Evaluation Report

OIG-CA-24-021

CYBERSECURITY/INFORMATION TECHNOLOGY

The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2024

July 29, 2024

Office of Inspector General
Department of the Treasury

This Page Intentionally Left Blank

OFFICE OF
INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

July 29, 2024

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 2024 (OIG-CA-24-021)

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 2024*, dated July 29, 2024. 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, 2023 through March 31, 2024. 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, 2023 through March 31, 2024.

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

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 2024

RMA | Associates
Auditors. Consultants. Advisors.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone : (571) 429-6600
www.rmafed.com

July 29, 2024

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 2024

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) 2024. 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, 2023, through March 31, 2024.

For FY 2024, the Office of Management and Budget (OMB) identified 20 core and 17 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. We conducted an assessment of FY 2024 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 2024 IG FISMA Reporting Metrics.

In summary, we found the Council's information security program and practices were effective for the period April 1, 2023, through March 31, 2024.

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

AAL	Authenticator Assurance Level
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
BIA	Business Impact Analysis
BOD	Binding Operational Directive
BYOD	Bring Your Own Device
CA	Assessment, Authorization, and Monitoring
CCB	Change Control Board
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
Council	Gulf Coast Ecosystem Restoration Council
CP	Contingency Planning
CSF	Cybersecurity Framework
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
ERM	Enterprise Risk Management
FCD	Federal Continuity Directive
FEA	Federal Enterprise Architecture
FedRAMP	Federal Risk and Authorization Management Program
FIDO2	Fast Identity Online 2
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAO	Government Accountability Office
GFE	Government Furnished Equipment
HSPD	Homeland Security Presidential Directive
IA	Identification and Authentication
IAL	Identity Assurance Level
ICT	Information and Communications Technology
ID.AM	Identify – Asset Management
ID.BE	Identify – Business Environment
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
IR	Incident Response
NICE Framework	Workforce Framework for Cybersecurity
NIST	National Institute of Standards and Technology
NIST IR	National Institute of Standards and Technology Interagency or Internal Report
NIST SP	National Institute of Standards and Technology Special Publication
MP	Media Protection
OMB	Office of Management and Budget
OSN	Office Support Network
PII	Personally Identifiable Information
PIV	Personal Identity Verification
P.L.	Public Law
PL	Planning
PM	Program Management
PO	Purchase Order
PPD	Presidential Policy Directive
PR.AC	Protect – Identity Management and Access Control
PR.AT	Protect – Access Training
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
RS.AN	Respond – Analysis
RS.MI	Respond – Mitigation
RS.RP	Respond – Response Planning
SA	System and Service Acquisition
SAOP	Senior Agency Official for Privacy
SDLC	System Development Life Cycle
SECURE	Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure
SI	System and Information Integrity
SC	System and Communication Protection
SM	Security Management
SP	Special Publication
SR	Supply Chain Risk Management
TIC	Trusted Internet Connection
US-CERT	United States Computer Emergency Readiness Team

RMA Associates
Auditors. Consultants. Advisors.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone : (571) 429-6600
www.rmafed.com

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 Office of Inspector General engaged RMA Associates, LLC (RMA) to conduct the Fiscal Year (FY) 2024 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, 2023, through March 31, 2024.

As part of our evaluation, we responded to the FY 2024 metrics from OMB's *FY 2023-2024 Inspector General (IG) FISMA Reporting Metrics,* Version 1.1, dated February 10, 2023.[2] For FY 2024, 17 supplemental metrics were evaluated in addition to the 20 core metrics evaluated in FY 2023. These metrics aligned with the five function areas in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity: 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 of Evaluation Results

We concluded that the Council's information security program and practices were established and maintained for the five Cybersecurity Function areas consistent with FISMA requirements, OMB policy and guidance, and NIST standards and guidelines,[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. We found the Council's information security program and practices were effective for the period April 1, 2023, through March 31, 2024. Although within the context of the maturity model, Level 4, Managed and Measurable, represents

[1] Public Law (P.L.) 113-283, Federal Information Security Modernization Act of 2014 (Dec. 18, 2014).
[2] OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency 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.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone : (571) 429-6600
www.rmafed.com

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 Gulf Coast Restoration 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. Additionally, the Council includes the Governors of the States of Alabama, Florida, Louisiana, Mississippi, and Texas, as well as the Environmental Protection Agency 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 strengthened the use of continuous monitoring in systems, increased focus on the agencies' compliance, and produced 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

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone : (571) 429-6600
www.rmafed.com

government's data and information systems security, such as requiring the development of minimum control standards for agencies' systems.

FISMA extends oversight authority of agency security policies and practices to OMB and provides DHS, in consultation with OMB, the authority for implementing agency policies and practices for information systems.[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, principles, standards, and guidelines.[6]

The Director of OMB "directs the Secretary [of DHS] to consult with and consider guidance developed by the 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;

[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/2521.
[6] Ibid.
[7] Ibid.
[8] Ibid.
[9] Ibid.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone : (571) 429-6600
www.rmafed.com

- Complying with the requirements of NIST's related policies, procedures, and standards;
- Ensuring information security management processes are integrated with agency 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 2024 Core and Supplemental IG Metrics

OMB's *FY 2023 – 2024 IG FISMA Reporting Metrics* Version 1.1, dated February 10, 2023, specified the FY 2024 20 Core and 17 Supplemental IG Metrics (refer to Appendix I). It directed IGs to report the assessed maturity levels of these metrics in CyberScope[11] no later than July 31, 2024. The FY 2024 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;
- 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.

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 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. 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 5.1.1, *Security and Privacy Controls for Federal Information Systems and Organizations* (November 2023).
[11] CyberScope is an online reporting tool, established by OMB, developed to streamline the collection of cybersecurity performance data, including FISMA metric results, from federal agencies.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone : (571) 429-6600
www.rmafed.com

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, 2023, and March 31, 2024. It consisted of testing the 20 Core and 17 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. Since FY 2023, a calculated average scoring model has been used, where core and supplemental metrics are 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. The Council's overall program calculation is shown in **Table 2**. The Council's FY 2024 corresponding maturity levels for the five function areas and the overall level are presented in **Table 3**.

Table 2: The Council's Overall Calculated Averages Maturity Calculation in FY 2024

Function	Core Metrics	FY 2024 Supplemental Metrics	FY 2024 Assessed Maturity Average[12]	FY 2024 Assessed Maturity
Identify	3.83	3.67	3.75	Consistently Implemented
Protect	3.88	4.13	4.00	Managed and Measurable

[12] The FY 2024 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.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone : (571) 429-6600
www.rmafed.com

Function	Core Metrics	FY 2024 Supplemental Metrics	FY 2024 Assessed Maturity Average[12]	FY 2024 Assessed Maturity
Detect	4.00	4.00	4.00	Managed and Measurable
Respond	3.50	3.33	3.42	Consistently Implemented
Recover	3.50	3.00	3.25	Consistently Implemented
Overall Maturity	**3.74**	**3.63**	**3.68**	**Consistently Implemented**

Table 3: The Council's FY 2024 Maturity Levels

Function	Core Metrics	FY 2024 Supplemental Metrics	FY 2024 Assessed Maturity	RMA's FY 2024 Assessed Maturity Level[13]
Identify	Consistently Implemented	Consistently Implemented	Consistently Implemented	Effective
Protect	Consistently Implemented	Managed and Measurable	Managed and Measurable	Effective
Detect	Managed and Measurable	Managed and Measurable	Managed and Measurable	Effective
Respond	Consistently Implemented	Consistently Implemented	Consistently Implemented	Effective
Recover	Consistently Implemented	Consistently Implemented	Consistently Implemented	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.

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.

NOTE: No significant operational changes for the Council occurred from the previous year; however, DHS adopted a new scoring model in 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.

[13] 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.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone : (571) 429-6600
www.rmafed.com

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.

Due to the CIO's direct involvement in information technology (IT) security decisions, his oversight of security controls, and the Council's simple IT environment with stand-alone laptops and service vendors, the overall maturity level of the information security program was determined as Consistently Implemented based on calculated average scores for each domain. 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 that the Council uses third-party service providers for its information system needs, the Council did not require highly sophisticated internal controls to protect its assets. Our testing found no exceptions in risk management, and the existing 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. Our testing found no exceptions, and the controls were operating as intended. We concluded the Council's Risk Management controls in place were effective.

Supply Chain Risk Management: We determined the Council's overall maturity level for the Supply Chain Risk Management domain was Managed and Measurable. The Council defined supply chain policies and procedures. 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.[14] Our testing found no exceptions, and the controls were operating as intended. We concluded the Council's Supply Chain Risk Management controls in place were effective.

Configuration Management: We determined the Council's overall maturity level for the Configuration Management domain was Managed and Measurable. The Council performed qualitative and quantitative performance measures on the effectiveness of its configuration management plan. The Council utilized automation to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for information system components connected to the Council's network. Our testing found no exceptions, and the controls

[14] 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.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone : (571) 429-6600
www.rmafed.com

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 was only one privileged user, deploying automated tools for user account inventory and management wouldn't have been cost-effective. 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 Managed and Measurable. 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 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 Information Security and Continuous Monitoring 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 Information Security and Continuous Monitoring 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 Information Security and Continuous Monitoring 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

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone : (571) 429-6600
www.rmafed.com

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 the 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 Consistently Implemented. Since the Council does not own any network servers, it developed contingency planning policies and procedures that were consistently implemented. 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, 2023, through March 31, 2024, and the overall maturity level of the Council's information security program was Consistently Implemented.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone : (571) 429-6600
www.rmafed.com

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, 2023, through March 31, 2024.

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, 2023, and March 31, 2024.

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 fiscal year (FY) 2024 20 Core and 17 Supplemental Inspector General (IG) Metrics specified by Office of Management and Budget (OMB) in the *FY 2023-2024 IG Federal Modernization Act (FISMA) Reporting Metrics* (issued on February 10, 2023). We assessed the maturity levels on behalf of the Department of the Treasury's Office of Inspector General. See Appendix I for the results of each metric and assessed maturity level.

Methodology

The overall strategy of our evaluation considered the following: (1) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5.1.1, *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 2024 20 Core and 17 Supplemental IG Metrics, we indicated whether the Council achieved each maturity level by stating "MET" or "NOT MET." Core and Supplemental metrics were averaged independently

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone : (571) 429-6600
www.rmafed.com

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 SPs. 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 17 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. For the non-Department of the Treasury service providers, we examined the applicable service level agreements in place to gain an understanding of the terms and conditions and agreed-upon procedures for delivering enterprise services provided to the Council. For the Department of the Treasury-based service provider, we examined the relevant System and Organization Controls report, to determine if the controls were designed and operating effectively and if there were any issues that could impact the user's entity environment.

We conducted the FISMA 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); and other evaluation requirements contained in the following: (1) OMB Circular No. A-130, *Managing Information as a Strategic Resource*; (2) OMB Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*; (3) NIST SP 800-53, Revision 5.1.1, *Security and Privacy Controls for Information Systems and Organizations dated November 7, 2023;* (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 2024 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 2024 FISMA evaluation.

NIST Federal Information Processing Standards (FIPS) and SPs

- 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 SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone : (571) 429-6600
www.rmafed.com

- 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 Technologies: Preventive Maintenance for Technology*
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
- NIST SP 800-53, Revision 5.1.1, *Security and Privacy Controls for Information Systems and Organizations*
- NIST SP 800-53A, Revision 5.1.1, *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 Federal Information Systems and Organizations*
- NIST SP 800-181, Revision 1, *Workforce Framework for Cybersecurity* (*NICE Framework)*
- NIST Interagency Report 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*

OMB Policy Directives

- OMB Memorandum M-24-04, *Fiscal Year 2024 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*

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone : (571) 429-6600
www.rmafed.com

- 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-19-03, *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-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*
- OMB Circular No. A-130, *Managing Information as a Strategic Resource*

GAO

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

DHS

- *FY 2023 – 2024 IG FISMA Reporting Metrics*
- DHS Binding Operational Directive 23-01, *Implementation Guidance for Improving Asset Visibility and Vulnerability Detection on Federal Networks*
- DHS Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*
- 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 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*
- 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*

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone : (571) 429-6600
www.rmafed.com

- 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 Domain Name System (DNS) Server Vulnerability from July 2020 Patch Tuesday*
- DHS Emergency Directive 20-02, *Mitigate Windows Vulnerabilities from January 2020 Patch Tuesday*
- DHS Emergency Directive 19-01, *Mitigate DNS Infrastructure Tampering*

The CIO Council's FISMA's policies and procedures

- Council Information Technology Policy and Procedures (May 2024)

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone : (571) 429-6600
www.rmafed.com

Appendix I: Fiscal Year (FY) 2024 Inspector General (IG) Federal Information Modernization Act (FISMA) Reporting Metrics Results

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone : (571) 429-6600
www.rmafed.com

Key Changes to the FY 2024 IG FISMA Metrics

One of the annual FISMA evaluation goals is 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-24-04[15], *Fiscal Year (FY) 2024 Guidance on Federal Information Security and Privacy Management Requirements*, on December 4, 2023. This memorandum directs Federal agencies to increase their Continuous Diagnostics and Mitigation implementation efforts. M-24-04 also provides guidance on how OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) are transitioning the Inspector General (IG) metrics process to a multi-year cycle. This cycle involves a core group of metrics evaluated annually and the remaining standards and controls assessed in metrics on a two-year cycle based on a calendar agreed upon by CIGIE, OMB, the Federal Chief Information Security Officer (CISO) Council, and the Cybersecurity and Infrastructure Security Agency (CISA).

As a representation of this guidance, on February 10, 2023, the final IG FISMA Metrics for FY 2024 were released[16], which included the Core Metrics plus an additional 17 Supplemental Metrics to be assessed in review cycle FY 2024. The FY 2024 IG metrics are based on coordinated discussions between (and the consensus opinion of) representatives from OMB, CIGIE, Federal Civilian Executive Branch Chief Information Security Officers and their staff, the Intelligence Community, and among other Office of Inspector General's throughout the Federal government included in an established working group.[17]

Additionally, OMB Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements,* 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. For FY 2024, the IG evaluation has a deadline of July 31, 2024, for FISMA reporting to OMB and the Department of Homeland Security (DHS) to better align the release of IG assessments to facilitate the timely funding for the remediation of problems identified. The previous timing limited agency leadership's ability to request resources in the next Budget Year submissions to provide for remediations. Outlined below is implementation guidance to support IGs as they manage this adjustment.

[15] M-24-04 *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, (December 2023)
[16] *FY 2023 – 2024 V 1.1 IG FISMA Reporting Metrics*
[17] CISO Council FISMA Metrics Subcommittee

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone : (571) 429-6600
www.rmafed.com

FY 2024 Core and Supplemental IG Metrics

OMB developed the FY 2024 Core and Supplemental IG Metrics by selecting 37 of the 66 FISMA questions from the DHS' *FY 2022 IG FISMA Reporting Metrics* Version 1.1 (May 12, 2022).[18] 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
- Question 2: Asset Management – Hardware Inventory Listing
- Question 3: Asset Management – Software Inventory Listing
- Question 4: High-Value Asset Management
- Question 5: System-Level Risk Management
- Question 6: Information Security Architecture
- Question 10: Automated View of Cybersecurity Risk

Identify – Supply Chain Risk Management

- Question 14: Supply Chain Risk Management Oversight
- Question 15: Counterfeit Components

Protect – Configuration Management

- Question 17: Roles and Responsibilities
- Question 18: Configuration Management Plan
- Question 20: Configuration Settings
- Question 21: Flaw Remediation
- Question 23: Configuration Change Control

Protect – Identity and Access Management

- Question 28: Position Risk Designation
- Question 30: Strong Authentication Mechanisms for Non-Privileged Users
- Question 31: Strong Authentication Mechanisms for Privileged Users
- Question 32: Least Privilege/Separation of Duties

Protect – Data Protection and Privacy

- Question 36: Personally Identifiable Information Security Controls
- Question 37: Security Controls for Exfiltration
- Question 38: Data Breach Response Plan

[18] 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.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone : (571) 429-6600
www.rmafed.com

- Question 39: Privacy Awareness Training

Protect – Security Awareness and Training

- Question 42: Assessment of Skills, Knowledge, and Abilities of Organization Workforces
- Question 44: Security Awareness Training
- Question 45: Specialized Security Training

Detect – Information Security Continuous Monitoring

- Question 47: Information System Continuous Monitoring Strategy
- Question 49: Ongoing Authorization
- Question 50: Information Security Continuous Monitoring performance measures

Respond – Incident Response

- Question 52: Incident Response Plan
- Question 53: Incident Response Team
- Question 54: Incident Detection
- Question 55: Incident Handling
- Question 56: Incident Notification

Recover – Contingency Planning

- Question 61: Business Impact Analysis
- Question 62: Contingency Planning
- Question 63: IT Contingency Plan Testing
- Question 64: System Backup and Storage

Risk Management – IDENTIFY FUNCTION

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) (**Core**)[19]

   Managed and Measurable (Level 4)

   Comments: 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. Also, the centralized inventory was not updated on a near real-time basis. Recognizing the unique size and structure of the Council's information systems, the Council's maturity level for this metric was "Managed and Measurable."

2. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including GFE) and Bring Your Own Device (BYOD) mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting (NIST SP 800-37 (Rev. 2): Tasks P-10 and P-16; NIST SP 800-53 (Rev. 5): CA-7 and CM-8; NIST SP 800-137; NIST SP 800-207; NIST 1800-5; NIST IR 8011; NIST CSF: ID.AM-1; Federal Enterprise Architecture (FEA) Framework; FY 2023 CIO FISMA Metrics: 1.2, 1.3, and 10.8; CIS Top 18 Security Controls: Control 1; OMB M-23-03; DHS Binding Operational Directive (BOD) 23-01; BOD 23-01 Implementation Guidance) (**Core**)[20]

   Managed and Measurable (Level 4)

   Comments: The Council did not employ automation to track the life cycle of the organization's hardware assets, using processes that limit the manual/procedural methods for asset management. However, due to the Council's small organizational size, automated methods for asset management are unnecessary and not cost-effective. As such, the Council's maturity level for this metric was "Managed and Measurable."

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-

[19] Abbreviations: (NIST SP): National Institute of Standards and Technology Special Publication, (CA): Assessment, Authorization, and Monitoring, (PM): Program Management, (CM): Configuration Management, (ID.AM): Identify – Asset Management, (CIO): Chief Information Officer.

[20] Abbreviation: (NIST IR): National Institute of Standards and Technology Interagency or Internal Report, (FY): Fiscal Year, (FISMA): Federal Information Security Modernization Act of 2014, (CIS): Center for Internet Security, (DHS): Department of Homeland Security, (GFE): Government Furnished Equipment.

03; CIS Top 18 Security Controls: Control 2; CISA Cybersecurity Incident Response Playbooks) (**Core**)[21]

Managed and Measurable (Level 4)

Comments: 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 were the operating system installed on its laptops. It should be noted that the Council was a user (stakeholder) of all its information systems. Recognizing the unique size and structure of the Council's information systems, the Council's maturity level for this metric was "Managed and Measurable."

4. To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets (NIST SP 800-37 (Rev. 2): Tasks C-2, C-3, P-4, P-12, P-13, S-1 – S-3; NIST SP 800-53 (Rev. 5): RA-2, PM-7, and PM-11; NIST SP 800-60; NIST IR 8170; NIST CSF: ID.BE-3, ID.AM-5, and ID.SC-2; FIPS 199; FY 2023 CIO FISMA Metrics: 1.1; OMB M-19-03) (**Supplemental**)[22]

   Managed and Measurable (Level 4)

   Comments: The Council did not use impact-level prioritization for additional granularity, and cybersecurity framework profiles, as appropriate, to support risk-based decision-making. Recognizing the unique size and structure of the Council's information systems, the Council's maturity level for this metric was "Managed and Measurable."

5. To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels (NIST SP 800-37 (Rev. 2): Tasks P-2, P-3, P-14, R-2, and R-3; NIST SP 800-39; NIST SP 800-53 (Rev. 5): RA-3 and PM-9; NIST IR 8286; NIST IR 8286A; NIST IR 8286B; NIST IR 8286C; NIST IR 8286D; NIST CSF: ID.RM-1 – ID.RM-3; OMB A-123; OMB M-16-17; OMB M-23-03) (**Core**)[23]

   Managed and Measurable (Level 4)

   Comments: Based on the examination of the evidence, the Council has not fully integrated its organizational and business processes at all levels of the agency or established 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 risk remains at acceptable levels. However, we determined the Council is a micro-agency with

[21] Abbreviation: (EO): Executive Order.
[22] Abbreviations: (RA): Risk Assessment, (ID.BE): Identify – Business Environment, (ID.SC): Identify – Supply Chain Risk Management, (FIPS): Federal Information Processing Standards.
[23] Abbreviations: (ID.RM): Identify – Risk Management Strategy.

a unique organizational size and structure. As such, we assessed the maturity level as "Managed and Measurable."

6. To what extent does the organization use an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain (NIST SP 800-37 (Rev. 2): Task P-16; NIST SP 800-39; NIST SP 800-53 (Rev. 5): PL-8, SA-3, SA-8. SA-9, SA-12, and PM-9; NIST SP 800-160; NIST SP 800-163, (Rev. 1); NIST SP 800-218; NIST CSF: ID.SC-1 and PR.IP-2; FEA Framework; OMB M-15-14; OMB M-19-03; OMB M-22-18; SECURE Technology Act: s. 1326; Federal Information Technology Acquisition Reform Act (FITARA)) (**Supplemental**)[24]

   Consistently Implemented (Level 3)

   Comments: The Council has a small organizational structure, and other agencies manage all its information systems through interagency agreements except the Council's network, which is managed by the Chief Information Officer (CIO). As such, the maturity level was "Consistently Implemented."

10. To what extent does the organization use technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; NIST SP 800-207: Tenets 5 and 7; NIST IR 8286; OMB A-123; OMB M-22-09; CISA Zero Trust Maturity Model: Pillars 2-4; FY 2023 CIO FISMA Metrics: 7.4.2) (**Core**)

    Consistently Implemented (Level 3)

    Comments: The Council did not use advanced technologies to analyze trends and performance against benchmarks to continuously improve its cybersecurity risk management program. However, due to the Council's small organizational size the maturity level was "Consistently Implemented."

Supply Chain Risk Management – IDENTIFY FUNCTION

14. To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements (NIST SP 800-53 (Rev. 5): SA-4, SR-3, SR-5, and SR-6; NIST SP 800-152; NIST SP 800-161 (Rev. 1); NIST SP 800-218: Task PO.1.3; NIST IR 8276; NIST CSF: ID.SC-2 through ID.SC-4; OMB A-130; OMB M-19-03; OMB M-22-18; CIS Top 18 Security Controls: Control 15; The Federal Acquisition Supply Chain Security Act of 2018; FedRAMP standard contract clauses; Cloud computing contract best practices; DHS's ICT Supply Chain Library) (**Core**)[25]

[24] Abbreviations: (PL): Planning, (SA): System and Service Acquisition, (PR.IP): Protect – Information Protection Processes and Procedures, (SECURE): Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure.
[25] Abbreviations: (SR): Supply Chain Risk Management, (PO): Purchase Order, (FedRAMP): Federal Risk and Authorization Management Program, (ICT): Information and Communications Technology.

Managed and Measurable (Level 4)

Comments: We determined that the Council did not, on a near-real-time basis, analyze the impact of material changes to security and Supply Chain Risk Management assurance requirements on its relationships with external providers and ensure that acquisition tools, methods, and processes were updated as soon as possible. However, we determined the Council is a micro-agency with a unique organizational size and structure. As such, the maturity level was "Managed and Measurable."

15. To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization's systems (NIST SP 800-53 (Rev. 5): SR-11 (1)(2); NIST SP 800-161 (Rev. 1); OMB M-22-18; NIST SP 800-218) (**Supplemental**)

Managed and Measurable (Level 4)

Comments: We determined that the Council did not update its supply chain policies and processes on a near real-time basis as appropriate to respond to evolving and sophisticated threats. However, we determined the Council is a micro-agency with a unique organizational size and structure. As such, the maturity level was "Managed and Measurable."

Configuration Management – PROTECT FUNCTION

17. To what extent have the roles and responsibilities of configuration management stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced (NIST SP 800-53 REV. 5: CM-1; NIST SP 800-128: Section 2.4; Green Book: Principles 3, 4, and 5) (**Supplemental**)

Managed and Measurable (Level 4)

Comments: The Council did not continuously evaluate and adapt its configuration management-based roles and responsibilities to account for a changing cybersecurity landscape. However, given the unique structure of the Council, the maturity level was "Managed and Measurable."

18. To what extent does the organization use an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems (NIST SP 800-53 (Rev. 5): CM-9; NIST SP 800-128: Section 2.3.2) (**Supplemental**)[26]

Managed and Measurable (Level 4)

Comments: The Council did not utilize automation to adapt its configuration management plan and related processes and activities to a changing cybersecurity landscape on a near real-time

[26] Abbreviation: (SDLC): System Development Life Cycle.

basis. However, due to the unique organizational structure of the Council's information systems, the maturity level was "Managed and Measurable."

20. To what extent does the organization use configuration settings/common secure configurations for its information systems? (NIST SP 800-53 (Rev. 5): CM-6, CM-7, RA-5, and SI-2; NIST SP 800-70 (Rev. 4); NIST CSF: ID.RA-1 and DE.CM-8; NIST Security Measures for EO-Critical Software Use: SM 3.3; OMB M-22-09; OMB M-23-03; BOD 23-01; CIS Top 18 Security Controls: Controls 4 and 7; CISA Cybersecurity Incident Response Playbooks) (**Core**)[27]

    Managed and Measurable (Level 4)

    Comments: The Council did 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. However, due to the unique structure of the Council's information systems, the maturity level was "Managed and Measurable."

21. To what extent does the organization use flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management, to manage software vulnerabilities on all network addressable IP-assets (NIST SP 800-40 (Rev. 4); NIST SP 800-53 (Rev. 5): CM-3, RA-5, SI-2, and SI-3; NIST SP 800-207: Section 2.1; NIST CSF: ID.RA-1; NIST Security Measures for EO-Critical Software Use: SM 3.2; OMB M-22-09; FY 2023 CIO FISMA Metrics: 1.4, 8.1 and 8.2; CIS Top 18 Security Controls: Controls 4 and 7; BOD 18-02; BOD 19-02; BOD 22-01; BOD 23-01; BOD 23-01 Implementation Guidance; CISA Cybersecurity Incident Response Playbooks) (**Core**)

    Managed and Measurable (Level 4)

    Comments: The Council utilizes automated tools for the patch compliance and vulnerability scanning that generates monthly report summary to determine Council's compliance as well as it provide details of patch compliance for each device Council possess. The automated tool provided a dashboard view of the Council's open vulnerabilities (critical, high, medium) and if any ransomware had been detected. The automated tool helps the Council maintain an up-to-date, complete, accurate, and readily available view of the security configurations. Recognizing the unique size and structure of the Council's information systems, the Council's maturity level for this metric was "Managed and Measurable."

23. To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; evaluating and review of configuration changes; and coordination and

[27] Abbreviations: (SI): System and Information Integrity, (ID. RA): Identify – Risk Assessment, (DE.CM): Detect – Security Continuous Monitoring, (SM): Security Management.

oversight of changes by the CCB, as appropriate (NIST SP 800-53 (Rev. 5): CM-2, CM-3, and CM-4; NIST CSF: PR.IP-3) (**Supplemental**)

Managed and Measurable (Level 4)

Comments: The Council did not utilize automation to improve the accuracy, consistency, and availability of configuration change control and configuration baseline information. However, due to the unique structure of the Council's information systems, the maturity level was "Managed and Measurable."

Identity and Access Management – PROTECT FUNCTION

28. To what extent has the organization developed and implemented processes for assigning position risk designations and performing appropriate personnel screening prior to granting access to its systems (NIST SP 800-53 (Rev. 5): PS-2 and PS-3; NIST CSF: PR.IP-11; OMB M-19-17; National Insider Threat Policy; FY 2023 CIO FISMA Metrics: 7.4.3) (**Supplemental**)[28]

Consistently Implemented (Level 3)

Comments: The Council did not employ automation to centrally document, track, and share risk designations and screening information with necessary parties. However, due to the unique structure of the Council's information systems, the maturity level was "Consistently Implemented."

30. To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO2, or web authentication) for nonprivileged 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: 2.3.1, 2.3.2, 2.4, 2.9, 2.10, and 2.10.2) (**Core**)[29]

Managed and Measurable (Level 4)

Comments: Recognizing the unique size and structure of the Council's information systems, implementing an enterprise-wide single sign-on solution would require a significant financial investment. While such a solution would centralize non-privileged user accounts and privilege management, enabling near real-time reporting on effectiveness, the cost-benefits might not

[28] Abbreviation: (PS): Personal Security.

[29] Abbreviations: (PIV): Personal Identity Verification, (FIDO2) Fast Identity Online 2, (AC): Access Control, (IA): Identification and Authentication, (PE): Physical and Environment Protection, (PR.AC): Protect – Identity Management and Access Control, (HSPD) Homeland Security Presidential Directive.

justify the expense in the Council's specific environment. As such, the maturity level was "Managed and Measurable."

31. To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL) 3/Authenticator Assurance Level (AAL) 3 credential) for privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access (NIST SP 800-53 (Rev. 5): AC-17 and PE-3; NIST SP 800-63; NIST SP 800-128; NIST SP 800-157; NIST SP 800-207: Tenet 6; NIST CSF: PR.AC-1 and PR.AC-6; NIST Security Measures for EO-Critical Software Use: SM 1.1; FIPS 201-2; HSPD-12; OMB M-19-17; OMB M-22-09; OMB M-23-03; DHS ED 19-01; CIS Top 18 Security Controls: Control 6; FY 2023 CIO FISMA Metrics: 2.3, 2.4, 2.9, and 2.10) (**Core**)[30]

    Consistently Implemented (Level 3)

    Comments: Recognizing the unique size and structure of the Council's information systems, the Council does not have access to change Domain Name System (DNS) records. The Council does not have network resources requiring a DNS system. As such, the maturity level was "Consistently Implemented."

32. To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed? (NIST SP 800-53 (Rev. 5): AC-1, AC-2, AC-5, AC-6, AC-17, AU-2, AU-3, AU-6, and IA-4; NIST CSF PR.AC-4; NIST Security Measures for EO-Critical Software Use: SM 2.2; FY 2023 CIO FISMA Metrics: 3.1; OMB M-19-17; OMB M-21-31; DHS ED 19-01; CIS Top 18 Security Controls: Controls 5, 6, and 8) (**Core**)[31]

    Managed and Measurable (Level 4)

    Comments: The Council has not made progress towards implementing EL3's advanced requirements for user behavior monitoring to detect and alert privileged user compromise. However, due to the unique organizational structure of the Council's information systems, the maturity level was "Managed and Measurable."[32]

Data Protection and Privacy – PROTECT FUNCTION

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 (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

[30] Abbreviation: (ED): Emergency Directive.
[31] Abbreviation: (AU): Audit and Accountability.
[32] Abbreviation: (EL): Event Logging.

EO-Critical Software Use: SM 2.3 and SM 2.4; OMB M-22-09; DHS BOD 18-02; FY 2023 CIO FISMA Metrics: 2.1, 2.1.1 and 2.2; CIS Top 18 Security Controls: Control 3) (**Core**)[33]

Managed and Measurable (Level 4)

Comments: The Council did not employ advanced capabilities to enhance protective controls, including remote wiping, dual authorization for sanitization of media devices, exemption of media marking, and configuring systems to record the date the PII was collected, created, or updated and when the data is to be deleted or destroyed according to an approved data retention schedule. However, due to the unique structure of the Council's information systems, the maturity level was "Managed and Measurable."

37. To what extent has the organization implemented security controls (e.g., EDR) to prevent data exfiltration and enhance network defenses (NIST SP 800-53 (Rev. 5): SI-3, SI-7(8), SI-4(4)(18), SC-7(10), and SC-18; NIST CSF: PR.DS-5; NIST Security Measures for EO-Critical Software Use: SM 4.3; OMB M-21-07; OMB M-22-01; CIS Top 18 Security Controls: Controls 9 and 10; DHS BOD 18-01; DHS ED 19-01) (**Core**)

Managed and Measurable (Level 4)

Comments: The Council did not provide near real-time monitoring of the data that is entering and exiting the network and other suspicious inbound and outbound communications. Also, the Council did not continuously run device posture assessments to maintain visibility and analytics capabilities related to data exfiltration. However, due to the unique structure of the Council's information systems, the maturity level was "Managed and Measurable."

38. To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events? (NIST SP 800-53 (Rev. 5): IR-8 and IR-8(1); NIST SP 800-122; OMB M-17-12; OMB M-23-03; FY 2022 SAOP FISMA Metrics: Section 12) (**Supplemental**)[34]

Consistently Implemented (Level 3)

Comments: The Council conducted tabletop exercises to review the effectiveness of its Data Breach Response Plan; however, the Council has not suffered from a breach as such, they have not monitored and analyzed qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan. Recognizing the unique size and structure of the Council's information system, as such, the maturity level was "Consistently Implemented."

39. To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training (NIST SP 800-53 (Rev. 5): AT-1, AT-2, AT-3, and PL-4; FY 2022 SAOP FISMA Metrics: Section 9, 10, and 11) (**Supplemental**)[35]

[33] Abbreviation: (PII): Personally Identifiable Information, (SC): System and Communication Protection, (PR.DS): Protect – Data Security, (PR.PT): Protect – Protective Technology, (MP): Media Protection.
[34] Abbreviations: (IR): Incident Response, (SAOP): Senior Agency Official for Privacy.
[35] Abbreviation: (AT): Awareness Training.

(Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements)

Optimized (Level 5)

Comments: The Council has institutionalized a process of continuous improvement incorporating advanced privacy training practices and technologies. As such the maturity level was "Optimized."

Security Training – PROTECT FUNCTION

42. To what extent does the organization use an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover (NIST SP 800-50: Section 3.2; NIST SP 800-53 (Rev. 5): AT-2, AT-3, and PM-13; NIST SP 800-181; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework; CIS Top 18 Security Controls: Control 14; FY 2023 CIO FISMA Metrics: 6.1; EO 13870) (**Core**)

Managed and Measurable (Level 4)

Comments:The CIO updates security training based on the assessment of the knowledge, skills, and abilities of the workforce and these trainings are tailored to the workforce and are updated quarterly. However, the Council did not employ trend analysis that could demonstrate that security incidents resulting from personnel actions or inactions are being reduced over time. Recognizing the unique size and structure of the Council's information systems, the maturity level was "Managed and Measurable."

44. To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems (Note: awareness training topics should include, as appropriate, consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting) (NIST SP 800-50: 6.2; NIST SP 800-53 (Rev. 5): AT-1 and AT-2; NIST CSF: PR.AT-2; CIS Top 18 Security Controls: Control 14) (**Supplemental**)[36]

Optimized (Level 5)

Comments: The Council has institutionalized a process of continuous improvement incorporating advanced security awareness practices and technologies. On a near real-time basis (as determined by the agency given its threat environment), the Council actively adapted its security awareness policies, procedures, and processes to a changing cybersecurity

[36] Abbreviation: (PR.AT): Protect – Access Training.

landscape. It provided awareness and training, as appropriate, on evolving and sophisticated threats. As such, the maturity level was "Optimized."

45. To what extent does the organization ensure that specialized security training is provided to individuals with significant security responsibilities (as defined in the organization's security policies and procedures and in accordance with 5 Code of Federal Regulation 930.301) (NIST SP 800-53 (Rev. 5): AT-3 and AT-4; EO 13870; 5 Code of Federal Regulation 930.301) (**Supplemental**)

    Optimized (Level 5)

    Comments: The Council has institutionalized a process of continuous improvement incorporating advanced security training practices and technologies. On a near real-time basis, the Council actively adapted its security training policies, procedures, and processes to a changing cybersecurity landscape. It provided awareness and training, as appropriate, on evolving and sophisticated threats. As such, the maturity level was "Optimized."

Information Security and Continuous Monitoring – DETECT FUNCTION

47. To what extent does the organization use information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier (NIST SP 800-37 (Rev. 2): Task P-7; NIST SP 800-53 (Rev. 5): CA-7, PM-6, PM-14, and PM-31; NIST SP 800-137: Sections 3.1 and 3.6; NIST Security Measures for EO-Critical Software Use: SM 4.2; CIS Top 18 Security Controls: Control 13) (**Core**)

    Managed and Measurable (Level 4)

    Comments: It was not necessary to use its ISCM policies and strategy to reduce costs and increase the efficiency of security and privacy programs. Recognizing the unique size and structure of the Council's information systems, the maturity level for this metric was "Managed and Measurable."

49. How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls (NIST SP 800-18 (Rev. 1); NIST SP 800-37 (Rev. 2): Task S-5; NIST SP 800-53 (Rev. 5): CA-2, CA-5, CA-6, CA-7, PL-2, and PM-10; NIST SP 800-137: Section 2.2; NIST IR 8011; NIST IR 8397; OMB A-130; OMB M-14-03; OMB M-19-03; OMB M-22-09; FY 2023 CIO FISMA Metrics: 7.1) (**Core**)

    Managed and Measurable (Level 4)

    Comments: It was not necessary to use its ISCM policies and strategy to reduce costs and increase the efficiency of security and privacy programs. Recognizing the unique size and structure of the Council's information systems, the Council's maturity level for this metric was "Managed and Measurable."

50. How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137) (**Supplemental**)

Managed and Measurable (Level 4)

Comments: The Council did not actively adapt its Information Security Continuous Monitoring program to the evolving cybersecurity landscape or respond to increasingly sophisticated threats in a timely manner. However, the Council has established procedures and processes for continuous monitoring, providing some level of situation awareness across various organizational areas. Even with this gap in adapting to changing threats, due to the unique size and structure of the Council's information systems, the maturity level was "Managed and Measurable."

Incident Response– RESPOND FUNCTION

52. To what extent does the organization use an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents (NIST SP 800-53 (Rev. 5): IR-8; NIST SP 800-61 (Rev. 2): Section 2.3.2; NIST CSF: RS.RP-1; Presidential Policy Directive (PPD) 8 – National Preparedness; FY 2023 CIO FISMA Metrics: 10.1.1; FY 2022 CIO FISMA Metrics: 10.6) (**Supplemental**)[37]

Consistently Implemented (Level 3)

Comments: While the Council had not experienced any incidents and they had not collected any qualitative and quantaive performance measures, we still assessed their matrity level for this metric to be "Consistently Implemented" due to the unique size and structure of the Council's information systems.

53. To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization (NIST SP 800-53 (Rev. 5) IR-7; NIST SP 800-61 (Rev. 2); NIST SP 800-83; NIST CSF: RS.CO-1; OMB M-20-04; US-CERT Federal Incident Notification Guidelines; Green Book: Principles 3, 4, and 5) (**Supplemental**)[38]

Managed and Measurable (Level 4)

Comments: The Council did not continuously evaluate and adapt its incident response-based roles and responsibilities to account for a changing cybersecurity landscape. Recognizing the unique size and structure of the Council's information systems, the Council's maturity level for this metric was "Managed and Measurable."

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:

[37] Abbreviation: (RS.RP): Response Planning.
[38] Abbreviations: (RS.CO): Recover Communications, (US-CERT): United States Computer Emergency Readiness Team.

Control 17; US-CERT Federal Incident Notification Guidelines; FY 2023 CIO FISMA Metrics: 3.1, 10.4, 10.5, and 10.6) (**Core**)[39]

Managed and Measurable (Level 4)

Comments: The Council did not demonstrate progress toward implementing EL3's (advanced) requirements for its logging capabilities. Recognizing the unique size and structure of the Council's information systems, the Council's maturity level for this metric was "Managed and Measurable."

55. How mature are the organization's processes for incident handling (O (Rev. NIST SP 800-53 (Rev. 5): IR-4; NIST SP 800-61 (Rev. 2); NIST IR 8374; NIST CSF: RS.MI-1 and RS.MI-2; OMB M-21-31; OMB M-23-03; CISA Cybersecurity Incident Response Playbooks; FY 2023 CIO FISMA Metrics: 10.4, 10.5, and 10.6) (**Core**)[40]

Consistently Implemented (Level 3)

Comments: The Council did not experience any incidents in FY 24, and hence, we cannot validate if the Council 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. Recognizing the unique size and structure of the Council's information systems, the Council's maturity level for this metric was "Consistently Implemented."

56. To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; NIST SP 800-53 (Rev. 5): IR-6; NIST CSF: RS.CO-2 through RS.CO-5; OMB M-20-04; US-CERT Federal Incident Notification Guidelines; PPD-41; DHS Cyber Incident Reporting Unified Message) (**Supplemental**)[41]

Consistently Implemented (Level 3)

Comments: The Council has not experienced any incidents in FY 24. Third parties managed the Council's incident response. Since no incidents were reported, we cannot determine whether the Council's Incident response metrics were used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders. As such, the maturity level was "Consistently Implemented."

Contingency Planning– RECOVER FUNCTION

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

[39] Abbreviations: (DE.AE): Detect – Anomalies and Events, (RS.AN): Respond – Analysis.
[40] Abbreviations (RS.MI): Respond – Mitigation.
[41] Abbreviation: (PPD): Presidential Policy Directive.

SP 800-53 (Rev. 5): CP-2 and RA-9; NIST IR 8179; NIST IR 8286; NIST IR 8286D; NIST CSF: ID.RA-4; FIPS 199; FCD-1; FCD-2; OMB M-19-03) (**Core**)[42]

Managed and Measurable (Level 4)

Comments: The Council ensured that the results of organizational and system-level BIAs are integrated with enterprise risk management processes and in conjunction with its risk register. Recognizing the unique size and structure of the Council's information systems, the Council's maturity level for this metric was "Managed and Measurable."

62. To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST SP 800-34; NIST SP 800-53 (Rev. 5) CP-2; NIST CSF: PR.IP-9; FY 2023 CIO FISMA Metrics: 10.1.2, 10.2, and 10.3; OMB M-19-03) (**Supplemental**)

Consistently Implemented (Level 3)

Comments: The Council did not integrate metrics on the effectiveness of its information systems contingency plans with information on the effectiveness of related plans, such as organization and business process continuity, disaster recovery, incident management, insider threats, and occupant emergency, as appropriate to deliver persistent situation awareness across the organization. As such, the maturity level was "Consistently Implemented."

63. To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST SP 800-34; NIST SP 800-53 (Rev. 5): CP-3 and CP-4; NIST CSF: ID.SC-5 and PR.IP-10; CIS Top 18 Security Controls: Control 11) (**Core**)

Consistently Implemented (Level 3)

Comments: The Council system is rated low risk and has a unique organizational structure and a simplified system. Therefore, an automated system is not required to test contingency plans. Recognizing the unique size and structure of the Council's information systems, the Council's maturity level for this metric was "Consistently Implemented."

64. To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST SP 800-34: Sections 3.4.1 through 3.4.3; NIST SP 800-53 (Rev. 5): CP-6, CP-7, CP-8, CP-9, and CP-10; NIST SP 800-209; NIST CSF: PR.IP-4; FCD-1; FY 2023 CIO FISMA Metrics: 10.3.1 and 10.3.2; NIST Security Measures for EO-Critical Software Use: SM 2.5) (**Supplemental**)

Consistently Implemented (Level 3)

[42] Abbreviations: (CP): Contingency Planning, (FCD): Federal Continuity Directive.

Comments: The Council has no alternate processing facility established, and the backup data is the responsibility of the third-party provider. Recognizing the unique size and structure of the Council's information systems, the Council's maturity level for this metric was "Consistently Implemented."

Appendix II: Management's Response

Gulf Coast Ecosystem Restoration Council

July 22, 2024

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 2024

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 2024.

The Council agrees with the results of the evaluation for Fiscal Year 2024 that the Council's information security program and practices were effective for the period April 1, 2023 through March 31, 2024. The Council works to ensure compliance with the five Cybersecurity Functions defined by NIST and the nine FISMA Metric domains defined by OMB and CISA.

In Fiscal Year 2025, 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: 2024.07.22 10:10:07 -05'00'

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/