Evaluation Report

OIG-CA-22-018

GULF COAST RESTORATION

The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2022

August 15, 2022

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

August 15, 2022

MEMORANDUM FOR MARY WALKER, EXECUTIVE DIRECTOR
GULF COAST ECOSYSTEM RESTORATION COUNCIL

FROM: Larissa Klimpel /s/
Director, Cyber/Information Technology Audit

SUBJECT: Evaluation Report – *The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation for Fiscal Year 2022* (OIG-CA-22-018)

We hereby transmit the attached report, *The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2022*, dated August 15, 2022. 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 July 1, 2021 through March 31, 2022. 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 Functions and nine FISMA Metric Domains. RMA found that the Council's information security program and practices were effective for the period July 1, 2021 through March 31, 2022.

Appendix I of the attached RMA report includes the *Fiscal Year 2022 Core Inspector General Metrics.*

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

Attachment

RMA | Associates
Auditors. Consultants. Advisors.

The Gulf Coast Ecosystem Restoration Council
Federal Information Security Modernization Act of 2014

Evaluation Report for Fiscal Year 2022

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-660
www.rmafed.com

August 11, 2022

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 2022

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) 2022. 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 July 1, 2021, through March 31, 2022.

Beginning with the FY 2022 FISMA period, the Office of Management and Budget (OMB) identified 20 Core Inspector General Metrics (FY 2022 Core IG Metrics) in its *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*, of which IGs were required to assess the maturity levels. As part of our audit, we evaluated the FY 2022 Core IG Metrics and assessed the maturity levels on behalf of the Department of the Treasury Office of Inspector General as shown in Appendix I. These metrics provide reporting requirements across functional areas to be addressed in the independent assessment of agencies' information security programs.

In summary, we found the Council's information security program and practices were effective for the period July 1, 2021, through March 31, 2022.

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

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

Table of Contents

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

Abbreviations

AAL	Authenticator Assurance Level
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
ARC	Administrative Resource Center
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BOD	Binding Operational Directive
BYOD	Bring Your Own Device
CA	Assessment, Authorization, and Monitoring
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CM	Configuration Management
COOP	Continuity of Operations Plan
Council	Gulf Coast Ecosystem Restoration Council
CP	Contingency Planning
CSF	Cybersecurity Framework
DE.AE	Detect – Anomalies and Events
DE.CM	Detect – Security Continuous Monitoring
DHS	Department of Homeland Security
DNS	Domain Name System
ED	Emergency Directive
EO	Executive Order
ERM	Enterprise Risk Management
FCD	Federal Continuity Directive
FEA	Federal Enterprise Architecture
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
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.RA	Identify – Risk Assessment
ID.RM	Identify – Risk Management Strategy
ID.SC	Identify – Supply Chain Risk Management
IG	Inspector General
ISCM	Information Security Continuous Monitoring

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

ISCP	Information System Contingency Planning
IR	Incident Response
IT	Information Technology
NFC	National Finance Center
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency or Internal Report
MERLIN	Metadata Records Library and Information Network
MFA	Multifactor Authentication
MP	Media Protection
OIG	Office of Inspector General
OMB	Office of Management and Budget
OS	Operating System
OSN	Office Support Network
PE	Physical and Environment Protection
PII	Personally Identifiable Information
PIPER	Program Information Platform for Ecosystem Restoration
PIV	Personal Identity Verification
PM	Program Management
P.L.	Public Law
PL	Planning
POA&M	Plan of Action and Milestones
PR.AC	Protect – Identity Management and Access Control
PR.DS	Protect – Data Security
PR.IP	Protect – Information Protection Processes and Procedures
PR.PT	Protect – Protective Technology
RA	Risk Assessment
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
SA	System and Service Acquisition
SCRM	Supply Chain Risk Management
SI	System and Information Integrity
SC	System and Communication Protection
SP	Special Publication
SR	Supply Chain Risk Management
TIC	Trusted Internet Connection
Treasury	Department of the Treasury

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
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 results of the evaluations 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 (Treasury) Office of Inspector General (OIG) engaged RMA Associates, LLC (RMA) to conduct an annual evaluation of the Council's information security program and practices in support of the FISMA evaluation requirement. The objective of this evaluation was to evaluate the effectiveness of the Council's information security program and practices for the period July 1, 2021, through March 31, 2022.

As part of our evaluation, we responded to the fiscal year (FY) 2022 Core Inspector General Metrics (FY 2022 Core IG Metrics) specified in OMB's *FY 2022 Core IG Metrics Implementation Analysis and Guidelines* (issued on April 13, 2022).Our responses to the 20 Core IG Metrics, which align to questions from DHS' *Fiscal Year (FY) 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.1* (May 12, 2021), are provided in Appendix I: *Fiscal Year 2022 Core Inspector General Metrics*. These core metrics provide reporting requirements across the functional areas to be addressed in the independent assessment of agencies' information security programs.[2] See *Objective, Scope, and Methodology* for more detail. We also considered applicable OMB policy and guidelines, and the National Institute of Standards and Technology (NIST) standards and guidelines.

This evaluation was performed in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) *Quality Standards for Inspection and Evaluation*, issued in December 2020.

Summary Evaluation Results

We concluded that consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, the Council's information security program and practices were

[1] Public Law (P.L.) 113-283, Federal Information Security Modernization Act of 2014 (Dec. 18, 2014).
[2] Per OMB Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements* (December 6, 2021), the timeline for the Inspector General (IG) evaluation of agency effectiveness was adjusted to align the results of the evaluation with the budget submission cycle. Representatives from OMB, the Federal Civilian Executive Branch Chief Information Security Officers, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and the Intelligence Community agreed that the 20 Core IG Metrics should provide sufficient data to determine the effectiveness of an agency's information security program with a high level of confidence. For additional details please refer to the "Key Changes to the Metrics" in Appendix I.

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

established and maintained for the five Cybersecurity Functions[3] and nine FISMA Metric Domains.[4] The overall maturity level of the Council's information security program was determined to be Managed and Measurable, as described in this report. Accordingly, we found the Council's information security program and practices were effective for the period July 1, 2021, through March 31, 2022.

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

Background

Gulf Coast Ecosystem Restoration Council

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

In addition to creating the Trust Fund, the RESTORE Act established the Council. The Council is comprised of a Chairperson from a member Federal agency and includes the Governors of the States of Alabama, Florida, Louisiana, Mississippi, and Texas, and the Secretaries or designees of the U.S. Departments of Agriculture, the Army, Commerce, Homeland Security, and the Interior, and the Administrator of the U.S. Environmental Protection Agency.

The Council's information system infrastructure consists of an Office Support Network (OSN) and eight system service providers. The Council's OSN is technically not a computer network as it did not include any 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 (TIC) portal.

[3] OMB, DHS, and CIGIE developed the FISMA Reporting Metrics in consultation with the Federal Chief Information Officers Council. The nine FISMA Metric Domains were aligned with the five functions: (1) identify, (2) protect, (3) detect, (4) respond, and (5) recover as defined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.

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

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

The Council's unclassified cloud-based systems and functions include:

1. For payroll processing, WebTA (hosted by the U.S. Department of Agriculture's National Finance Center (NFC));[5]
2. For financial management and report processing, the Administrative Resource Center (ARC) (hosted by Treasury's Bureau of the Fiscal Service);
3. For program data management, Program Information Platform for Ecosystem Restoration (PIPER) and the Council website (hosted by U.S. Geological Survey);
4. For metadata, Metadata Records Library and Information Network (MERLIN)[6] (hosted by U.S. Geological Survey);
5. For award management, GrantSolutions (hosted by U.S. Department of Health and Human Services);
6. For email and G Suite,[7] Google Office (hosted by National Oceanic and Atmospheric Administration);
7. For continuous diagnostic monitoring and EINSTEIN[8] capabilities (hosted by DHS); and
8. For electronic records management, Electronic Record Archives (hosted by National Archives and Records Administration).

Federal Information Security Modernization Act of 2014

Title III of the *E-Government Act*, entitled the *Federal Information Security Management Act of 2002*, required each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources. FISMA amended the *Federal Information Security Management Act of 2002* and provided several modifications that modernize Federal security practices to address evolving security concerns. These changes resulted in less overall reporting, strengthened use of continuous monitoring in systems, and increased focus on the agencies for compliance and reporting that is more concentrated on the issues caused by security incidents.

FISMA, along with the *Paperwork Reduction Act of 1995* and the *Information Technology Management Reform Act of 1996* (known as the Clinger-Cohen Act), explicitly emphasizes a risk-based policy for cost-effective security. In support of and reinforcing this legislation, OMB, through Circular No. A-130, *Managing Federal Information as a Strategic Resource*, requires executive agencies within the Federal government to:

- Plan for security;
- Ensure that appropriate officials are assigned security responsibility;
- Periodically review the security controls in their systems; and

[5] During FY 2022 the Council completed the transition of the service provider for WebTA from NFC to ARC.
[6] MERLIN is an online metadata records application that assists award recipients in submitting required metadata records that describe observational data collected and provides a catalogue of these records for stakeholders.
[7] G Suite is a suite of collaborative productivity applications that offers business professional email, shared calendars, online document editing, storage, and video meetings.
[8] EINSTEIN is a system the Cybersecurity and Infrastructure Security Agency employs to provide a common baseline of security across the Federal Civilian Executive Branch and to help agencies manage their cyber risk.

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

- Authorize system processing prior to operations and periodically after that.

These management responsibilities presume responsible agency officials understand the risks, and other factors, which could adversely affect their missions. Moreover, these officials must understand the current status of their security programs, and the security controls planned or in place, to protect their information and systems to make informed judgments and investments which appropriately mitigate risk to an acceptable level. The ultimate objective is to conduct the day-to-day operations of the agency and to accomplish the agency's stated missions with adequate security or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems.

NIST developed an integrated Risk Management Framework which effectively brings together all the FISMA-related security standards and guidance to promote the development of a comprehensive and balanced information security program by agencies.

FY 2022 Core IG Metrics

OMB's *FY 2022 Core IG Metrics Implementation Analysis and Guidelines* specified the 20 FY 2022 Core IG Metrics (refer to Appendix I) and directed IGs to report the assessed maturity levels of these metrics in CyberScope no later than July 30, 2022. The FY 2022 Core IG Metrics were aligned with the five Cybersecurity Framework security functions areas (key performance areas) as follows:

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

We evaluated the effectiveness of 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 2022 Core IG Metrics classify information security programs and practices into five maturity model levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized. Within the context of the maturity model, Level 4, Managed and Measurable, represents an effective level of security.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
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 July 1, 2021, and March 31, 2022. It consisted of testing the 20 Core IG Metrics as shown in Appendix I, which reflects the results of our assessment of the Council's information security program and practices.

Evaluation Results

We determined the maturity level for each FISMA domain based on the responses to the 20 questions in the FY 2022 Core IG Metrics and testing for each domain. The Council's information technology (IT) controls, processes, and personnel did not change since the prior year's FISMA evaluation. We also considered the Chief Information Officer (CIO) was closely involved in all aspects of the Council's IT environment and was aware of every important decision regarding the Council's IT operations. The overall maturity level of the Council's information security program was determined as Managed and Measurable based upon a simple majority of the component scores for each domain's maturity level, and due to the CIO's direct involvement in every IT security decision, his direct oversight of security controls, and the simple IT structure of stand-alone laptops and service vendors. Our tests of effectiveness found no exceptions.

Below is the maturity level for each domain.

Risk Management: We determined the Council's overall maturity level for the Risk Management program was Managed and Measurable. The Council defined the priority levels for the Office Support Network (OSN) and considered risks from the supporting business functions and mission impacts to help its leadership make informed risk management decisions. Those informed risk management decisions helped continually improve and update the Council's risk management policies, procedures, and strategy, including methodologies for categorizing risk, developing a risk profile, assessing risk, determining risk appetite/tolerance levels, responding to risk, and monitoring risk. Our testing found no exceptions, and the controls were operating as intended. We concluded the Council's Risk Management program controls in place were effective.

Supply Chain Risk Management: We determined the Council's overall maturity level for the SCRM program was Ad Hoc. Although the Council had defined supply chain policies and procedures, the Council did not define the minimum components as required by Question 14 of the FY 2022 Core IG Metrics (see Appendix I). The Council managed its supply chain risks by

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

purchasing products from trusted and approved manufacturers. The Council's OSN is considered a server-less network with a *Federal Information Processing Standards Publication* (FIPS) 199 rating of 'low.'[9] Although the maturity level of this domain was Ad Hoc, our testing found no exceptions, and the controls were operating as intended. The Council only has a single IT vendor with limited operating machines. Hence, the Council has limited SCRM risks. We concluded the Council's SCRM program controls in place were effective.

Configuration Management: We determined the Council's overall maturity level for the Configuration Management program was Managed and Measurable. The Council's laptops were connected to a local network and its primary configuration management considerations were related to the standard configuration of their laptops. Our testing found no exceptions, and the controls were operating as intended. We concluded the Council's Configuration Management program controls in place were effective.

Identity and Access Management: We determined the Council's overall maturity level for the Identity and Access Management program was Managed and Measurable. The Council had to manage 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 can only be made on local machines. All accounts are local accounts that are not shared and can only be modified by a privileged user logging into each machine. The Council did not use automated tools to inventory and manage accounts and perform segregation of duties/least privilege reviews. Our testing found no exceptions, and controls were operating as intended. We concluded the Council's Identity and Access Management program controls in place were effective.

Data Protection and Privacy: We determined the Council's overall maturity level for the Data Protection and the Privacy program was Consistently Implemented. The Council did not process Personally Identifiable Information (PII) data as PII needed for human resources and payroll were handled through agreements with ARC and WebTA. Their systems were approved to collect and process PII. Controls over PII were the responsibility of the Council's outsourced service providers. Therefore, the Council did not monitor and analyze quantitative and qualitative performance measures on the effectiveness of its privacy activities and use the information to make needed adjustments that were necessary to reach the Managed and Measurable level. Although the maturity level of this domain was Consistently Implemented, our control testing found no exceptions, and the controls were operating as intended. We concluded the Council's Data Protection and Privacy program controls were effective.

Security Training: We determined the Council's overall maturity level for the Security Training program was Managed and Measurable. The Council has addressed its identified knowledge, skills, and abilities gaps through talent acquisition. Our testing of the Council's workforce

[9] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, states that a potential impact on organizations or individuals is 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.

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

assessment found no exceptions, and controls were operating as intended. We concluded the Council's Security Training program controls in place were effective.

Information Security and Continuous Monitoring: We determined the Council's overall maturity level for the ISCM program was Managed and Measurable. The Council has a unique organizational structure and the Council relies on third-party service providers, for its ISCM capabilities. Decisions regarding IT operations were made with the direct involvement and approval of the Council's CIO, allowing leadership to monitor and analyze the effectiveness of its ISCM program. Our testing found no exceptions, and the controls were operating as intended. We concluded the Council's ISCM program controls in place were effective.

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

Contingency Planning: We determined the Council's overall maturity level for the Contingency Planning program was Consistently Implemented. Given the Council did not own any network servers, it developed policies and procedures for Contingency Planning which were consistently implemented but did not develop quantitative and qualitative effectiveness measures necessary to reach the Managed and Measurable level. As the Council's systems, with the exception of OSN, were managed by third-party providers, controls such as quantitative and qualitative measures to reach the Managed and Measurable maturity level were the responsibility of the third-party providers. Although the maturity level of this domain was Consistently Implemented, our control testing for this domain found no exceptions, and the controls were operating as intended. We concluded the Council's Contingency Planning program 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 had been maintained for the five Cybersecurity Functions and nine FISMA Metric Domains. We found the Council's information security program and practices were effective for the period July 1, 2021, through March 31, 2022, and the overall maturity level of the Council's information security program was Managed and Measurable.

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

Objective, Scope, and Methodology

Objective

The objective of this evaluation was to determine the effectiveness of the Gulf Coast Ecosystem Restoration Council's (Council) information security program and practices for the period of July 1, 2021, through March 31, 2022.

Scope

The scope of our work included the Council's Office Support Network (OSN) and the following unclassified cloud-based systems and functions supported by third-party providers:

1. For payroll processing, WebTA (hosted by the U.S. Department of Agriculture's National Finance Center (NFC));[10]
2. For financial management and report processing, the Administrative Resource Center (ARC) (hosted by Treasury's Bureau of the Fiscal Service);
3. For program data management, Program Information Platform for Ecosystem Restoration (PIPER) and the Council website (hosted by U.S. Geological Survey);
4. For metadata, Metadata Records Library and Information Network (MERLIN) (hosted by U.S. Geological Survey);
5. For award management, GrantSolutions (hosted by U.S. Department of Health and Human Services);
6. For email and G Suite, Google Office (hosted by National Oceanic and Atmospheric Administration);
7. For continuous diagnostic monitoring and EINSTEIN capabilities (hosted by DHS); and
8. For electronic records management, Electronic Record Archives (hosted by National Archives and Records Administration).

The Council's OSN is technically not a computer network as it did not include any 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. Our evaluation scope covered the period between July 1, 2021, and March 31, 2022.

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

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

[10] During FY 2022 the Council completed the transition of the service provider for WebTA from NFC to ARC.

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

- Recover, which includes questions pertaining to Contingency Planning.

As part of our audit, we evaluated and responded to the 20 Fiscal Year (FY) 2022 Core Inspector General (IG) Metrics specified by the Office of Management and Budget (OMB) in the *FY 2022 Core IG Metrics Implementation Analysis and Guidelines* (issued on April 13, 2022). These metrics align to the Department of Homeland Security's (DHS) *Fiscal Year (FY) 2021 IG Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.1* (May 12, 2021). We assessed the maturity levels on behalf of the Treasury Office of Inspector General. See Appendix I for details of the FY 2022 Core IG Metrics.

Methodology

The overall strategy of our evaluation considered the following: (1) the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations;* (2) NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations;* (3) FY 2022 Core IG 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 20 FY 2022 Core IG Metrics, we indicated whether each maturity level was achieved by the Council by stating "MET" or "NOT MET." We determined the overall maturity level of each of the nine domains by a simple majority of the component scores of the maturity level of each question within the domain, in accordance with the FY 2022 Core IG Metrics. Appendix I shows the FISMA questions followed by the narrative of the maturity level, the criteria, and our test procedures.

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

In testing for the effectiveness of the security controls relevant to the 20 Core IG Metrics specified in OMB's *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*, we tested the entire population of administrative controls of the Council. The application controls were the responsibility of the Council's service providers.

We conducted the FISMA evaluation in accordance with the CIGIE's *Quality Standards for Inspection and Evaluation* (issued in December 2020); and other evaluation requirements contained in the following: (1) OMB Circular No. A-130, *Managing Information as a Strategic Resource*; (2) OMB Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*; (3) NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations dated September 23, 2020;* (4) NIST *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1,* (dated April 16, 2018), and (5) FY 2022 Core IG Metrics criteria.

We based our FY 2022 FISMA evaluation approach on Federal information security guidelines developed by NIST, OMB, and the Council. NIST SPs provide guidelines considered essential to

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

developing and implementing the Council's security programs. We applied the following criteria in performing the Council's FY 2022 FISMA evaluation:

NIST Federal Information Processing Standards (FIPS) Publications 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*
- 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 3, *Guide to Enterprise Patch Management Technologies*
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*
- NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*
- NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*
- NIST SP 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide*
- NIST SP 800-63-3, *Digital Identity Guidelines*
- NIST SP 800-83, Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*
- NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*
- NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*
- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
- NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
- NIST SP 800-181, Revision 1, *Workforce Framework for Cybersecurity* (*NICE Framework)*

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

- NIST Interagency Report 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*

OMB Policy Directives

- OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*
- OMB Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*
- OMB Memorandum M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*
- OMB Memorandum M-21-30, *Protecting Critical Software Through Enhanced Security Measures*
- OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*
- 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 (CISP) for the Federal Civilian Government*
- OMB Circular No. A-130, *Managing Information as a Strategic Resource*
- OMB *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*

DHS Directives and Other Guidance

- DHS Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*
- DHS Emergency Directive 21-04, *Mitigate Windows Print Spooler Service Vulnerability*
- DHS Emergency Directive 21-03, *Mitigate Pulse Connect Secure Product Vulnerabilities*
- DHS Emergency Directive 21-02, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*
- DHS Emergency Directive 21-01, *Mitigate SolarWinds Orion Code Compromise*
- DHS Emergency Directive 20-04, *Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday*

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

- 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 Binding Operational Directive 20-01, *Develop and Publish Vulnerability Disclosure Policy*
- DHS Binding Operational Directive 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*
- DHS Emergency Directive 19-01, *Mitigate DNS Infrastructure Tampering*
- DHS Binding Operational Directive 18-02 *Securing High-Value Assets*
- DHS Binding Operational Directive 18-01, *Enhance Email and Web Security*
- DHS Binding Operational Directive 17-01, *Removal of Kaspersky-branded Products*
- DHS Binding Operational Directive 16-03, *2016 Agency Cybersecurity Reporting Requirements*
- DHS Binding Operational Directive 16-02, *Threat to Network Infrastructure Devices*

Council

- IT-Provided by Client-01 Council Information Technology Policy and Procedures (May 18, 2021)

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

Appendix I: Fiscal Year 2022 Core Inspector General Metrics

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

***Key Changes to the Metrics**

One of the annual Federal Information Security Modernization Act of 2014 (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) Office of the Federal Chief Information Officer published the 20 Fiscal Year (FY) Core Inspector General (IG) Metrics in the *FY 2022 Core IG Metrics Implementation Analysis and Guidelines* (issued on April 13, 2022), which is geared towards those priorities. OMB also issued Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements* (December 6, 2021), which provides guidance on Federal Information Security and Privacy Management Requirements. The metrics are based on coordinated discussions between, and the consensus opinion of, representatives from OMB, Council of the Inspectors General on Integrity and Efficiency (CIGIE), Federal Civilian Executive Branch Chief Information Security Officers, and their staff, and the Intelligence Community. Research, interviews, and Inspector General (IG) survey data provided quantitative and qualitative information to formulate these guidelines. The core metrics consist of 20 out of 66 FISMA questions from the Department of Homeland Security's (DHS) *Fiscal Year (FY) 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.1* (May 12, 2021). The FY 2022 Core IG Metrics were chosen based on alignment with Executive Order (EO) 14028 (May 12, 2021), *Improving the Nation's Cybersecurity,* as well as recent OMB guidance to agencies in furtherance of the modernization of Federal cybersecurity, including:

- *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (M-22-09) (January 26, 2022) – OMB and the Cybersecurity & Infrastructure Security Agency (CISA) solicited public feedback on strategic and technical guidance documents meant to move the U.S. government towards a zero-trust architecture. OMB's Federal Zero Trust Strategy aims to accelerate agencies towards a baseline of early zero trust maturity.
- Multifactor Authentication (MFA) and Encryption (EO 14028) (May 12, 2021) – Per the EO, agencies were required to fully adopt MFA and encryption for data at rest and in transit by November 8, 2021. For agencies that were unable to meet these requirements within 180 days of the date of the order, the agency head was directed to provide a written rationale to the Secretary of Homeland Security through the Director of CISA, the Director of OMB, and the Assistant to the President and National Security Advisor.
- *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (M-21-31) (August 21, 2021) – This memorandum provided specific requirements for log management, log retention with a focus on ensuring centralized access and visibility for the highest-level enterprise security operations center of each agency. It includes a maturity model for event log management, agency implementation requirements, and government-wide responsibilities.
- *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* (M-22-01) (October 8, 2021) – This memorandum was issued for agencies to focus on improving early detection capabilities, creating "enterprise-level visibility" across components and sub-agencies, and requires agencies to deploy an Endpoint Detection and Response solution.

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

- *FY 2022 Core IG Metrics Implementation Analysis and Guidelines* (issued on April 13, 2022), *Software Supply Chain Security & Critical Software* – Section 4 of EO 14028 tasks OMB, National Institute of Standards and Technology (NIST), and other Federal entities with developing new guidelines and frameworks to improve the security and integrity of the technology supply chain. In collaboration with industry and other partners, this effort provides frameworks and guidelines on how to assess and build secure technology, including open-source software.

Additionally, OMB Memorandum M-22-05 *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements* (December 6, 2021), adjusts the timeline for the IG evaluation of agency effectiveness to align the results of the evaluation with the budget submission cycle. Historically, the evaluation of agency effectiveness by IGs finished in October. However, the FY 2022 IG evaluation completion deadline has shifted from October to July to better align the release of IG assessments with the development of the President's Budget as noted in OMB M-22-05. The previous timeline limited agency leadership's ability to request resources in the next Budget Year submissions to provide for remediation. The expectation is this change will reduce the time between issue identification, resource request, and allocation.

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

FY 2022 Core IG Metrics

OMB developed the FY 2022 Core IG Metrics by selecting 20 of the 66 FISMA questions from DHS' *Fiscal Year (FY) 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.1* (May 12, 2021).[11] For ease of mapping, the same question numbers were used for the FY 2022 Core IG Metrics as follows:

Identify – Risk Management

- Question 1: Information Technology (IT) Inventory, which supports Zero trust requirements of M-22-05
- Question 2: Asset Management – Hardware Inventory Listing
- Question 3: Asset Management – Software Inventory Listing
- Question 5: System-Level Risk Management
- Question 10: Automated View of Cybersecurity Risk

Identify – Supply Chain Risk Management

- Question 14: SCRM Oversight

Protect – Configuration Management

- Question 20: Configuration Settings
- Question 21: Flaw Remediation

Protect – Identity and Access Management

- 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 (PII) Security Controls
- Question 37: Security Controls for Exfiltration

Protect – Security Awareness and Training

- Question 42: Assessment of Skills, Knowledge, and Abilities of Organization Workforces

Detect – Information Security Continuous Monitoring

- Question 47: Information System Continuous Monitoring (ISCM) Strategy
- Question 49: Ongoing Authorization

Respond – Incident Response

- Question 54: Incident Detection
- Question 55: Incident Handling

[11] 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, the Federal Chief Information (CISO) Council, OMB, and CISA.

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

Recover – Contingency Planning

- Question 61: Business Impact Analysis
- Question 63: IT Contingency Plan Testing

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

Identify Function Area – Risk Management Domain

Question 1
To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public-facing websites, and third-party systems) and system interconnections (NIST SP 800-53, Rev. 5: CA-3 and PM-5; NIST Cybersecurity Framework (CSF): ID.AM-1– 4; FY 2022 CIO FISMA Metrics: 1.1-1.1.5, 1.3; OMB A-130, NIST SP 800-37, Rev. 2: Task P-18; NIST 800-207, Section 7.3; EO 14028, Section 3; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B and D (5); CISA Cybersecurity & Incident Response Playbooks)?[12]
Managed and Measurable
The organization ensures that the information systems included in its inventory are subject to the monitoring processes defined within the organization's ISCM strategy.   **MET –** The Gulf Coast Ecosystem Restoration Council (Council) used third party cloud-based systems for all its information technology (IT) needs and had only its Office Support Network (OSN) which consisted of a stand-alone group of laptops connected to a leased wireless access point that provided a leased virtual private network connection to the Trusted Internet Connection portal, and mobile devices that were not connected to the OSN. As a user (stakeholder) of its information systems, the Council had limited control over its information systems. The Council had six information systems and services that third parties hosted via interagency agreement. We found the Council ensured that the information systems included in its inventory were subject to the monitoring processes defined within the organization's information security continuous monitoring (ISCM) strategy.
Optimized
The organization uses automation to develop and maintain a centralized information system inventory that includes hardware and software components from all organizational information systems. The centralized inventory is updated in a near-real time basis.   **NOT MET –** Due to the unique size and structure of the Council's information systems, the Council did not use automation to develop and maintain a centralized information system inventory that includes hardware and software components from all organizational information systems. The centralized inventory was not updated in a near real-time basis.

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

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

Identify Function Area – Risk Management Domain

Question 2
To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including GFE and Bring Your Own Device (BYOD) mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting (NIST SP 800-53, Rev. 5: CA-7 and CM-8; NIST SP 800-137; NIST IR 8011; NIST 800-207, 7.3.2; Federal Enterprise Architecture (FEA) Framework, v2; FY 2022 CIO FISMA Metrics: 1.2-1.2.3; CSF: ID.AM-1, ID.AM-5; NIST SP 800-37,Rev. 2: Task P-10 and P-16; NIST 800-207, Section 7.3; EO 14028, Section 3; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8: Control 1)?[13]
Managed and Measurable
The organization ensures that the hardware assets connected to the network are covered by an organization-wide hardware asset management capability and are subject to the monitoring processes defined within the organization's ISCM strategy. ***For mobile devices, the agency enforces the capability to deny access to agency enterprise services when security and operating system updates have not been applied within a given period based on agency policy or guidance.*** **MET –** The Council had no network server. Therefore, there were no agency enterprise services to which the Council would have denied access. The Council relied on third-party system service providers and only controlled its OSN. In addition to the laptops, the Council used mobile devices that were not connected to the OSN. The Council Chief Information Officer (CIO) tracks and maintains an inventory of its hardware assets and monitors its assets monthly. As the Council had very few IT assets, it was more cost-effective to maintain a hardware asset list manually.
Optimized
The organization employs automation to track the life cycle of the organization's hardware assets with processes that limit the manual/procedural methods for asset management. Further, hardware inventories are regularly updated as part of the organization's enterprise architecture's current and future states. **NOT MET –** The Council did not employ automation to track the life cycle of the organization's hardware assets with processes that limit the manual/procedural methods for asset management. Due to the Council's small organizational size, automated methods for asset management were unnecessary and not cost-effective.

[13] Abbreviations: (CM) Configuration Management, (GFE) Government Furnished Equipment and (NISTIR) National Institute of Standards and Technology Interagency or Internal Report, (CIS) Center for Internet Security.

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

Identify Function Area – Risk Management Domain

Question 3
To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting (NIST SP 800-53, Rev. 5: CA-7, CM-8, CM-10, and CM-11; NIST SP 800-137; NIST IR 8011; FEA Framework, v2; FY 2022 CIO FISMA Metrics: 1.3 and 4.0; OMB M-21-30; EO 14028, Section 4; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B; CSF: ID.AM-2; NIST SP 800- 37, Rev. 2: Task P-10 and P-16; NIST 800-207, Section 7.3; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8: Control 2)?[14]
Managed and Measurable
The organization ensures that the software assets, including mobile applications as appropriate, on the network (and their associated licenses), are covered by an organization-wide software asset management (or Mobile Device Management) capability and are subject to the monitoring processes defined within the organization's ISCM strategy. ***For mobile devices, the agency enforces the capability to prevent the execution of unauthorized software (e.g., blacklist, whitelist, or cryptographic containerization).*** **MET –** The Council is a micro-agency with stand-alone laptops and mobile devices that were not interconnected. The Council ensured its software assets on the OSN, except mobile devices that were not connected to its OSN, were subject to the monitoring processes defined within the organization's ISCM strategy. The Council users did not have administrator rights to install any software on laptops. For mobile devices, the Council did not need to enforce the capability to prevent the execution of unauthorized software since they were not connected to the OSN. The only software asset the Council was responsible for were the operating system (OS), Microsoft Office, and Adobe software installed on its endpoints. The Council kept accurate records of its software assets.
Optimized
The organization employs automation to track the life cycle of the organization's software assets (and their associated licenses), including for mobile applications, with processes that limit the manual/procedural methods for asset management. Further, software inventories are regularly updated as part of the organization's enterprise architecture's current and future states. **NOT MET –** We found the Council did not employ automation to track the life cycle of the organization's software assets (and their associated licenses) with processes that limit the manual/procedural methods for asset management. However, software inventories were regularly updated as part of the organization's enterprise architecture's current and future states. It should be noted the Council was a user (stakeholder) of all its information systems. The only software assets the Council was responsible for were the OS, Microsoft Office, and Adobe software installed on its laptops.

[14] Abbreviation: (FEA) Federal Enterprise Architecture.

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

Identify Function Area – Risk Management Domain

Question 5
To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels (NIST SP 800-39; NIST SP 800-53, Rev. 5: RA-3 and PM-9; NIST IR 8286; CSF: ID RM-1–ID.RM-3; OMB A-123; OMB M-16-17; OMB M-17-25; NIST SP 800-37 (Rev. 2): Tasks P-2, P-3, P-14, R-2, and R-3? [15]
Managed and Measurable
The organization utilizes the results of its system-level risk assessments, along with other inputs, to perform and maintain an organization-wide cybersecurity and privacy risk assessment. The result of this assessment is documented in a cybersecurity risk register and serves as an input into the organization's enterprise risk management program. The organization consistently monitors the effectiveness of risk responses to ensure that risk tolerances are maintained at an appropriate level. ***The organization ensures that information in cybersecurity risk registers is obtained accurately, consistently, and in a reproducible format and is used to (i) quantify and aggregate security risks, (ii) normalize cybersecurity risk information across organizational units, and (iii) prioritize operational risk response.*** **MET –** The Council monitored and analyzed its defined qualitative and quantitative performance measures on the effectiveness of its risk management strategy across disciplines and collected, analyzed, and reported information on the effectiveness of its risk management program through the use of the Plan of Action and Milestones (POA&M) Tracker and Continuous Diagnostics and Mitigation (CDM) Dashboards. The Council had developed a risk profile and utilized POA&M Tracker to serve as an input into the organization's enterprise risk management program. The Council ensured that information in cybersecurity risk registers was obtained accurately and consistently.
Optimized
The cybersecurity risk management program is fully integrated at the organizational, mission/business process, and information system levels, as well as with the entity's enterprise risk management program. ***Further, the organization's cybersecurity risk management program is embedded into daily decision-making across the organization and provides for continuous identification and monitoring to ensure that risk remains within organizationally defined acceptable levels.*** ***The organization utilizes Cybersecurity Framework profiles to align cybersecurity outcomes with mission or business requirements, risk tolerance, and resources of the organization.*** **NOT MET -** It would not be cost-effective to achieve this maturity level since the Council is a micro-agency with a unique organizational size and structure. Furthermore, the Council did not fully integrate its organizational and business processes at all levels of the agency, nor have they

[15] Abbreviation: (RA) Risk Assessment, (ID.RM) Identify – Risk Management Strategy.

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

Identify Function Area – Risk Management Domain

Question 5
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.

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

Identify Function Area – Risk Management Domain

Question 10
To what extent does the organization utilize technology/ automation to provide a centralized, enterprise-wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123; NIST IR 8286; CISA Zero Trust Maturity Model, Pillars 2-4, NIST 800-207, Tenets 5 and 7; OMB M-22-09, Federal Zero Trust Strategy, Security Orchestration, Automation, and Response)?
Consistently Implemented
The organization consistently implements an automated solution across the enterprise that provides a centralized, enterprise-wide view of cybersecurity risks, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards. All necessary sources of cybersecurity risk information are integrated into the solution. **MET –** The Council had automated solutions that provided a centralized, enterprise-wide view of risks across the organization, with all necessary sources of risk information integrated.
Managed and Measurable
The organization uses automation to perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting impact on organizational systems and data. ***In addition, the organization ensures that cybersecurity risk management information is integrated into reporting tools, such as governance, risk management, and compliance tool), as appropriate.*** **NOT MET –** Given the unique structure of the Council, the Council did not use automation to perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting implications for organizational systems and data. In addition, the cybersecurity risk management information was not integrated into ERM [Enterprise Risk Management] CDM reporting tools.

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

Identify Function Area – Supply Chain Risk Management Domain

Question 14
To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements (The Federal Acquisition Supply Chain Security Act of 2018, NIST SP 800-53, Rev. 5: SA-4, SR-3, SR-5, and SR-6 (as appropriate); NIST SP 800-152; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4, NIST IR 8276, NIST 800-218, Task PO.1.3; FY 2022 CIO FISMA Metrics: 7.4.2; CIS Top 18 Security Controls v.8: Control 15)?[16]
Ad Hoc
The organization has not defined and communicated policies and procedures to ensure that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and supply chain risk management requirements. **MET -** The Council defined and communicated policies and procedures to ensure that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and supply chain risk management requirements.
Defined
The organization has defined and communicated policies and procedures to ensure that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and supply chain risk management requirements. The following components, at a minimum, are defined - ***The identification and prioritization of externally provided systems, system components, and services as well as how the organization maintains awareness of its upstream suppliers*** - ***Integration of acquisition processes, including the use of contractual agreements that stipulate appropriate cyber and SCRM measures for external providers.*** - ***Tools and techniques to utilize the acquisition process to protect the supply chain, including, risk-based processes for evaluating cyber supply chain risks associated with third-party providers, as appropriate.*** - ***Contract tools or procurement methods to confirm contractors are meeting their contractual SCRM obligations.*** **NOT MET –** The Council defined and communicated policies and procedures to ensure that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and supply chain risk management requirements. However, the Council did not define the minimum above components as required by the Defined maturity level.

[16] Abbreviations: (SA) System and Service Acquisition, (SR) Supply Chain Risk Management, (FedRAMP) Federal Risk and Authorization Management Program, (ID.SC) Identify – Supply Chain Risk Management.

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

Protect Function Area - Configuration Management Domain

Question 20
To what extent does the organization utilize configuration settings/common secure configurations for its information systems (NIST SP 800-53, Rev. 5: CM-6, CM-7, and RA-5; NIST SP 800-70, Rev. 4; FY 2022 CIO FISMA Metrics, Section 7, Ground Truth Testing; EO 14028, Section 4, 6, and 7; OMB M-22-09, Federal Zero Trust Strategy, Section D; OMB M 22-05; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8, Controls 4 and 7; CSF: ID.RA-1 and DE.CM-8)?[17]
Managed and Measurable
The organization employs automation to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for all information system components connected to the organization's network and makes appropriate modifications in accordance with organization-defined timelines. **MET –** The Council employed automation to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for all information system components connected to the organization's network and makes appropriate modifications in accordance with organization-defined timelines.
Optimized
The organization deploys system configuration management tools that automatically enforce and redeploy configuration settings to systems at frequent intervals as defined by the organization, or on an event driven basis. **NOT MET –** Due to the unique structure of the Council's information systems, 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.

[17] Abbreviations: (ID.RA) Identify – Risk Assessment, (DE.CM) Detect – Security Continuous Monitoring.

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

Protect Function Area - Configuration Management Domain

Question 21
To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (EO 14028, Sections 3 and 4; NIST SP 800-53, Rev. 5: CM-3, RA-5, SI-2, and SI-3; NIST SP 800-40, Rev. 3; NIST 800-207, section 2.1; CIS Top 18 Security Controls v.8, Controls 4 and 7; FY 2022 CIO FISMA Metrics: Section 8; CSF: ID.RA-1; DHS BOD 18-02, 19-02, and 22-01; OMB M-22-09, Federal Zero Trust Strategy, Section D; CISA Cybersecurity Incident and Vulnerability Response Playbooks)?[18]
Managed and Measurable
The organization centrally manages its flaw remediation process and utilizes automated patch management and software update tools for operating systems, where such tools are available and safe. ***The organization monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of flaw remediation processes and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.*** **MET –** The Council centrally managed its flaw remediation process and utilized automated patch management and software update tools for the operating systems, where such tools were available and safe.
Optimized
The organization utilizes automated patch management and software update tools for all applications and network devices (including mobile devices), as appropriate, where such tools are available and safe. ***As part of its flaw remediation processes, the organization performs deeper analysis of software code, such as through patch sourcing and testing.*** **NOT MET –** The Council is a small organization that did not have the infrastructure, or the resources needed to automate patch management and software update tools for all applications and network devices. As part of its flaw remediation processes, the Council did not perform a deeper analysis of software code through patch sourcing and testing.

[18] Abbreviations: (SI) System and Information Integrity.

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

Protect Function Area - Identity and Access Management Domain

Question 30
To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for non-privileged users to access the organization's facilities [organization defined entry/exit points], networks, and systems, including for remote access (EO 14028, Section 3; HSPD-12; NIST SP 800-53, Rev. 5: AC-17, IA-2, IA-5, IA-8, and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63 and 800-157; OMB M-19-17; FY 2022 CIO FISMA Metrics: Section 2; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section A (2); CSF: PR.AC-1 and 6; NIST 800-207 Tenet 6; CIS Top 18 Security Controls v.8: Control 6)?[19]
Managed and Measurable
All non-privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems and facilities [organization-defined entry/exit points]. **MET –** The Council's non-privileged users used strong authentication mechanisms to authenticate to applicable organizational systems and facilities.
Optimized
The organization has implemented an enterprise-wide single sign-on solution and all of the organization's systems interface with the solution, resulting in an ability to manage user (non-privileged) accounts and privileges centrally and report on the effectiveness on a near real-time basis. **NOT MET –** Due to the unique structure of the Council's information systems, an enterprise-wide single sign-on solution that can manage user (non-privileged) accounts and privileges centrally and report on the effectiveness on a near real-time basis will require a financial commitment where the cost-benefits may not be justifiable in the Council's environment.

[19] Abbreviations: (HSPD) Homeland Security Presidential Directive, (AC) Access Controls, (PE) Physical and Environment Protection, (PR.AC) Protect – Identity Management and Access Control.

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

Protect Function Area - Identity and Access Management Domain

Question 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 (EO 14028, Section 3; HSPD-12; NIST SP 800-53, Rev. 5: AC-17 and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63 and 800-157; OMB M-19-17; FY 2022 CIO FISMA Metrics: Section 2; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section A (2); CSF: PR.AC-1 and 6; DHS ED 19-01; NIST 800-207 Tenet 6; CIS Top 18 Security Controls v.8: Control 6)?[20]
Managed and Measurable
All privileged users, including those who can make changes to DNS records, utilize strong authentication mechanisms to authenticate to applicable organizational systems. **MET –** The Council had a unique organizational structure without formal departments and layers of management typically found in larger organizations. As a result, the CIO was the lone IT personnel assigned a moderate-risk designation. The Council did not change DNS records as it did not host the DNS system. The Council did not have network resources requiring a DNS system.
Optimized
The organization has implemented an enterprise-wide single sign-on solution and all the organization's systems interface with the solution, resulting in an ability to manage user (privileged) accounts and privileges centrally and report on the effectiveness on a near real-time basis. **NOT MET** – Due to the unique structure of the Council's information systems, an enterprise-wide single sign-on solution that can manage user (privileged) accounts and privileges centrally and report on the effectiveness on a near real-time basis will require a financial commitment where the cost-benefits may not be justifiable in the Council's environment.

[20] Abbreviations: (ED) Emergency Directive.

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

Protect Function Area - Identity and Access Management Domain

Question 32
To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed (EO 14028, Section 8; FY 2022 CIO FISMA Metrics: 3.1; OMB M-21-31; OMB M-19-17; NIST SP 800-53, Rev. 5: AC-1, AC- 2, AC-5, AC-6, AC-17; AU-2, AU-3, AU-6, and IA-4; DHS ED 19-01; CSF: PR.AC-4; CIS Top 18 Security Controls v.8: Controls 5, 6, and 8)?[21]
Managed and Measurable
The organization employs automated mechanisms (e.g. machine-based, or user-based enforcement) to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate. **MET –** The Council employed automated mechanisms (e.g., machine-based, or user-based enforcement) to support privileged accounts management, including the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate. The Council implemented strong authentication mechanisms for all privileged and non-privileged users and required the use of personal identity verification (PIV) to gain access to Council's government shared service provider.
Optimized
Per the FY 2022 Core IG Metrics, this maturity level did not apply to this question.

[21] Abbreviation: (AU) Audit and Accountability, (IA) Identification and Authentication.

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

Protect Function Area - Data Protection and Privacy Domain

Question 36
To what extent has the organization implemented the encryption of data rest, in transit, limitation of transference of data by removable media, and sanitization of digital media prior to disposal or reuse to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle (EO 14028, Section 3(d); OMB M-22-09, Federal Zero Trust Strategy; NIST 800-207; NIST SP 800-53, Rev. 5; SC-8, SC-28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2022 CIO FISMA Metrics: 2.1, 2.2, 2.12, 2.13; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6; CIS Top 18 Security Controls v. 8: Control 3)?[22]
Consistently Implemented
The organization's policies and procedures have been consistently implemented for the specified areas, including (i) use of FIPS-validated encryption of PII and other agency sensitive data, as appropriate, both at rest and in transit, (ii) prevention and detection of untrusted removable media, and (iii) destruction or reuse of media containing PII or other sensitive agency data. **MET –** According to the Council's *Privacy Program Plan,* "None of the GCERC [Council] Systems create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII." The Council only had OSN directly under its control and other Council systems were managed by a third party. Hence, the third party is responsible for its privacy controls. We assessed this maturity level as Consistently Implemented since the Council did not process any form of PII.
Managed and Measurable
The organization ensures that the security controls for protecting PII and other agency sensitive data, as appropriate, throughout the data lifecycle are subject to the monitoring processes defined within the organization's ISCM strategy. **NOT MET –** As the Council did not collect PII, security controls for protecting PII throughout the data lifecycle were not subject to the monitoring processes and were not applicable.

[22] Abbreviation: (SC) System and Communication Protection, (MP) Media Protection, (BOD) Binding Operational Directive, (PR.DS) Protect – Data Security, (PR.PT) Protect – Protective Technology, (PR.IP) Protect – Information Protection Processes and Procedures.

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

Protect Function Area - Data Protection and Privacy Domain

Question 37
To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses (FY 2022 CIO FISMA Metrics, 5.1; NIST SP 800-53, Rev. 5: SI-3, SI-7, SI-4, SC-7, and SC-18; DHS BOD 18-01; DHS ED 1901; CSF: PR.DS-5, OMB M-21-07; CIS Top 18 Security Controls v.8: Controls 9 and 10)?
Consistently Implemented
The organization consistently monitors inbound and outbound network traffic, ensuring that all traffic passes through a web content filter that protects against phishing, malware, and blocks known malicious sites. Additionally, the organization checks outbound communications traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of PII. Also, suspected malicious traffic is quarantined or blocked. ***In addition, the organization utilizes email authentication technology and ensures the use of valid encryption certificates for its domains.*** **MET –** The Council consistently monitored inbound and outbound network traffic, ensured all traffic passed through a web content filter that protects against phishing and malware, and blocks against known malicious sites. The Council utilized the Department of Homeland Security's CDM Capabilities and EINSTEIN to enhance network defenses. Additionally, the Council checked outbound communications traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of PII. Also, suspected malicious traffic was quarantined or blocked. As the Council used a third party service provider for email, the third party service provider was responsible for email authentication.
Managed and Measurable
The organization analyzes qualitative and quantitative measures of the performance of its data exfiltration and enhanced network defenses. The organization also conducts exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses. ***Further, the organization monitors its DNS infrastructure for potential tampering, in accordance with its ISCM strategy. In addition, the organization audits its DNS records.*** **NOT MET –** The Council is a small organization that did not have the infrastructure, risks, or resources needed to analyze qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses.

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

Protect Function Area - Security Awareness Training Domain

Question 42
To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover (FY 2022 CIO FISMA Metrics, Section 6; NIST SP 800-53, Rev. 5: AT-2, AT-3, and PM-13; NIST SP 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181; and CIS Top 18 Security Controls v.8: Control 14)?[23]
Managed and Measurable
The organization has addressed its identified knowledge, skills, and abilities gaps through training or talent acquisition. **MET –** The Council addressed its identified knowledge, skills, and abilities gaps through talent acquisition. Based on our understanding of the organization's small size and the limited scope of the IT environment, we determined the Council met the maturity level of Managed and Measurable for this question.
Optimized
The organization's personnel collectively possess a training level such that the organization can demonstrate that security incidents resulting from personnel actions or inactions are being reduced over time. **NOT MET –** No security incidents occurred at the Council during the FISMA year. If any incidents happened on the systems managed through interagency agreements, the Council would be notified by the third-party system service providers. The Council could demonstrate that security incidents resulting from personnel actions or inactions were reduced over time. We could not determine whether the Council's personnel collectively possessed a training level.

[23] Abbreviation: (AT) Awareness and Training.

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

Detect Function Area - Information Security and Continuous Monitoring Domain

Question 47
To what extent does the organization utilize ISCM policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier (NIST SP 800-53, Rev. 5: CA-7, PM-6, PM-14, and PM-31; NIST SP 800-37 (Rev. 2) Task P-7; NIST SP 800-137: Sections 3.1 and 3.6; CIS Top 18 Security Controls v.8: Control 13)?
Managed and Measurable
The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM strategy and makes updates, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. ***The organization has transitioned to ongoing control and system authorization through the implementation of its continuous monitoring policies and strategy.*** **MET –** The Council relied on third party service providers for its ISCM capabilities. The third party service providers monitored and analyzed measures on the effectiveness of the Council's ISCM policies and procedures. The Council reviewed reports provided by the third party service providers to better ascertain the effectiveness of its ISCM policies and procedures. The Council has transitioned to ongoing control and system authorization through the implementation of its continuous monitoring policies and strategy.
Optimized
The organization's ISCM strategy is fully integrated with its risk management, configuration management, incident response, and business continuity functions. ***The organization can demonstrate that it is using its ISCM policies and strategy to reduce the costand increase the efficiency of security and privacy programs.*** **NOT MET –** The Council did not fully integrate its ISCM strategy with risk management, configuration management, incident response, and business continuity functions. In addition, the Council is not using its ISCM policies and strategy to reduce the cost and increase the efficiency of security and privacy programs.

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

Detect Function Area - Information Security and Continuous Monitoring Domain

Question 49
How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls (OMB A-130; NIST SP 800-137: Section 2.2; NIST SP 800-53, Rev. 5: CA-2, CA-5, CA-6, CA-7, PL-2, and PM-10; NIST Supplemental Guidance on Ongoing Authorization; NIST SP 800-37 (Rev. 2) Task S-5; NIST SP 800-18, Rev. 1, NIST IR 8011; OMB M-14-03; OMB M-19-03)?[24]
Managed and Measurable
The organization utilizes the results of security control assessments and monitoring to maintain ongoing authorizations of information systems, including the maintenance of system security plans. **MET –** The Council utilizes the results of security control assessments and monitoring to maintain ongoing authorizations of information systems, including the maintenance of system security plans.
Optimized
The organization's system level ISCM policies and strategies are fully integrated with its enterprise and supply chain risk management, configuration management, incident response, and business continuity programs. ***The organization can demonstrate that it is using its system level ISCM policies and strategy to reduce the cost and increase the efficiency of security and privacy programs.*** **NOT MET –** The Council's system level ISCM policies and strategies were not fully integrated with its enterprise and supply chain risk management, configuration management, incident response, and business continuity programs. The Council is not using its system level ISCM policies and strategy to reduce the cost and increase the efficiency of security and privacy programs.

[24] Abbreviation: (PL) Planning.

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

Respond Function Area - Incident Response Domain

Question 54
How mature are the organization's processes for incident detection and analysis (EO 14028, Section 6; OMB M-22-05, Section I; CISA Cybersecurity Incident and Vulnerability Response Playbooks; FY 2022 CIO FISMA Metrics: 10.6; NIST 800-53, Rev. 5: IR-4, IR-5, and IR-6; NIST SP 800-61 Rev. 2; OMB M20-04; CSF: DE.AE-1, DE.AE-2 -5, PR.DS-6, RS.AN-1 and 4, and PR.DS-8; and CIS Top 18 Security Controls v.8: Control 17)?[25]
Managed and Measurable
The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident detection and analysis policies and procedures. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. ***The organization utilizes profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents. Examples of profiling include running file integrity checking software on hosts to derive checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times. Through profiling techniques, the organization maintains a comprehensive baseline of network operations and expected data flows for users and systems.*** **MET –** The Council conducted table-top exercises and used third party providers to measure the effectiveness of its incident detection and analysis policies and procedures. In addition, through a third-party provider, the Council utilized profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents.
Optimized
Per the FY 2022 Core IG Metrics, this maturity level did not apply to this question.

[25] Abbreviations: (IR) Incident Response, (DE.AE) Detect – Anomalies and Events, and (RS.AN) Respond – Analysis.

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

Respond Function Area - Incident Response Domain

Question 55
How mature are the organization's processes for incident handling (EO 14028, Section 6; OMB M-22-05, Section I; CISA Cybersecurity Incident and Vulnerability Response Playbooks; FY 2022 CIO FISMA Metrics: 10.6; NIST 800-53, Rev. 5: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 2)?[26]
Consistently Implemented
The organization consistently implements its incident handling policies, procedures, containment strategies, and incident eradication processes. ***In addition, the organization consistently implements processes to remediate vulnerabilities that may have been exploited on the target system(s) and recovers system operations.*** ***Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident handling policies and procedures and making updates as necessary.*** **MET –** The Council has developed containment strategies for each major incident type through its Incident Response Plan. In developing its strategies, the Council has taken into consideration: the potential damage to and theft of resources, the need for evidence preservation, service availability, time and resources needed to implement the strategy, the effectiveness of the strategy, and the duration of the solution. In addition, the Council has defined its processes to eradicate components of an incident, mitigate any vulnerabilities that were exploited, and recover system operations. The Council relies on third party service providers to help identify and eradicate components of an incident, mitigate any vulnerabilities that were exploited, and recover system operations. Due to the Council's reliance on third party service providers for its information systems needs and the Council's unique organizational structure, the Council has limited exposure to security incidents in its information systems. The Council performs table-top exercises yearly to look at incident response policies, and it was found through these exercises that the policy is effective, and procedures are effective.
Managed and Measurable
The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident handling policies and procedures. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. ***The organization manages and measures the impact of successful incidents and can quickly mitigate related vulnerabilities on other systems so that they are not subject to exploitation of the same vulnerability.*** **NOT MET –** As a small agency that primarily uses information systems that third party providers host, the Council has limited exposure to vulnerabilities and security incidents on its

[26] Abbreviation: (RS.MI) Respond – Mitigation.

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

Respond Function Area - Incident Response Domain

Question 55
information systems. The Council relies on third party service providers for its information system needs. The Council had not reported any incident during the audit period. Since the Council did not experience any incidents during the FISMA period from July 1, 2021, through March 31, 2022, 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.

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

Recover Function Area - Contingency Planning Domain

Question 61
To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts (FY 2022 CIO FISMA Metrics: 10.1.4; NIST SP 800-53, Rev. 5: CP-2, and RA-9; NIST SP 800-34, Rev. 1, 3.2; NIST IR 8286; FIPS 199; FCD-1; OMB M-19-03; CSF:ID.RA-4)?[27]
Consistently Implemented
The organization consistently incorporates the results of organizational and system level BIAs into strategy and plan development efforts. System level BIAs are integrated with the organizational level BIA and include: characterization of all system components, determination of missions/business processes and recovery criticality, identification of resource requirements, and identification of recovery priorities for system resources. The results of the BIA are consistently used to determine contingency planning requirements and priorities, including mission essential functions/high value assets. **MET –** The Council is a small organization and did not have the typical network available in larger organizations that may require an organizational and system-level BIA. The Council's cloud-based systems, except the OSN, were managed by third party service providers; however, the Council's CIO created a BIA for the OSN.
Managed and Measurable
The organization ensures that the results of organizational and system level BIA's are integrated with enterprise risk management processes, for consistently evaluating, recording, and monitoring the criticality and sensitivity of enterprise assets. ***As appropriate, the organization utilizes the results of its BIA in conjunction with its risk register to calculate potential losses and inform senior level decision making.*** **NOT MET –** The Council utilized the results of its BIA in conjunction with its risk register to calculate potential losses and inform senior level decision making. However, the Council did not ensure that the organizational and system level BIA results are integrated with enterprise risk management processes, for consistently evaluating, recording, and monitoring the criticality and sensitivity of enterprise assets.

[27] Abbreviation: (CP) Contingency Planning, (FCD) Federal Continuity Directive.

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

Recover Function Area - Contingency Planning Domain

Question 63
To what extent does the organization perform tests/exercises of its information system contingency planning processes (FY 2022 CIO FISMA Metrics: 10.1; NIST SP 800-34; NIST SP 800-53, Rev. 5: CP-3 and CP-4; CSF: ID.SC-5 and CSF: PR.IP- 10; CIS Top 18 Security Controls v.8: Control 11)?
Consistently Implemented
Information system contingency plan testing and exercises are consistently implemented. Information System Contingency Plan (ISCP) testing and exercises are integrated, to the extent practicable, with testing of related plans, such as incident response plan/COOP/BCP. **MET –** ISCP testing and exercises were consistently implemented. ISCP testing and exercises were integrated, to the extent practicable, with testing of related plans.
Managed and Measurable
The organization employs automated mechanisms to test system contingency plans more thoroughly and effectively. ***In addition, the organization coordinates plan testing with external stakeholders (e.g., ICT supply chain partners/providers) as appropriate.***[28] **NOT MET –** The Council is a small organization that did not have the infrastructure, risks, or resources needed to manage and employ automated mechanisms to test system contingency plans more thoroughly and effectively. In addition, the Council did not coordinate plan testing with external stakeholders.

[28] Abbreviation: (COOP) Continuity of Operations Plan, (BCP) Business Continuity Plan, (ICT) Information and Communications Technology.

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

Evaluation Results

The overall maturity level of the Gulf Coast Ecosystem Restoration Council (Council's) information security program was Managed and Measurable.[29] We have presented the maturity level for the nine domains below:

Table 2: The Council's FY 2022 Maturity Levels

Cybersecurity Framework Security Functions	FY 2022 IG FISMA Metric Domains	Maturity Level
Identify	Risk Management	Managed and Measurable
Identify	Supply Chain Risk Management	Ad Hoc
Protect	Configuration Management	Managed and Measurable
Protect	Identity and Access Management	Managed and Measurable
Protect	Data Protection and Privacy	Consistently Implemented
Protect	Security Training	Managed and Measurable
Detect	Information Security Continuous Monitoring	Managed and Measurable
Respond	Incident Response	Managed and Measurable
Recover	Contingency Planning	Consistently Implemented
Overall		**Managed and Measurable**

RMA has included a summary for the domains that Council has not achieved a rating of Managed and Measurable:

- **Supply Chain Risk Management (SCRM)**: We determined the Council's overall maturity level for the SCRM program was Ad Hoc. Although the Council had defined supply chain policies and procedures, the Council did not define the minimum components as required by Question 14 of the *Fiscal Year (FY) 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.1* (May 12, 2021). The Council managed its supply chain risks by purchasing products from trusted and approved manufacturers. The Council's Office Support Network (OSN) is considered a server-less network with a Federal Information Processing Standards Publication (FIPS) 199 rating of 'low.'[30] Although the maturity level of this domain was Ad Hoc, our testing found no exceptions, and the controls were operating as intended. The Council only has a single information technology (IT) vendor with limited operating machines. Hence, the Council has limited SCRM risks. We concluded the Council's SCRM program controls in place were effective.
- **Data Protection and Privacy**: We determined the Council's overall maturity level for the Data Protection and the Privacy program was Consistently Implemented. The Council did

[29] A program at that assessed level is considered effective by OMB and DHS.
[30] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, states that a potential impact on organizations or individuals is 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.

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

not monitor and analyze quantitative and qualitative performance measures on the effectiveness of its privacy activities and use the information to make needed adjustments that were necessary to reach the Managed and Measurable level.

- **Contingency Planning**: We determined the Council's overall maturity level for the Contingency Planning program was Consistently Implemented. The Council did not develop quantitative and qualitative effectiveness measures necessary to reach the Managed and Measurable level.

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

Appendix II: Management Response

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

Gulf Coast Ecosystem Restoration Council

August 03, 2022

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 2022

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 2022.

The Council agrees with the report that the Council's information security program and practices were effective for the period July 1, 2021 through March 31, 2022. The Council works to ensure that the five Cybersecurity Functions defined by NIST and the nine FISMA Metric domains defined by OMB and CISA are met.

In fiscal year 2023, 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: 2022.08.03 14:42:23 -04'00'

Mary S. Walker
Executive Director
Gulf Coast Ecosystem Restoration Council

This Page Intentionally Left Blank

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/