acquisition. Our testing of the Council's workforce assessment found no exceptions, and controls were operating as intended. We concluded the Council's Security Training controls in place were effective.

Information Security and Continuous Monitoring: We determined the Council's overall maturity level for the ISCM program was Managed and Measurable. The Council regularly analyzed performance metrics to adjust and improve its program. The decisions regarding IT operations were made with the direct involvement and approval of the Council's CIO, allowing leadership to monitor and analyze the effectiveness of its ISCM program. The Council also utilized the results of security control assessments and monitoring to maintain ongoing authorizations of information systems. Our testing found no exceptions, and the controls were operating as intended. We concluded the Council's ISCM program in place were effective.

Incident Response: We determined the Council's overall maturity level for the Incident Response program was Consistently Implemented. Given the Council did not own network servers, the Council had limited exposure to the possibility of security incidents. The Council performed tabletop exercises yearly to evaluate the implementation of its incident response policies, and it was found through these exercises that the policies were effective. The small organizational structure enabled the Council to respond to and address security incidents quickly. As a result, the Council's Computer Security Incident Response Center could be assembled quickly to meet the required reporting timelines and expedite reporting of incidents. As the Council did not experience any incidents, the effectiveness of controls, such as quantitative and qualitative measures specific to incident handling could not be evaluated. However, our overall control testing for this domain found no exceptions, and the controls were operating as intended. We concluded the Council's Incident Response program in place were effective.

Contingency Planning: We determined the Council's overall maturity level for the Contingency Planning program was Managed and Measurable. Given the Council did not own any network servers, it developed policies and procedures for Contingency Planning which were consistently implemented, as well as developed quantitative and qualitative effectiveness measures necessary to reach the Managed and Measurable level. As the Council's systems, apart from OSN, were managed by third-party providers, controls such as quantitative and qualitative measures to reach the Managed and Measurable maturity level were the responsibility of the third-party providers. Through our control testing for this domain, we found no exceptions and determined the controls were operating as intended. We concluded the Council's Contingency Planning controls in place were effective.

Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, we concluded that the Council's information security program and practices were established. They were maintained for the five Cybersecurity Function areas and nine FISMA Metric Domains. Even though within the context of the maturity model, Level 4, Managed and Measurable, represents an effective level of security, based on the Council's overall implementation of security controls and considering the unique mission, resources, and challenges of the Council, we found the Council's information security program, and practices were effective for the period April 1, 2022, through March 31, 2023, and the overall maturity level of the Council's information security program was Consistently Implemented.

Objective, Scope, and Methodology

Objective

The objective of this evaluation was to determine the effectiveness of the Council's information security program and practices for the period of April 1, 2022, through March 31, 2023.

Scope

The scope of our work included the Council's Office Support Network (OSN) and eight system service providers.

The Council's OSN was technically not a computer network as it included no network servers. OSN was a stand-alone group of laptops connected to a leased wireless access point that provides a leased Virtual Private Network connection to the Trusted Internet Connection portal. Our evaluation scope covered the period between April 1, 2022, and March 31, 2023.

We determined the effectiveness of the Council's security program and practices by evaluating the following five Cybersecurity Framework security function areas as follows:

- Identify, which includes questions pertaining to Risk Management and Supply Chain Risk Management;
- Protect, which includes questions pertaining to Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training;
- Detect, which includes questions pertaining to Information Security Continuous Monitoring;
- Respond, which includes questions pertaining to Incident Response; and
- Recover, which includes questions pertaining to Contingency Planning.

As part of our evaluation, we evaluated and responded to the 20 FY 2023 Core and 20 Supplemental Inspector General (IG) Metrics specified by Office of Management and Budget (OMB) in the *FY 2023-2024 IG FISMA Reporting Metrics* (issued on February 10, 2023). We assessed the maturity levels on behalf of the Treasury Office of Inspector General. See Appendix I for details of FY 2023 – 2024 IG *Federal Information Security Modernization Act of 2014* (FISMA) Reporting Metric*s*.

Methodology

The overall strategy of our evaluation considered the following: (1) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations;* (2) NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations;* (3) FY 2023-2024 IG FISMA Reporting Metrics; and (4) the Council's policies and procedures. Our testing procedures were developed from NIST SP 800-53A, Revision 5. For each of the FY 2023 20 Core and 20 Supplemental Inspector General (IG) Metrics, we indicated whether the Council achieved each maturity level by stating "MET" or "NOT MET." Core and Supplemental metrics were averaged independently to determine a domain's maturity calculation and provide data points for the assessed program and function effectiveness. Appendix I shows the FISMA questions followed by the narrative of the maturity level, the criteria, and our test procedures.

We conducted interviews with Council officials and reviewed legal and regulatory requirements stipulated in FISMA. We also examined documents supporting the information security program and practices. Where appropriate, we compared documents, such as the Council's information technology policies and procedures, to requirements stipulated in NIST special publications. Also, we performed tests of system processes to determine the adequacy and effectiveness of those controls.

In testing the effectiveness of the security controls relevant to the 20 Core and 20 Supplemental Metrics specified in OMB's *FY 2023 – 2024 IG FISMA Reporting Metrics*, we tested the entire population of administrative controls of the Council. The application controls were the responsibility of the Council's service providers.

We conducted the FISMA evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE)'s *Quality Standards for Inspection and Evaluation* (issued in December 2020); and other evaluation requirements contained in the following: (1) OMB Circular No. A-130, *Managing Information as a Strategic Resource*; (2) OMB Memorandum M-22-05, *Fiscal Year 2022-2023 Guidance on Federal Information Security and Privacy Management Requirements*; (3) NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations dated September 23, 2020;* (4) NIST *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1,* dated April 16, 2018, and (5) FY 2023 -2024 IG FISMA Reporting Metrics criteria.

We based our FY 2023 FISMA evaluation approach on Federal information security guidelines developed by NIST, OMB, and the Council. NIST SPs provide guidelines considered essential to developing and implementing the Council's security programs. We applied the following criteria in performing the Council's FY 2023 FISMA evaluation.

NIST FIPS Publications, SPs, and Other Guidance

- FIPS Publication 199*, Standards for Security Categorization of Federal Information and Information Systems*
- FIPS Publication 200*, Minimum Security Requirements for Federal Information and Information Systems*
- FIPS Publication 201-3, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
- NIST Cybersecurity Framework (CSF)
- NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*
- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*
- NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*

- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- NIST SP 800-40, Revision 4, *Guide to Enterprise Patch Management Planning: Preventative Maintenance for Technology*
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*
- NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*
- NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*
- NIST SP 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide*
- NIST SP 800-63-3, *Digital Identity Guidelines*
- NIST SP 800-83, Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*
- NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*
- NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*
- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
- NIST SP 800-161, Revision 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*
- NIST SP 800-181, Revision 1, *Workforce Framework for Cybersecurity* (*NICE Framework)*
- NIST SP 800-207, *Zero Trust Architecture*
- NIST SP 800-218, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*
- NIST Interagency Report 8011, *Automation Support for Security Control Assessments, Volume 1: Overview*
- NIST Interagency Report 8011, *Automation Support for Security Control Assessments, Volume 2: Hardware Asset Management*
- NIST Interagency Report 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*

OMB Policy Directives

- OMB Circular No. A-130, *Managing Information as a Strategic Resource*
- OMB Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*

- OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*
- OMB Memorandum M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*
- OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*
- OMB Memorandum M-21-30, *Protecting Critical Software Through Enhanced Security Measures*
- OMB Memorandum M-20-32, *Improving Vulnerability Identification, Management, and Remediation*
- OMB Memorandum M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative*
- OMB Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*
- OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*
- OMB Memorandum M-17-26, *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda*
- OMB Memorandum M-17-09, *Management of Federal High Value Assets*
- OMB Memorandum M-16-17, *OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*
- OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*
- OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*
- OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors*

GAO

- Standards for Internal Control in the Federal Government (September 2014)

DHS Directives and Other Guidance

- FY 2023 – 2024 IG FISMA Reporting Metrics
- DHS Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*
- DHS Emergency Directive 21-04, *Mitigate Windows Print Spooler Service Vulnerability*
- DHS Emergency Directive 21-03, *Mitigate Pulse Connect Secure Product Vulnerabilities*

- DHS Emergency Directive 21-02, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*
- DHS Emergency Directive 21-01, *Mitigate SolarWinds Orion Code Compromise*
- DHS Emergency Directive 20-04, *Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday*
- DHS Emergency Directive 20-03, *Mitigate Windows DNS Server Vulnerability from July 2020 Patch Tuesday*
- DHS Emergency Directive 20-02, *Mitigate Windows Vulnerabilities from January 2020 Patch Tuesday*
- DHS Binding Operational Directive 20-01, *Develop and Publish Vulnerability Disclosure Policy*
- DHS Binding Operational Directive 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*
- DHS Emergency Directive 19-01, *Mitigate DNS Infrastructure Tampering*
- DHS Binding Operational Directive 18-02 *Securing High Value Assets*
- DHS Binding Operational Directive 18-01, *Enhance Email and Web Security*
- DHS Binding Operational Directive 17-01, *Removal of Kaspersky-branded Products.*
- DHS Binding Operational Directive 16-03, *2016 Agency Cybersecurity Reporting Requirements*
- DHS Binding Operational Directive 16-02, *Threat to Network Infrastructure Devices*

Council

- Council Information Technology Policy and Procedures (2021 – 2023)

Appendix I: FY 2023 – 2024 IG FISMA Reporting Metrics

Key Changes to the FY 2023 IG FISMA Metrics

One of the annual *Federal Information Security Modernization Act of 2014* (FISMA) evaluation goals was to assess agencies' progress toward achieving outcomes that strengthen Federal cybersecurity, including implementing the Administration's priorities and best practices. The Office of Management and Budget (OMB) issued Memorandum M-23-03, *Fiscal Year (FY) 2023 Guidance on Federal Information Security and Privacy Management Requirements,* on December 2, 2022, which among other areas such as directing Federal agencies to increase their Continuous Diagnostics and Mitigation implementation efforts, provides guidance on how OMB and the Council of the Inspectors General (IG) on Integrity and Efficiency (CIGIE) are transitioning the IG metrics process to a multi-year cycle where a core group of metrics must be evaluated annually and that the remainder of the standards and controls will be evaluated in metrics on a two year cycle based on a calendar agreed to by CIGIE, OMB, the Federal Chief Information Security Officer (CISO) Council, and Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

As a representation of this guidance, on February 10, 2023, the final Inspector General FISMA Metrics for FY 2023 were released,[14] which included the core metrics plus an additional 20 supplemental metrics to be assessed in the review cycle of FY 2023. The remaining supplemental metrics will be tested during the review cycle of FY 2024. RMA Associates, LLC (RMA) included the results of the core metrics and 20 supplemental metrics identified as Group 1 in Appendix I.

Additionally, OMB Memorandum M-23-03 solidifies the adjustment of the timeline for the IG evaluation of agency effectiveness to align the results of the evaluation with the budget submission cycle to facilitate the timely funding for the remediation of problems identified. Historically, IG's evaluation of agency effectiveness finished in October, until FY 2022 when the deadline shifted to July 31 of each year unless an extension was granted to September 30, 2022. For FY 2023, the IG evaluation has a deadline of July 31, 2023, for FISMA reporting to OMB and DHS.

Finally, in previous years, IGs were directed to use a model-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 to the function and overall information security program level. However, OMB and CIGIE determined this was not the best approach. The approach for FY 2023 will focus on a calculated average approach (instead of mode), wherein IGs will use the average of the metrics in a particular domain to determine the effectiveness of individual function areas (identify, protect, detect, respond, and recover) and the overall program.

[14] DHS FY 2023 – 2024 IG FISMA Reporting Metrics

FY 2023 Core and Supplemental IG Metrics

OMB developed the FY 2023 Core and Supplemental IG Metrics by selecting 40 of the 66 FISMA questions from DHS' *FY 2022 IG FISMA Reporting Metrics* Version 1.1 (May 12, 2022).[15] For ease of mapping, the same question numbers were used for the FY 2023 – 2024 IG FISMA Reporting Metrics as follows:

Identify – Risk Management

- Question 1: Information Technology (IT) Inventory, which supports Zero trust requirements of M-22-05
- Question 2: Asset Management – Hardware Inventory Listing
- Question 3: Asset Management – Software Inventory Listing
- Question 5: System-Level Risk Management
- Question 7: Risk Management Roles and Responsibilities
- Question 8: Plan of Actions and Milestones (POA&M)
- Question 9: Cyber Risk Communication
- Question 10: Automated View of Cybersecurity Risk

Identify – Supply Chain Risk Management (SCRM)

- Question 12: SCRM Strategy
- Question 13: SCRM Policies and Procedures
- Question 14: SCRM Oversight

Protect – Configuration Management

- Question 19: Baseline Configuration
- Question 20: Configuration Settings
- Question 21: Flaw Remediation
- Question 22: Trusted Internet Connection Program
- Question 24: Vulnerability Disclosure Policy

Protect – Identity and Access Management (ICAM)

- Question 26: ICAM Roles and Responsibilities
- Question 27: ICAM Policy/Strategy
- Question 29: Access Agreements
- Question 30: Strong Authentication Mechanisms for Non-Privileged Users
- Question 31: Strong Authentication Mechanisms for Privileged Users
- Question 32: Least Privilege/Separation of Duties
- Question 33: Remote Access

Protect – Data Protection and Privacy

- Question 35: Privacy Program

[15] The remainder of the standards and controls will be evaluated in metrics on a two-year cycle based on a calendar agreed to by CIGIE, CISO Council, OMB, and CISA.

- Question 36: Personally Identifiable Information Security Controls
- Question 37: Security Controls for Exfiltration

Protect – Security Awareness and Training

- Question 41: Security Training Roles and Responsibilities
- Question 42: Assessment of Skills, Knowledge, and Abilities of Organization Workforces
- Question 43: Security Awareness Training Plan

Detect – Information Security Continuous Monitoring

- Question 47: Information System Continuous Monitoring (ISCM) Strategy
- Question 48: ISCM Roles and Responsibilities
- Question 49: Ongoing Authorization

Respond – Incident Response

- Question 54: Incident Detection
- Question 55: Incident Handling
- Question 57: IT Technical Assistance
- Question 58: Incident Response Tools

Recover – Contingency Planning (CP)

- Question 60: Contingency Roles and Responsibilities
- Question 61: Business Impact Analysis
- Question 63: IT Contingency Plan Testing
- Question 65: CP Stakeholder Communication

Identify Function Area – Risk Management Domain

Question 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 800-53. Rev. 5: CA-3, PM-5, and CM-8; NIST Cybersecurity Framework (CSF) ID.AM-1 – 4; NIST SP 800-37, Rev. 2; OMB A-130; OMB 23-03; FY 2023 CIO FISMA Metrics: 1.1 and 1.5)? [16]
Managed and Measurable
The organization ensures that the information systems included in its inventory are subject to the monitoring processes defined within the organization's ISCM strategy. **MET** – Based on previous evaluations, we noted the Council used third-party systems for all its information systems. As a user (stakeholder) of its information systems, the Council had limited control of its information systems. The Council had eight information systems and was most effectively managed by a third party through an interagency agreement. Additionally, based on our examination, we noted that the ISCM Strategy was defined in the System Security Plan (SSP) for the Office Support Network (OSN) and the Continuous Monitoring Plan for OSN. We examined the Council's Continuous Monitoring Plan, which defined guidelines for metrics and security controls that aligned with their information security goals and identified improvements to the security posture of the systems. The plan depicted that the information system inventory was reviewed annually in June. We reviewed the Information System Component Inventory control and noted that the Council updated and reviewed its inventory in June 2022. We reviewed the Council's Inventory listing, updated from FY 2022. As such, the Council developed a continuous monitoring plan incorporating the ISCM strategy, and the monitoring process of performing an annual review of its information system inventory was consistent.
Optimized
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 was updated in a near-real time basis. **NOT MET** – Due to the unique size and structure of the Council's information systems, the Council did not use automation to develop and maintain a centralized information system inventory that included hardware and software components from all organizational information systems. The centralized inventory was not updated in a near real-time basis.

[16] Abbreviations: (CA) Assessment, Authorization, and Monitoring, (PM) Program Management, (CM) Configuration Management, (ID.AM) Identify – Asset Management.

Identify Function Area – Risk Management Domain

Question 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)?[17]

Managed and Measurable

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.

MET –The Council was a small organization with a small number of hardware assets, laptops, and smartphones connected to its OSN. The Council maintained an inventory of its hardware assets and monitors its assets on a real-time basis; the report showed the real-time inventory of hardware assets and other items. The Chief Information Officer (CIO) ensured that the hardware assets were connected to the network and its internet and subject to the monitoring processes defined within its ISCM strategy. RMA examined the Council's Continuous Monitoring Plan and noticed that the plan defined a complete inventory of system components that should be completed yearly. Additionally, as part of the monitoring plan, RMA noted that the CIO needed to review the Continuous Diagnostics Mitigation (CDM) Dashboards, third party help desk provider reports, and internal tracking sheet monthly to ensure inventory lists include all assets. RMA then obtained and reviewed the most recent Equipment List and determined the Council tracked all its assets, including laptops, mobile phones, and network devices, in the internal tracking spreadsheet. Additionally, we reviewed a screenshot of the CDM Asset Dashboard and determined the Council monitored and managed its assets through third-party software as defined in the ISCM strategy. RMA also obtained and reviewed the third-party help desk reports. The Council CIO tracked and maintained an inventory of its hardware assets and monitored its assets on a real-time basis. The Council had no network server. Therefore, there was no agency enterprise services to which the Council would have denied access. The Council relied on third party system service providers and only controlled its OSN. In addition to the laptops, the Council used mobile devices not connected to the OSN.

[17] Abbreviations: (GFE) Government Furnished Equipment, (NIST IR) National Institute of Standards and Technology Interagency or Internal Report, (CIS) Center for Internet Security.

Identify Function Area – Risk Management Domain

Optimized
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. **NOT MET** – The Council did not employ automation to track the life cycle of the organization's hardware assets with processes that limit the manual/procedural methods for asset management. Due to the Council's small organizational size, automated methods for asset management are unnecessary and not cost-effective.

Identify Function Area – Risk Management Domain

Question 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)?

Managed and Measurable

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).

MET –The Council was a micro-agency with interconnected stand-alone laptops and mobile devices. The Council ensured its software assets on the OSN, except mobile devices that were not connected to its OSN, were subject to the monitoring processes defined within the organization's ISCM strategy. The Council implemented the CDM software program, which could prevent the execution of unauthorized software. The only software assets the Council was responsible for were the third-party operating system and third-party software installed on its endpoints. The software was installed through the helpdesk resources. Users submitted a request to the CIO, who submitted the request to the help desk to install the software. Users had regular accounts without installation privileges. The Council bought third party software. As new laptops were issued to staff, Council used user-based third party licenses. The Council kept accurate records of its software assets and was in the process of converting mobile assets to CDM tools. We examined the Council's Mobile Device Policy, section *GCERC Issues Phones*, that stated employees may not obtain apps outside of the third party mobile store. Users must use a 6-digit PIN/Touch ID to ensure the data on the phone remains encrypted. Users must install phone updates when prompted to protect themselves from security threats. All mobile device security was reviewed on a recurring basis to ensure that the requirements were met, and the security guidelines were in line with Federal requirements. The Council was working with Cybersecurity Infrastructure Security Agency (CISA) to implement CDM Mobile device software which should be completed by mid-June. The policy was scheduled to be reviewed to determine the necessary changes. For mobile devices, the Council implemented the CDM software program, which enforced the capability to prevent the execution of unauthorized software. RMA noted the software blocking screenshot, which showed a screen capture of custom Indicators of Attack rules that blocked executables.

Identify Function Area – Risk Management Domain

Optimized
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. **NOT MET** – We found the Council did not employ automation to track the life cycle of the organization's software assets (and their associated licenses) with processes that limit the manual/procedural methods for asset management. However, software inventories were regularly updated as part of the organization's enterprise architecture in current and future states. The only software assets the Council was responsible for the third-party operating system and the third party software installed on its laptops. It should be noted that the Council was a user (stakeholder) of all its information systems.

Identify Function Area – Risk Management Domain

Question 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)?[18]
Managed and Measurable
The organization utilizes 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 was documented in a cybersecurity risk register and serves 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 was obtained accurately, consistently, and in a reproducible format and was used to (i) quantify and aggregate security risks, (ii) normalize cybersecurity risk information across organizational units, and (iii) prioritize operational risk response.*** **MET** –In the OSN SSP, the Council evaluated the risk based on the system level for the potential impact on an organization should certain events jeopardize the information and information systems needed by the Council to accomplish its assigned mission, protect its assets, maintain its day-to-day functions, and protect individuals. The Council considered the risk of losing confidentiality, integrity, and availability. The Council used a POA&M (Plan of Actions & Milestones) to track Information Technology (IT) security risks as a Risk Register. The POA&M tracker listed the risks that the Council monitors. Due to the unique structure of the Council's information systems, the Council monitored and analyzed its defined qualitative and quantitative performance measures by reviewing a POA&M tracker, CDM Asset Dashboard, and studying cybersecurity testing quarterly. The POA&M tracker depicted the weakness and mitigation plan the Council developed for its IT security posture. The CDM Dashboard implementation and the third party help desk reports and internal tracking sheet depicted the tracking of the Council's assets. The CIO reported directly to the agency's senior Enterprise Risk Management (ERM) Officer. We reviewed the Risk Profile that depicted the assessment results determining the Council's Risk Profile and Critical Risk Mitigation highlights. The profile highlighted the Council's focus on ERM as one of the top seven critical risks. In addition, the Council developed a plan to mitigate critical risks. Based on a review of its risk profile, this served as input into the organization's enterprise risk management program.

[18] Abbreviations: (RA) Risk Assessment.

Identify Function Area – Risk Management Domain

Optimized
The cybersecurity risk management program was 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 was 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 utilizes Cybersecurity Framework profiles to align cybersecurity outcomes with mission or business requirements, risk tolerance, and resources of the organization.*** **NOT MET –** In the interview with the CIO, it was stated that achieving an optimized maturity level would not be cost-effective since the Council was a micro-agency with a unique organizational size and structure. We found the Council did not establish a Cybersecurity Framework profile to align cybersecurity outcomes with mission requirements, risk tolerance, and resources of the organization to ensure that continuous identification and monitoring of all risks is at acceptable levels.

Identify Function Area – Risk Management

Question 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)?[19]
Managed and Measurable
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. **MET** –The Council had a unique organizational size and structure. The Council CIO was the only employee responsible for all IT-related activities. The CIO was intimately involved in all aspects of the Council's risk management program and was aware of every major decision involving its IT operations and risk management program. The CIO communicated to oversee and address the risk management capabilities of the Council. Additionally, the Council documented the identified risks and developed a defined strategy to mitigate those risks.
Optimized
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. **NOT MET** – Council's risk management program did not address the full spectrum of an agency's risk portfolio across all organizational (major units, offices, and lines of business) and business (agency mission, programs, projects, etc.) aspects. Due to the Council's unique organizational structure and size, it may be misleading to state the maturity level of the Council as Optimized.

[19] Abbreviations: (ID.RM) Identify – Risk Management Strategy, (ID. GV) Identify – Governance.

Identify Function Area – Risk Management

Question 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)?[20]

Managed and Measurable

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 was maintained.

MET –The Council performed qualitative and quantitative performance measures by manually tracking all their POA&M on a spreadsheet. The spreadsheet contained the following fields:

- ID – Date when POA&M opened.
- Type of Weakness – Describes the weakness the Council had discovered.
- Point of Contact – Appropriate party responsible for the POA&M.
- Resources Required – Additional Items needed to mitigate the POA&M.
- Scheduled Completion Date – Estimated timeframe when POA&M can be closed.
- Milestone – Any remedial actions needed.
- Status – Whether the POA&M had been open/closed/in progress.
- Mitigation – Corrective Action Plan.

Optimized

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.

NOT MET – Given the unique structure of the Council, the Council did not employ automation to correlate security weaknesses amongst information systems and identify enterprise-wide trends and solutions on a near real- time basis. Furthermore, processes were not in place to identify and manage emerging risks and known security weaknesses.

[20] Abbreviations: ID.RA Identify – Risk Assessment.

Identify Function Area – Risk Management

Question 9
To what extent does the organization ensure that information about cybersecurity risks was 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)
Managed and Measurable
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 was used to:*** ***• Quantify and aggregate security risks*** ***• Normalize information across organizational units*** ***• Prioritize operational risk response activities*** **MET** – We inspected the Memorandum of Agreement with the CISA, relating to deploying CDM capability through a shared service environment. The utilization of DHS' CDM capability in a shared service environment lowered the total cost of ownership for all stakeholders involved; connected and obtained hardware, software, configuration, and vulnerability data from the agency sensors or through a relay/aggregator; and allowed the Council to use a Dashboard portal which allowed the Council to view its asset and vulnerability data. We inspected CDM Dashboard Snapshot, providing a real-time view of the asset overview. The Council employed robust diagnostic and reporting frameworks, including DHS CDM capabilities, which allowed the Council to use the CDM Dashboard. The Council used a collector portal to control its tools/sensors via the CDM collectors, and the Dashboard portal allowed the Council to view its assets and vulnerability data. The dashboard helped to facilitate a portfolio view of interrelated risks across the organization and presents qualitative and quantitative metrics that provide risk indicators.

Identify Function Area – Risk Management

Optimized
Using risk profiles and dynamic reporting mechanisms, cybersecurity risk information was 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. ***NOT MET*** – Due to the unique organizational structure, the Council's cybersecurity risk information was not incorporated into the organization's enterprise risk management program. It was not utilized to provide a fully integrated, prioritized, enterprise-wide view of organizational risks to drive strategic and business decisions. Cyber risks were not 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.

Identify Function Area – Risk Management

Question 10

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)?

Consistently Implemented

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.

MET –We inspected the continuous monitoring reports for OSN performed by a third party. The third party's monthly reports included a monthly service ticket list that listed all the service tickets opened during the corresponding month, monthly patch compliance reports, and a monthly Executive Summary Report. The Council implemented both CDM programs and third party software to monitor monthly inventory. In addition, a bi-weekly test of third party software was created to ensure the system was working properly. The CIO noted that the Council utilized the CDM software tool for real-time reporting and dashboard views. The CDM program included all the endpoint security tools and anti-virus/anti-malware services. Subsequently, the CIO noted that ERM for the Council performed risk profile updates that look at risk in the agency programs. The Common Vulnerability Scoring Systems defined the risk of cybersecurity, where detected vulnerabilities were rated on a scale of exploitation and the resulting impact. The Council's one system, OSN, was rated low because its impact on organizational activities was minimal, even if compromised. The OSN SSP also noted that systems were rated low based on these factors. Subsequently, the CIO noted that ERM for the Council performed risk profile updates that look at risk in the agency programs. The Common Vulnerability Scoring Systems defined the risk of cybersecurity, where detected vulnerabilities were rated on a scale of exploitation and the resulting impact. The Council's one system, OSN, was rated low because its impact on organizational activities was minimal, even if compromised. The OSN SSP also noted that systems were rated low based on these factors. The Council had a simple flat organizational structure. The CIO and the Chief Financial Officer interact daily. The Council did not have formal departments and layers of management like larger organizations. As a result, the Council operated more efficiently and effectively than larger organizations. The CIO was the lone IT personnel personally responsible for monitoring all IT risks. The CIO stated the most significant risks were IT risks. All necessary sources of risk information were integrated into the solution.

Identify Function Area – Risk Management

Managed and Measurable
The organization uses automation to perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting impact on organizational systems and data. ***In addition, the organization ensures that cybersecurity risk management information was integrated into reporting tools, such as governance, risk management, and compliance tool) as appropriate.*** **NOT MET** – Given the unique structure of the Council, the Council did not use automation to perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting implications for organizational systems and data. The CIO noted that ERM Officer reviewed cybersecurity testing quarterly, and the CIO reported directly to the Senior ERM Officer for the Agency. However, the Council utilized third party service providers for their information system needs. The Council did not perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting implications for organizational systems and data. The Council did not need a level of sophistication to protect its assets. The Council did not have cybersecurity risk management information integrated into ERM reporting tools, such as governance, risk management, and compliance tool.

Identify Function Area – Supply Chain Risk Management

Question 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)?[21]

Consistently Implemented

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.

MET – The CIO stated that the Council manages limited IT resources. The resources operated are not considered critical systems. When considering SCRM, the Council made the decision to only to use laptop and hardware parts from a third party to ensure a secure supply chain. In addition, mobile devices are obtained through a Contract Vehicle. Mobile devices are not purchased from other suppliers. Normal laptop software was purchased through a General Services Administration vendor instead of the open market to ensure a secure supply chain.

The CIO further stated that lessons learned were integrated into the SCRM checklist for new software requests. The Council developed a short checklist for looking at software. RMA inspected a completed checklist for SCRM software review and noted that the Council used lessons learned to review and update the SCRM checklist with new software requests.

[21] Abbreviations: Abbreviations: (SR) Supply Chain Risk Management, (USC) U.S. Code, (P.L) Public Law, (H.R) House of Representatives.

Identify Function Area – Supply Chain Risk Management

Managed and Measurable
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. **NOT MET** – RMA reviewed SCRM Checklist. The Council implemented an SCRM checklist for obtaining IT Products. We found the Council did not use qualitative and quantitative performance metrics to measure, report on, and monitor information security. However, it should be noted that the Council only used laptops from one supplier. The CIO also stated that after attending SCRM discussion with CISA, additional aspects of doing an SCRM review were discussed. The Council reviewed and developed a checklist that needed to be expanded to ensure all risk was accounted for. This included adding questions concerning the country of origin and looking for known vulnerabilities in the system. These things were added based on the review of the SCRM software, which was deemed too great of a risk to use within the Council environment.

Identify Function Area – Supply Chain Risk Management

Question 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)?[22]

Consistently Implemented

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.

MET – The Council inventory consisted of only laptops and mobile devices. The CIO directly purchased the laptops and mobile devices from the third party manufacturer. The Council is considered a serverless network. We inquired with the CIO about what controls the Council had that prevented them from ordering supply chain components from unauthorized vendors. The CIO stated Delegation Option Authorization (DOA) approved all purchases. In addition, the CIO filled out Purchase forms for IT-related items. The DOA, CIO, and purchase card holders attended section 889 training for prohibited vendors. A section 889 checkbox was added to the purchase card form. The CIO reviewed all IT purchases and ensured that authorized vendors were used. Regarding lessons learned, RMA received a response from CIO, which stated that the Council developed a short checklist for looking at software products that the Council was using. After attending SCRM talks with CISA, additional aspects of doing an SCRM review were discussed. The Council reviewed and developed a checklist that needed to be expanded to ensure all risk was accounted for. This included adding questions concerning the country of origin and looking for known vulnerabilities in the system. These things were added based on the review of the SCRM software, which was deemed too great of a risk to use within the Council environment. RMA also received a completed checklist for SCRM software, which showed the process of how the checklist was completed.

[22] Abbreviations: Information Supply Chain Technology, (ID.SC) Identify – Supply Chain Risk Management.

Identify Function Area – Supply Chain Risk Management

Managed and Measurable
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 was 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.*** **NOT MET** – The Council implemented an SCRM checklist for obtaining IT products. The development of this checklist was in response to the Council determining that a more detailed check was needed when looking at software products other than a basic search of the product and using known vulnerabilities to determine the risk of using the product. We found the Council did not use qualitative and quantitative performance measures to gauge the effectiveness of its SCRM policies and procedures. It should be noted that the Council only had one third party as a supplier so given their size, metrics were tracked through the checklist.

Identify Function Area – Supply Chain Risk Management

Question 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)?[23]
Consistently Implemented
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.*** **MET** – RMA examined that a yearly test of a subset of controls was accomplished to ensure they were working and meeting requirements. RMA reviewed list of controls related to the supply chain. We found no control exceptions. The Council maintained awareness of its upstream suppliers. The Council worked through an account representative. When a laptop is refreshed, the CIO contacted the account representative to request quotes and lead times. In addition, working directly with the company ensured that equipment was not handled by third party suppliers that could impact SCRM. We examined screenshots of the third party order system, which gave the CIO real-time updates if there were issues with an order or backorders. CIO also noted that all equipment was shipped in tamper-resistant packaging.

[23] Abbreviations: (SA) System and Service Acquisition.

Identify Function Area – Supply Chain Risk Management

Managed and Measurable
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 of the supply chain risks. **NOT MET** – The Council implemented an SCRM checklist for obtaining IT products. RMA found that the Council did not use qualitative and quantitative performance metrics to measure, report on, and monitor information security. However, it should be noted that the Council only had one third party as a supplier, so given their size, metrics were tracked through the checklist.

Protect Function Area – Configuration Management Domain

Question 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)?[24]
Managed and Measurable
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. **MET** – We noted that the Council implemented CDM capabilities for real-time reporting and dashboard views. Additionally, CIO noted that the Council verified systems using the Security Content Automation Protocol (SCAP) compliance tester. We determined the Council employed automated mechanisms, including CDM software and EINSTEIN, to detect unauthorized hardware, software, and firmware on its network and take immediate actions to limit any security impact.
Optimized
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. **NOT MET** – Due to the unique structure of the Council's information systems, the Council did not utilize technology to implement a centralized baseline configuration and information system component inventory process that includes information from all organization systems (hardware and software) and was updated on a near real-time basis.

[24] Abbreviations: (DE. CM) Detect – Security Continuous Monitoring, (PR. IP) Protect – Information Protection and Processes and Procedures.

Protect Function Area – Configuration Management Domain

Question 20
To what extent does the organization utilize configuration 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 2023 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)?
Managed and Measurable
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. **MET** – We interviewed the CIO and noted that the Council implemented CDM capabilities through CDM software for real-time reporting and dashboard views. Additionally, the CIO noted that the Council used monitoring tools for patch management and asset tracking and reviews SCAP Compliance Checker Reports produced by SCAP-validated software scanning capabilities. Additionally, Council's software was within the CDM tools and EINSTEIN Cybersecurity capabilities to provide automated mechanisms to protect its networks and systems. We inspected Council Patch Compliance Procedures. We noted that the Patch Compliance report displayed the patch compliance of the Council's systems and details each device. The automated tool helped the Council maintain an up-to-date, complete, accurate, and readily available view of the security configurations.
Optimized
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. **NOT MET** – The Council does not deploy 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.

Protect Function Area – Configuration Management Domain

Question 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)?[25]
Managed and Measurable
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 was obtained accurately, consistently, and in a reproducible format.*** **MET** – We noted that the Council implemented CDM capabilities through CDM software for real-time reporting and dashboard views. Additionally, the Council used monthly reports for patch management and asset tracking and reviewed SCAP Compliance Checker Reports produced by SCAP validated software scanning capabilities. Also, the Council employed software within the CDM tools and EINSTEIN Cybersecurity capabilities to provide automated mechanisms to protect its networks and systems. We inspected Council Patch Compliance Procedures. We noted that the Patch Compliance report displayed the patch compliance of the Council's systems and details each device. The automated tool helped the Council maintain an up-to-date, complete, accurate, and readily available view of the security configurations.

[25] Abbreviations: (SI) System and Information Integrity, (EO) Executive Order.

Protect Function Area – Configuration Management Domain

Optimized
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 of its flaw remediation processes, the organization performs deeper analysis of software code through patch sourcing and testing.*** **NOT MET** – The Council had a simple, flat organizational structure without formal departments and layers of management typically found in larger organizations. As a result, the CIO was the lone IT personnel and was solely responsible for monitoring all IT assets. Further, no IT decisions were made without the CIO's direct involvement and approval. This allowed the Council to operate more efficiently and effectively than larger organizations.

Protect Function Area – Configuration Management Domain

Question 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)?[26]
Managed and Measurable
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.*** **MET** – The Council implemented the Trusted Internet Connection (TIC) initiative per OMB M-19-26, DHS guidance. In addition, the Council had its laptops to access the National Oceanic and Atmospheric Administration (NOAA) NWave network from a Virtual Private Network (VPN), as NOAA NWave functions as a TIC access provider for the Council and enabled them to comply with TIC 3.0 requirements.
Optimized
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. **NOT MET** – The Council had a simple, flat organizational structure without formal departments and layers of management typically found in larger organizations. As a result, the CIO was the lone IT personnel solely responsible for monitoring all IT assets. Further, no IT decisions were made without the CIO's direct involvement and approval. This allowed the Council to operate more efficiently and effectively than larger organizations.

[26] Abbreviations: (NCPS) National Cybersecurity Protection System.

Protect Function Area – Configuration Management Domain

Question 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)?

Consistently Implemented

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 newly launched internet accessible systems and services, and at least 50% of 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.***

MET – The Council did not own or host its own systems. U.S. Geological Survey Data Center hosts the Council website and falls under the Department of Interior vulnerability disclosure (VDP) policy. As such, the Council was not responsible for this maturity level.

Managed and Measurable

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 handling procedures.

In addition, all internet-accessible systems are included in the scope of the organization's VDP.

NOT MET – Due to the unique structure of the Council's information systems, the Council did not monitor, analyze, and report of the qualitative and quantitative performance measures used to gauge the effectiveness of its vulnerability disclosure policy and disclosure handling procedures. Also due to its unique structure, Council did not ensure all internet-accessible systems are included in the scope of its VDP.

Protect Function Area – Identity and Access Management Domain

Question 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)?[27]

Managed and Measurable

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.

MET – The Council had a simple, flat organizational structure without formal departments and layers of management typically found in larger organizations. As a result, the CIO was the lone IT personnel and was solely responsible for implementing all identity, credential, and access management activities. RMA followed up with the Council about how to make sure resources were allocated in a risk-based manner. The Council stated that all staff members receive Personal Identity Verification (PIV) cards, the standard method for identifying someone and ensuring compatibility across Federal systems. The Council added that resources were not allocated for alternate PIV based identity methods.

Due to the Council's organizational structure without formal departments and layers of management typically found in larger organizations, we determined that the Council had adequate resources (people, processes, and technology) to implement ICAM activities consistently.

Optimized

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.

NOT MET – The CIO stated that achieving this maturity level would not be cost-effective since the Council was a micro-agency with a unique organizational size and structure.

[27] Abbreviations: (AC) Access Control, (IA) Identification and Authentication, (PL) Planning, (PS) Personnel Security, (HSPD) Homeland Security Presidential Directive.

Protect Function Area – Identity and Access Management Domain

Question 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)?[28]

Consistently Implemented

The organization was consistently implementing its ICAM policy, strategy, process, and technology solution road map and was 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 was consistently capturing and sharing lessons learned on the effectiveness of its ICAM policy, strategy, and road map and making updates as needed.

MET – The Council consistently captured and shared lessons learned on the effectiveness of its ICAM policy, strategy, and road map and made updates as needed.

We inquired with the CIO and noted the Council had a simple, flat organizational structure without formal departments and layers of management typically found in larger organizations. As a result, he was the lone IT personnel and was solely responsible for implementing all identity, credential, and access management activities. The Council tracked IT risks using POA&Ms, tracked on a spreadsheet due to only having one system. The Council additionally noted that the laptops do not support PIV logins because the Council does not have an Active Directory Environment. However, staff were issued PIV credentials for VPN and partner's systems access.

We interviewed the CIO to determine whether the Council captured and shared lessons learned. The CIO stated ICAM's internal policies were not modified. However, the systems used by the Council were converted to PIV logins due to Federal mandates.

[28] Abbreviations: (PR.AC) Protect – Identity Management and Access Controls.

Protect Function Area – Identity and Access Management Domain

Managed and Measurable
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. **NOT MET** – The Council implemented its ICAM strategy and met its milestones to align with Federal initiatives, including strong authentication, the Federal ICAM architecture and OMB M-19-17, and phase 2 of DHS's CDM program. The Council laptops did not support PIV logins because the Council did not have an Active Directory Environment. Still, the staff was issued PIV credentials for VPN and partner's systems access. We noted that employee laptops only used local user accounts, and the laptop's operating system (machine-based) enforces logins and ensures policies were followed. The Council did not use automated mechanisms (e.g., machine-based, or user-based enforcement) to manage the effective implementation of its policies and procedures. Deployment of automated mechanisms may not be cost-effective considering the structure of the Council environment.

Protect Function Area – Identity and Access Management Domain

Question 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, PL-4, and PS-6)?

Consistently Implemented

The organization ensures that access agreements for individuals are completed prior to access being granted to systems and are consistently maintained thereafter. The organization utilizes more specific/detailed agreements for privileged users or those with access to sensitive information, as appropriate.

MET – The Council had a simple, flat organizational structure without formal departments and layers of management typically found in larger organizations. As a result, CIO was the lone IT personnel and was solely responsible for implementing all identity, credential, and access management activities. The CIO ensured that access agreements for individuals were completed before access was granted to systems and were consistently maintained thereafter.

Additionally, CIO was the only privileged user with no sensitive information on the network.

We reviewed the Rules of Behavior (ROB)/Access agreement for recent hires, non-privileged users, and privileged users for the Q1 FY 2023 Security Training session.

We selected a random sample of five non-privileged Council employees from a total population of 33 users to determine whether ROB and Security Awareness Essentials Training was completed. We found no exceptions.

Managed and Measurable

The organization uses automation to manage and review user access agreements for privileged and non-privileged users. To the extent practical, this process was centralized.

NOT MET – Due to the unique structure of the Council information systems, the Council did not use automation to manage and review user access agreements for privileged and non-privileged users. To the extent practical, this process was not centralized.

Protect Function Area – Identity and Access Management Domain

Question 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)?[29]
Managed and Measurable
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. **MET** – The Council's non-privileged users used strong authentication mechanisms to authenticate applicable organizational systems and facilities. RMA reviewed the VPN login screenshot and noted that PIV was used for logging in to the VPN managed by NOAA.
Optimized
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. **NOT MET** – Due to the unique structure of the Council information systems, enterprise-wide single sign on the solution and all of the organization's systems interface with the solution, resulting in an ability to manage user (non-privileged) accounts and privileges centrally and report on the effectiveness on a near real-time basis will require financial commitment and cost-benefits may not be justifiable in the Council environment.

[29] Abbreviations: (PE) Physical and Environment Protection.

Protect Function Area – Identity and Access Management Domain

Question 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)?
Managed and Measurable
All privileged users, including those who can make changes to DNS records, use strong authentication mechanisms to authenticate to applicable organizational systems. **MET** – The Council did not have access to change Domain Name System (DNS) settings. The Council did not have network resources requiring a DNS system.
Optimized
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. **NOT MET** – Due to the unique structure of the Council information systems and that the Council was not connected to a general support system or network, it was unable to implement single-sign-on.

Protect Function Area – Identity and Access Management Domain

Question 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)?[30]

Managed and Measurable

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 was meeting privileged identity and credential management logging requirements at maturity EL2 in accordance with M-21-31.

MET – The Council employed 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. We examined the screenshot of the third party software dashboard and noted it had a containment option. Once a computer is contained, it blocks all communication except the CDM software server. The third party software could also disable or delete laptops remotely.

Also, the Council met privileged identity and credential management logging requirements at maturity event logging (EL)2, in accordance with M-21-31. RMA found that the CDM tool provides centralized logging and user login information.

Optimized

The organization was making demonstrated progress towards implementing EL3's advanced requirements for user behavior monitoring to detect and alert privileged user compromise.

NOT MET – The Council had not made progress towards implementing EL3's advanced requirements for user behavior monitoring to detect and alert on privileged user compromise.

[30] Abbreviations: (AU) Audit and Accountability.

Protect Function Area – Identity and Access Management Domain

Question 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)?[31]
Managed and Measurable
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. **MET** – RMA determined that all end-user devices were configured according to the Council Security Technical Implementation Guides settings. Users did not have administrator rights to change any settings. VPN requires the software, config file, and PIV card to access. These were only installed on properly configured government-furnished devices. We reviewed the screenshot of the PIV login and noted that the VPN installed in the devices requires PIV prior to access.
Optimized
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. **NOT MET** – The Council had not deployed the capability to rapidly disconnect remote access user sessions based on active monitoring.

[31] Abbreviations: (SC) System and Communication Protection.

Protect Function Area – Identity and Access Management Domain

Question 35

To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that was 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))?[32]

Managed and Measurable

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.

MET – RMA reviewed a screenshot of the third party software dashboard and noted that the dashboard monitored new detections and the severity level of security events. The Council stated they also used the CISA CareWatch Team, which monitored the third party software and helped detect events. We examined the screenshot of the CareWatch meeting minutes during its implementation and observed that the minutes provided specific information about the integration of CareWatch.

The Council did not manage any systems that handle personally identifiable information (PII).

Optimized

The privacy program was 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 was embedded into daily decision making across the organization and provides for continuous identification of privacy risks.

NOT MET – The Council’s privacy program was not fully integrated with other security areas, such as ISCM, and other business processes, such as strategic planning and risk management. Further, the Council's privacy program was not embedded into daily decision making across the organization and provides for continuous identification of privacy risks.

[32] Abbreviations: (PT) Personally Identifiable Information Processing and Transparency, (SAOP) Senior Agency Official for Privacy.

Protect Function Area – Identity and Access Management Domain

Question 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)?[33]
Managed and Measurable
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. **MET** – The Council did not collect PII. The Council did not have network applications and no general support systems. The Council IT environment consisted of laptops connected to shared service providers. There are no business reasons for laptops to store PII.
Optimized
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 was to be deleted or destroyed according to an approved data retention schedule.*** **NOT MET** – Because the Council did not collect or store PII, the Council did not employ advanced capabilities to enhance protective controls.

[33] Abbreviations: (PT) Personally Identifiable Information Processing and Transparency, (SAOP) Senior Agency Official for Privacy.

Protect Function Area – Data Protection and Privacy Domain

Question 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)?

Consistently Implemented

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.

MET – The Council consistently monitored inbound and outbound network traffic, ensured all traffic passed through a web content filter that protects against phishing and malware, and blocks against known malicious sites. The Council utilized the CDM program to enhance network defenses. Additionally, the Council checked outbound communications traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of PII. Also, suspected malicious traffic was quarantined or blocked. As the Council used a third party service provider for email, the third-party service provider was responsible for email authentication. The Council did not have a network server and the Council did not keep PII information.

Optimized

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 was coordinating with CISA for future EDR solution deployments.

NOT MET – The Council did not analyze qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses as they have not conducted data exfiltration exercises. OSN is a low system. We inspected NIST SP 800-53B Revision 5, System and Communications Protection Family Table (Table 3-18) on page 46 and noted that SC-7(10) Prevent Unauthorized Exfiltration is not applicable for low-impact systems. In addition, the Council did not maintain DNS infrastructure. DNS records are hosted by NOAA.

Protect Function Area – Security Training Domain

Question 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)[34]

Managed and Measurable

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.

MET – The Council has a unique organizational structure, and the Council CIO is the only privileged account user. The CIO is responsible for the day-to-day activities of the Council's IT. The CIO develops all IT security training, sends out training, and tracks the completion of training. As a result, we determined resources are allocated in a risk-based manner as he is the lone IT person in the organization. In addition, we reviewed Quarterly Security Quizzes which provided evidence of security training that has been provided to users. The quizzes are tracked by user email which helps to keep a record of user training and progress. Each quiz provided the user with questions regarding a specific security training topic such as: social engineering hacks, insider threats, phishing, and PII. After training was complete, user data was entered into a spreadsheet which is used to monitor the results of the training. Any user who failed the training is emailed with more security training information and training. Based on the evidence reviewed, RMA made the determination that resources were allocated in a risk-based manner.

Optimized

The organization continuously evaluates and adapts its security training roles and responsibilities to account for a changing cybersecurity landscape.

NOT MET – Based on our examination, CIO maintained a certificate that required 40 hours a year of continuous education. This education requirement requires up-to-date training on the latest cybersecurity landscape. However, based on the evidence provided, RMA could not determine if the Council continuously evaluates and adapts its security training roles and responsibilities to account for a changing cybersecurity landscape.

[34] Abbreviations: (AT) Awareness and Training.

Protect Function Area – Security Training Domain

Question 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)?
Managed and Measurable
The organization has addressed its identified knowledge, skills, and abilities gaps through training or talent acquisition. **MET** – Based on our examination of the Council's Annual Report on Cyber Work Roles and the User Listing, the Council addressed its identified knowledge, skills, and abilities gaps through talent acquisition. The Council had a total of 33 employees for FY 2023.
Optimized
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. **NOT MET** – The Council was a small organization. It did not employ trend analysis that could demonstrate that security incidents resulting from personnel actions or inactions were reduced over time.

Protect Function Area – Security Training Domain

Question 43

To what extent does the organization use a security awareness and training strategy/plan that leverages its skills assessment and was 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)?

Managed and Measurable

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.

MET – Based on our examination with Council we determined the organization monitored and analyzed qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. Per management response, CIO reviewed quarterly quizzes and contacted any staff that got wrong answers. Then it was explained to staff why their answers were wrong and if they understood the training. We reviewed quarterly security quizzes, and noted the Council provided Security Training quizzes to their users. The Council's IT ROB greeted users, then asked if they complied with the rules of behavior before starting the quiz. The quizzes asked a series of security training questions and scenarios to measure the level of awareness of the user. The Council also provided screenshots at the end of each quarterly quiz to provide records on their user's quizzes.

Optimized

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.

NOT MET – The Council security awareness and training activities were not integrated across other security-related domains. The Council had zero threats for FY 2023, and as such, no evidence security threats identified were part of the Council's security awareness and training activities.

Detect Function Area –Information and Security Continuous Monitoring

Question 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)?

Managed and Measurable

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.

MET – The Council had a unique organizational structure of the Council and relied on third-party service providers for its ISCM capabilities. The Council monitored and analyzed measures on the effectiveness of its ISCM policies and procedures and made updates as necessary. The Council reviewed reports provided by the third-party help desk service provider, and software to better ascertain the effectiveness of its ISCM policies and procedures. The Council ran monthly scanning reports and other management reports that show the Council monitored and analyzed qualitative and quantitative performance measures on the effectiveness of its ISCM strategy as shown in Monthly Reports. We also determined the Monthly Reports showed that Council transitioned to ongoing control and system authorization through the implementation of its continuous monitoring policies and strategy.

Optimized

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 was using its ISCM policies and strategy to reduce the cost and increase the efficiency of security and privacy programs.

NOT MET – The Council did not fully integrate its ISCM strategy with risk management, configuration management, incident response, and business continuity functions. In addition, the Council was not using its ISCM policies and strategy to reduce the cost and increase the efficiency of security and privacy programs.

Detect Function Area –Information and Security Continuous Monitoring

Question 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)[35]
Managed and Measurable
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. **MET** – The Council had a small organizational structure without a typical network available in a large organization, and the CIO was the lone IT personnel. The Council relied on a third party to manage its information systems. As such, the Council service providers were responsible for implementing ISCM activities on those systems.
Optimized
The organization continuously evaluates and adapts its ISCM-based roles and responsibilities to account for a changing cybersecurity landscape. **NOT MET** – The Council had a simple, flat organizational structure with few employees. The Council did not have formal departments and layers of management like larger organizations. Therefore, they do not continuously evaluate and adapt its ISCM-based roles and responsibilities to account for a changing cybersecurity landscape.

[35] Abbreviations: (DE. DP) Detect – Detection Processes.

Detect Function Area –Information and Security Continuous Monitoring

Question 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)?

Managed and Measurable

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.

MET – The Council utilized the results of security control assessments and monitoring to maintain ongoing authorizations of information systems. We found that Council performed a control review of its security assessment. If any deficiencies or findings were found, they were added to the POA&M to track and monitor corrective actions. The Council's simple and flat organizational structure did not have formal departments and layers of management like larger organizations allowing the Council to operate more efficiently and effectively than larger Federal agencies.

Optimized

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 was using its system level ISCM policies and strategy to reduce the cost and increase the efficiency of security and privacy programs.

NOT MET – The Council's ISCM policies and procedures were not fully integrated with its enterprise and supply chain risk management, configuration management, incident response, and business continuity programs. In addition, the Council did not demonstrate that it was using its system level ISCM policies and strategy to reduce the cost and increase the efficiency of security and privacy programs.

Respond Function Area –Incident Response Domain

Question 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)[36]
Managed and Measurable
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 was meeting logging requirements at maturity EL2 (intermediate) in accordance with M-21-31.*** **MET** – The Council did not experience any incidents in FY 2023 The Council used performance measures/dashboards to measure the effectiveness of its incident handling policies and procedures. The Council performed tabletop exercises yearly to examine incident response policies. It was found through these exercises that the policy was effective, and the procedures were correct. RMA reviewed the incident response table-top exercises and confirmed the Council performed the exercise for FY 2023. The Council did not have centralized logging implemented. The Council used CDM capabilities in which security logging was accomplished through third party software, which provided a centralized repository for logging if an incident was detected. Due to the Council having a simple, flat organizational structure, Council did logging using third party software, which was done locally instead of a centralized method. This logging was saved on the local laptop. The third party software provided a centralized repository for logging, and, based on the unique mission and resources, we determined the Council's information security program was effective.

[36] Abbreviations: (IR) Incident Response, (DE.AE) Detect – Anomalies and Events, (PR. DS) Protect – Data Security, (RS.AN) Respond – Analysis.

Respond Function Area –Incident Response Domain

Managed and Measurable
The Council used software within the CDM tools to perform profiling techniques. In addition, the Council used the CISA Carewatch service to ensure everything was configured correctly, met requirements, and assisted the Council with possible findings. We examined the evidence provided and determined that the detected incident was rated as suspicious (critical/high/medium/low) and showed tactics, technique, detect time, host, username, and status. A third party software was set to generate a test detection every two weeks. The system consisted of stand-alone laptops and desktops that are used to connect to a secure VPN. The VPN connection was not part of this system and was managed by a Federal Partner. The Council did not implement centralized logging, which was not applicable; however, based on the unique mission and resources, we determined Council's information security program was effective.
Optimized
The organization was making demonstrated progress towards implementing EL3's (advanced) requirements for its logging capabilities. **NOT MET** – The Council had a simple, flat organizational structure with few employees and did not implement centralized logging. The Council used CDM capabilities to accomplish security logging via Software, which provides a centralized repository for logging if an incident was detected. Therefore, they did not demonstrate progress towards implementing EL3's (advanced) requirements for its logging capabilities.

Respond Function Area –Incident Response Domain

Question 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)[37]
Consistently Implemented
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 was consistently capturing and sharing lessons learned on the effectiveness of its incident handling policies and procedures and making updates, as necessary.*** **MET** – The Council developed containment strategies for each major incident type through its Incident Response Plan. In developing its strategies, the Council had taken 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, the effectiveness of the strategy, and the duration of the solution. In addition, the Council defined its processes to eradicate an incident's components, mitigate any exploited vulnerabilities, and recover system operations. The Council relied on third party software, DHS, CISA, and utilized the CDM program to help identify and help to eradicate components of an incident, mitigate any vulnerabilities that were exploited, and recover system operations. Due to the Council's reliance on third party service providers for its information systems needs and the Council's unique organizational structure, the Council limited exposure to security incidents in its information systems. The Council performed tabletop exercises yearly to look at incident response policies, and it was found through these exercises that the policy was effective, and procedures were correct. We inspected the tabletop exercise for FY 2023 designed to validate their understanding of the OSN Incident Response Plan. The test report included testing procedures and captured and shared lessons learned/recommendations from the exercise.

[37] Abbreviations: (RS.MI) Respond – Mitigation.

Respond Function Area –Incident Response Domain

Managed and Measurable

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.

NOT MET – As a small agency that primarily used information systems that third party providers hosted, the Council had limited exposure to vulnerabilities and security incidents in its information systems. The Council did not report any incidents during the evaluation period. The Council relied on third-party service providers for its information system's needs. Since the Council did not experience any incidents in FY 2023, we could not validate if the Council manages and measures the impact of successful incidents and could quickly mitigate related vulnerabilities on other systems so that they were not subject to exploitation of the same vulnerability.

Respond Function Area –Incident Response Domain

Question 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)?[38]
Managed and Measurable
The organization monitors and analyzes qualitative and quantitative performance measures on theeffectiveness 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 utilizes profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents. Examples of profiling include running file integrity checking software on hosts to derive checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times. Through profiling techniques, the organization maintains a comprehensive baseline of network operations and expected data flows for users and systems.*** **MET** – The Council conducted tabletop exercises and used third party providers to measure the effectiveness of its incident detection and analysis policies and procedures. In addition, through a third-party provider, the Council utilized profiling techniques to measure the characteristics of expected activities on its networks and systems to detect security incidents more effectively.
Optimized
The organization was 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. **NOT MET** – The Council was not 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.

[38] Abbreviations: (RS.MI) Respond – Mitigation.

Respond Function Area –Incident Response Domain

Question 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)?

Managed and Measurable

The organization evaluates the effectiveness of its incident response technologies and makes adjustments to configurations and toolsets, as appropriate.

MET – The CISA CareWatch Team and CIO monitored the capabilities of incident response. CISA decided on product choices and procured for the Council. The Council itself did not operate a network. The Council hosts were protected using CDM software (host-based security). They used the NOAA NWave Network via VPN to connect to Federal resources needed for business processes.

Managed Trusted Internet Protocol Service provider, NOAA NWave network, provided a full-time SOC. Therefore, the Council did not review intrusion detection tools as the NOAA SOC accomplished this. The CIO will be notified if an issue is detected within the Council designated internet protocol ranges.

Optimized

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.

NOT MET – The Council was a micro-agency with a unique organizational structure that relied on third-party providers for its information systems. As a result, we determined that the Council had not institutionalized the implementation of advanced incident response technologies for analysis of trends and performance against benchmarks (e.g., simulation-based technologies to continuously assess the impact of potential security incidents to its IT assets) and adjusted incident response processes and security measures accordingly.

Recover Function Area –Contingency Planning Domain

Question 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)?[39]
Optimized
The organization incorporates simulated events into contingency training to facilitate effective responses 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. **MET** – We examined the FY 2023 Contingency Tabletop Exercise and determined the Council incorporated contingency training into contingency tabletop exercises. Since Council had a very simplified system OSN that consisted of laptops, the tabletop exercise was conducted in simulated events when a user could not log in to their laptop and NOAA response times. The exercise report included the appropriate contingency activities, testing results, and action items. We determined Council ensured its stakeholders were equipped to perform their roles and responsibilities accordingly.

[39] Abbreviations: (CP) Contingency Planning, (FCD) Federal Continuative Directive.

Recover Function Area –Contingency Planning Domain

Question 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)?

Managed and Measurable

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.

MET – The CIO stated the information for the Business Impact Analysis (BIA) was reported to the Director of Administration and other team leaders to ensure they were aware of system level acquisition requirements for systems. The BIA results were shared with senior leadership and The Council used a POA&M to track IT security risks. The POA&M Tracker listed the risks that the Council monitors. We reviewed POA&M Tracker and noted the Council only listed one risk, Patch Compliance.

Additionally, based on a review of the FY 2023 Risk Profile, this served as input into the organization's enterprise risk management program. The profile highlighted how the Council's focus on ERM was one of the top seven critical risks. As such, RMA determined the Council ensured that the results of BIAs were integrated with enterprise risk management processes and risk profiles to inform senior-level decision-making.

Optimized

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.

NOT MET –The results were shared with Council ERM staff to determine placement in the Council Risk Profile. However, we could not determine whether the Council integrated its BIA and asset management processes to improve risk identification, accurate exposure consideration (based on realistic calculations of harmful impacts), and effective risk response.

Recover Function Area –Contingency Planning Domain

Question 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)?
Consistently Implemented
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. **MET** – We inspected the results of the Contingency Tabletop Exercise FY 2023. The testing was conducted assuming users were having issues logging in to the computer and testing NOAA Response Time. Based on the results, we determined Information System Contingency Plan (ISCP) testing and exercises were integrated, to the extent practicable, with testing of related plans, such as incident response plan/Continuity of Operations Plan (COOP)/Business Continuity Plan (BCP).
Managed and Measurable
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.*** **NOT MET** – We noted that the Council system was rated minimal risk and had a unique organizational structure and a very simplified system that consists of laptops. Therefore, an automated system was not required to test contingency plans. Furthermore, the Council used laptop warranty services, including service timelines if a laptop failed.

Recover Function Area –Contingency Planning Domain

Question 65
To what level does the organization ensure that information on the planning and performance of recovery activities was communicated to internal stakeholders and executive management teams and used to make risk-based decision (NIST SP 800-53 (Rev. 5): CP-2 and IR-4; NIST CSF: RC.CO-3)? [40]
Managed and Measurable
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. **MET** – We inspected the Council's OSN ISCP and BIA and identified the metrics used to measure the effectiveness of the contingency team. We also reviewed the IT Contingency Tabletop Exercise test activities, test results and action items that were documented and shared with Senior Accountable Official Risk Manager.
Optimized
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. **NOT MET** –The CIO contacted equipment and software providers to ensure items were obtained promptly and securely. However, there was no evidence showing that the planning and performance of recovery activities for its ICT supply chain providers were integrated into communication processes on a near real-time basis. Due to the unique size and structure of the Council's information systems, near real-time incorporation with ICT supply chain providers was not cost-effective.

[40] Abbreviations: (RC.CO) Recover – Communications (COOP) Continuity of Operations Plan, (BCP) Business Continuity Plan.

Evaluation Results

The overall maturity level of the Council's information security program was Consistently Implemented. We have presented the maturity level for the nine domains below:

Table 4: The Council's FY 2023 Maturity Levels

Cybersecurity Framework Security Functions	FY 2023 IG FISMA Metric Domains	Maturity Level
Identify	Risk Management	Consistently Implemented
Identify	Supply Chain Risk Management	Consistently Implemented
Protect	Configuration Management	Consistently Implemented
Protect	Identity and Access Management	Consistently Implemented
Protect	Data Protection and Privacy	Consistently Implemented.
Protect	Security Training	Managed and Measurable
Detect	Information Security Continuous Monitoring	Managed and Measurable
Respond	Incident Response	Consistently Implemented
Recover	Contingency Planning	Managed and Measurable
Overall		**Consistently Implemented.**

RMA included a summary of the domains that Council did not achieve a rating of Managed and Measurable:

Risk Management: We determined the Council's overall maturity level for the Risk Management program was Consistently Implemented. The Council did not perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting implications for organizational systems and data. Given the Council utilizes third-party service providers for their information system needs, the Council did not need a high level of sophistication to protect its assets. Our testing found no risk management exceptions, and the controls were operating as intended. The Council implemented its security architecture across the enterprise, business process, and system levels to help leadership make informed risk management decisions. Those informed risk management decisions helped continually improve and update the Council's risk management policies, procedures, and strategy, including methodologies for categorizing risk, developing a risk profile, assessing risk, determining risk appetite/tolerance levels, responding to risk, and monitoring risk. Consequently, based on the Council's overall implementation of security controls and considering the unique mission and resources, we concluded the Council's Risk Management controls were effective overall.

Supply Chain Risk Management: We determined the Council's overall maturity level for the SCRM program was Consistently Implemented. Although the Council defined supply chain policies and procedures, the Council did not define qualitative and quantitative performance metrics as required by Questions 12-14 of the *FY 2023-2024 IG Reporting Metrics* (see Appendix I). The Council managed its supply chain risks by purchasing products from trusted and approved manufacturers. The Council's OSN was considered a server-less network with a FIPS

Publication 199' low rating.[41] Although the maturity level of this domain was Consistently Implemented, our testing found no exceptions, and the controls were operating as intended. The Council only had a single IT vendor with limited operating machines. Hence, the Council had limited SCRM risks. We concluded the Council's SCRM program controls in place were effective.

Configuration Management: We determined the Council's overall maturity level for the Configuration Management program was Consistently Implemented. The Council did not own or host its own systems. U.S. Geological Survey Data Center hosted the Council website under the Department of Interior VDP. As such, the Council was not responsible for managing VDP. In addition, the Council’s laptops were connected to a local network and its primary configuration management considerations were related to the standard configuration of their laptops. Our testing found no exceptions, and the controls were operating as intended. We concluded the Council's Configuration Management program controls in place were effective.

Identity and Access Management: We determined the Council's overall maturity level for the Identity and Access Management program was Consistently Implemented. The Council managed the Identity and Access Management protocols for its employees and contractors. Due to the Council's size and structure with all systems, except the OSN, being cloud-based and housed by third parties, account changes could only be made on local machines. All accounts were local accounts that were not shared and could only be modified by a privileged user logging into each machine. The Council did not use automated tools to inventory and manage accounts and perform segregation of duties/least privilege reviews. Our testing found no exceptions, and controls were operating as intended. We concluded the Council's Identity and Access Management program controls in place were effective.

Data Protection and Privacy: We determined the Council’s overall maturity level for the Data Protection and the Privacy program was Consistently Implemented. The Council did not process PII data. PII needed for human resources and payroll were handled through agreements with third parties, which have systems approved to collect and process PII. Controls over PII were the responsibility of the Council’s outsourced service providers. Our testing found no exceptions, and controls were operating as intended. We concluded the Council’s Data Protection and Privacy controls in place were effective.

Incident Response: We determined the Council's overall maturity level for the Incident Response program was Consistently Implemented. Given the Council did not own network servers, the Council had limited exposure to the possibility of security incidents. The Council performed tabletop exercises yearly to evaluate the implementation of its incident response policies, and it was found through these exercises that the policies were effective. The small organizational structure enabled the Council to respond to and address security incidents quickly. As a result, the Council's Computer Security Incident Response Center could be assembled quickly to meet the required reporting timelines and expedite reporting of incidents. As the Council did not experience

[41] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, states that a potential impact on organizations or individuals was considered low if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

any incidents, the effectiveness of controls, such as quantitative and qualitative measures specific to incident handling could not be evaluated. However, our overall control testing for this domain found no exceptions, and the controls were operating as intended. We concluded the Council's Incident Response program controls in place were effective.

Appendix II: Management Response

Gulf Coast Ecosystem Restoration Council

July 17, 2023

Richard K. Delmar
Deputy Inspector General
Department of the Treasury
1500 Pennsylvania Avenue NW
Room 4436
Washington, DC 20220

Re: The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2023

Thank you for the opportunity to review The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2023.

The Council agrees with the results of the evaluation, that the Council's information security program and practices were effective for the period April 1, 2022 through March 31, 2023. The Council works to ensure that the five Cybersecurity Functions defined by NIST and the nine FISMA Metric domains defined by OMB and CISA are met.

In fiscal year 2024, the Council will use this evaluation report to improve information assurance decisions to ensure a continued effective information security program. The Council will also continue its efforts to consistently implement, manage and measure its IT security program at an optimized level in order to support projects and programs to achieve the goals and objectives of the RESTORE Act for restoration in the Gulf Coast region

Sincerely,

MARY WALKER Digitally signed by MARY WALKER Date: 2023.07.17 09:39:00 -04'00

Mary S. Walker Executive Director
Gulf Coast Ecosystem Restoration Council

REPORT WASTE, FRAUD, AND ABUSE

Submit a complaint regarding Treasury OIG Treasury Programs and Operations using our online form: https://oig.treasury.gov/report-fraud-waste-and-abuse

TREASURY OIG WEBSITE

Access Treasury OIG reports and other information online: https://oig.treasury.gov/