Evaluation Report

OIG-CA-22-003

INFORMATION TECHNOLOGY

The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2021

October 20, 2021

Office of Inspector General
Department of the Treasury

This Page Intentionally Left Blank

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

October 20, 2021

MEMORANDUM FOR MARY WALKER
EXECUTIVE DIRECTOR

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 2021*

We hereby transmit the attached report, *The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2021*, dated October 20, 2021. 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 or an independent external auditor perform the annual evaluation as determined by the Inspector General.

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, 2020 through June 30, 2021. 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, 2020 through June 30, 2021.

Appendix I of the attached RMA report includes the *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics.*

If you have any questions or require further information, you may contact me at (202) 321-1480.

Attachment

RMA Associates
Auditors. Consultants. Advisors.

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

Evaluation Report for Fiscal Year 2021

RMA Associates
Auditors. Consultants. Advisors.

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

October 22, 2021

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

Re: The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2021

Dear Mr. Delmar:

RMA Associates, LLC is pleased to submit the Gulf Coast Ecosystem Restoration Council (Council) Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2021. 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 January 2012. We have also prepared the *FY 2021 Inspector General Federal Information Security Modernization Act of 2014(FISMA) Reporting Metrics Version 1.1* (May 12, 2021) as shown in Appendix I. These metrics provide reporting requirements across the function areas to be addressed in the independent assessment of agencies' information security programs. The objective of this evaluation was to evaluate the effectiveness of the Council's information security program and practices for the period July 1, 2020 through June 30, 2021.

In summary, we found the Council's information security program and practices were effective for the period July 1, 2020 through June 30, 2021.

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

RMA Associates
Auditors. Consultants. Advisors.

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
AR	Accountability, Audit, and Risk Management
AT	Awareness and Training
AU	Audit and Accountability
ARC	Administrative Resource Center
BIA	Business Impact Analysis
BOD	Binding Operational Directive
BYOD	Bring Your Own Device
CA	Security Assessment and Authorization
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
CCB	Change Control Board
CDM	Continuous Diagnostics and Mitigation
CM	Configuration Management
Council (or GCERC)	Gulf Coast Ecosystem Restoration Council
CP	Contingency Planning
CSF	Cybersecurity Framework
DE.AE	Anomalies and Events
DHS	Department of Homeland Security
DNS	Domain Name System
DoA	Director of Administration
ED	Emergency Directive
ERM	Enterprise Risk Management
ERA	Electronic Record Archives
FAQ	Frequently Asked Questions
FCD	Federal Continuity Directive
FEA	Federal Enterprise Architecture
FedRAMP	Federal Risk and Authorization Management Program
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FITARA	Federal Information Technology Acquisition Reform Act
GCC	Gulf Coast Council
GFE	Government Furnished Equipment
HSPD	Homeland Security Presidential Directive
IA	Identification and Authentication
IAL	Identity Assurance Level
ICAM	Identity, Credential, and Access Management
ICT	Information and Communications Technology

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

ID.AM	Asset Management
ID.BE	Business Environment
ID.GV	Governance
ID.RA	Risk Assessment
ID.RM	Risk Management Strategy
ID.SC	Supply Chain Risk Management
IG	Inspector General
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Planning
IR	Incident Response
IT	Information Technology
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency or Internal Report
NOAA	National Oceanic and Atmospheric Administration
MERLIN	Metadata Records Library and Information Network
MP	Media Protection
OIG	Office of Inspector General
OMB	Office of Management and Budget
Oracle	Oracle Federal Financials
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
PPD	Presidential Policy Directive
PS	Personnel Security
P.L.	Public Law
PL	Planning
POA&M	Plan of Action and Milestones
PR.AC	Identity Management and Access Control
PR.DS	Data Security
PR.IP	Information Protection Processes and Procedures
PR.PT	Protective Technology
RA	Risk Assessment
RAAMS	Restoration Assistance and Award Management System
RESTORE Act	Resources and Ecosystems Sustainability, Tourist Opportunities, and Revived Economies of the Gulf Coast States Act of 2012
RS.AN	Analysis
RS.CO	Communications
RS.MI	Mitigation

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

RS.RP	Response Planning
RMF	Risk Management Framework
SA	System and Service Acquisition
SAOP	Senior Agency Official for Privacy
SANS	SysAdmin, Audit, Network, and Security
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SI	System and Information Integrity
SIEM	Security Information and Event Management
SC	System and Communication Protection
SP	Special Publication
SR	Supply Chain Risk Management
TIC	Trusted Internet Connection
Treasury	Department of the Treasury
USC	U.S. Code
US-CERT	United States Computer Emergency Readiness Team
VDP	Vulnerability Disclosure Policy

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. DHS prepared the FISMA questionnaire to collect the responses, which is provided in Appendix I: *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (FISMA Reporting Metrics). We also considered applicable OMB policy and guidelines, and the National Institute of Standards and Technology (NIST) standards and guidelines.

FISMA requires the agency Inspector General (IG) or an independent external auditor, as determined by the IG, to perform the annual evaluation. 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, 2020 through June 30, 2021.

This evaluation was performed in accordance with the *Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation*, issued January 2012. We have also prepared the FISMA Reporting Metrics, as shown in Appendix I. These metrics provide reporting requirements across the functional areas to be addressed in the independent assessment of agencies' information security programs. See *Objective, Scope, and Methodology* for more detail.

Summary Evaluation Results

We concluded, consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, the Council's information security program and practices were established and maintained for the five Cybersecurity Functions[2] and nine FISMA Metric Domains.[3] The overall maturity level of the Council's information security program was determined as Managed and Measurable, as described in this report. Accordingly, we found the

[1] Public Law (P.L.) 113-283, Federal Information Security Modernization Act of 2014 (Dec. 18, 2014).
[2] OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency developed the 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.
[3] 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

Council's information security program and practices were effective for the period July 1, 2020 through June 30, 2021.

We provided the Council a draft of this report for comment. In a written response, management agreed with the results of our evaluation. See *Management's Response* in Appendix II for 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 of 2012* (RESTORE Act)[4] was signed into law on July 6, 2012. The RESTORE Act calls for a regional approach to restoring the long-term health of the valuable natural ecosystem and economy of the Gulf Coast region. The RESTORE Act dedicates 80 percent of civil and administrative penalties paid under the Clean Water Act, after the date of enactment, by responsible parties in connection with the Deepwater Horizon oil spill to the Gulf Coast Restoration Trust Fund for ecosystem restoration, economic recovery, and tourism promotion in the Gulf Coast region.

In addition to creating the Gulf Coast Restoration Trust Fund, the RESTORE Act established the Council. The Council is comprised of 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, Army, Commerce, Homeland Security, and Interior, and the Administrator of the U.S. Environmental Protection Agency.

The Council is a small agency with a simple, flat organizational structure. The Council had few information technology (IT) assets and 34 employees and contractors. The Council's information system infrastructure consists of an Office Support Network (OSN) and several 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.

The following unclassified cloud-based systems support the Council's functions:

1. For payroll processing, the Council used WebTA (hosted by the U.S. Department of Agriculture's National Finance Center);
2. For financial management and report processing, the Council used the Administrative Resource Center (ARC) (hosted by Treasury's Bureau of the Fiscal Service) to record financial transactions in Oracle Federal Financials (Oracle);

[4] P.L. 112-141, Resources and Ecosystems Sustainability, Tourist Opportunities, and Revived Economies of the Gulf Coast States Act of 2012 (July 6, 2012).

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

3. For metadata, the Council used Metadata Records Library and Information Network (MERLIN)[5] (hosted by U.S. Geological Survey);
4. For award management, the Council used GrantSolutions (hosted by U.S. Department of Health and Human Services) and Restoration Assistance and Award Management System (RAAMS)[6] (hosted by the U.S. Geological Survey);
5. For program data management, the Council used Program Information Platform for Ecosystem Restoration (PIPER), provided by U.S. Geological Survey. Website support was also provided by the U.S. Geological Survey;
6. For electronic records management, the Council used the National Archives and Records Administration (NARA) to record management transactions in Electronic Record Archives (ERA);
7. For email and G Suite[7], the Council used the U.S. Department of Commerce's National Oceanic and Atmospheric Administration (NOAA) to host the applications; and
8. For Continuous Diagnostic Monitoring and EINSTEIN[8] capabilities, the Council used DHS hosting services.

Federal Information Security Modernization Act of 2014

Title III of the *E-Government Act*, entitled the *Federal Information Security Management Act of 2002*,[9] 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*[10] and provided several modifications that modernize Federal security practices to address evolving security concerns. These changes result 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*[11] and the *Information Technology Management Reform Act of 1996*[12] (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;

[5] New System for FY 21.
[6] The Council replaced RAAMS with GrantSolutions for award management on October 2, 2020. Prior to that, RAAMS, was running parallel to GrantSolutions for six months until decommissioned.
[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 (CISA) employs to provide a common baseline of security across the Federal Civilian Executive Branch and to help agencies manage their cyber risk.
[9] P.L. 107-347, Federal Information Security Management Act of 2002 (Dec. 17, 2002).
[10] P.L. 107-347, Federal Information Security Management Act of 2002 (Dec. 17, 2002).
[11] P.L. 104-13, Paperwork Reduction Act of 1995 (May 22, 1995).
[12] P.L. 104-106, the Information Technology Management Reform Act of 1996 (Feb. 10, 1996).

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

- Ensure that appropriate officials are assigned security responsibility;
- Periodically review the security controls in their systems; and
- 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 also developed an integrated Risk Management Framework (RMF) which effectively brings together all the FISMA-related security standards and guidance to promote the development of comprehensive and balanced information security programs by agencies.

FISMA Reporting Metrics

We evaluated the effectiveness of the information security program and practices on a maturity model spectrum in which the foundation levels ensure the development of sound policies and procedures. The FISMA Reporting 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 are not formalized; activities were performed in an ad hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies are formalized and documented, but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures were lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Our evaluation was conducted for the period between July 1, 2020 and June 30, 2021. It consisted of testing the 66 metric questions listed in the FISMA Reporting Metrics issued by DHS. The answers to the 66 metric questions in Appendix I reflect the results of our testing of the Council's information security program and practices. The FISMA Reporting 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)[13];
- 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.

[13] The FISMA Reporting Metrics included a new domain, SCRM, within the Identify function. This new domain focused on the maturity of agency SCRM strategies, policies and procedures, plans, and processes to ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain risk management requirements. The new domain references SCRM criteria in NIST Special Publication (SP) 800-53, Revision, *Security and Privacy Controls for Information Systems and Organizations*. To provide agencies with sufficient time to fully implement NIST SP 800-53, Revision. 5, in accordance with OMB Circular No. A-130, these new metrics were not considered for the purposes of calculating the Identify framework function rating in FY 2021.

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

Evaluation Results

We determined the maturity level for each FISMA domain based on the responses to the questions contained in the FISMA Reporting Metrics and testing for each domain. The Council had GrantSolutions and RAAMS (prior to October 2, 2020) for award management, PIPER for program data management (as of October 3, 2020), and MERLIN for metadata. While there were changes to the Executive Director, the Council's Chief Information Officer (CIO) and the IT controls, processes, and personnel did not change since the prior year's FISMA evaluation. We also considered the 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 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 to 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 Consistently Implemented. The Council had defined supply chain policies and procedures. The Council managed its supply chain risks by purchasing products from trusted and approved manufacturers. The Council's OSN is considered a server-less network with a *Federal Information Processing Standards Publication* (FIPS) 199 rating of 'low.'[14]Although the maturity level of this domain was Consistently Implemented, our testing found no exceptions, and the controls were operating as intended. 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. Given the Council did not own a network server and did not have a general support system, its primary configuration management considerations were related to the standard configuration of their laptops. Our testing

[14] 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

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

Identity and Access Management: We determined the Council's overall maturity level for the Identity and Access Management program was Consistently Implemented. The Council had to manage the Identity, Credential, and Access Management (ICAM) 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, the Council did not use automated tools to inventory and manage accounts and perform segregation of duties/least privilege reviews. Although the maturity level of this domain was Consistently Implemented, our testing for this domain found no exceptions, and the controls were operating as intended. We concluded the Council's ICAM program controls in place were effective.

Data Protection and Privacy: We determined the Council's overall maturity level for the Data Protection and 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 whose 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 for this domain found no exceptions, and the controls were operating as intended. We concluded the Council's Data Protection and Privacy program controls in place were effective.

Security Training: We determined the Council's overall maturity level for the Security Training program was Managed and Measurable. Our testing of employees' security awareness and role-based training found no exceptions, and the 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. 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 Consistently Implemented. Given the Council did not own network servers and had no general support system, the Council had limited exposure to the possibility of security incidents. The Council only had part-time incident response team members who served more as a virtual incident response team. 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

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

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 and did not have a general support system, 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.

We concluded, consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, the Council's information security program and practices were established and 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, 2020 through June 30, 2021, 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, 2020 through June 30, 2021.

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. WebTA hosted by the U.S. Department of Agriculture National Finance Center;
2. Administrative Resource Center (ARC) to record financial transactions in Oracle Federal Financials (Oracle) for financial management and report processing hosted by the Department of the Treasury's Bureau of the Fiscal Service;
3. Metadata Records Library and Information Network (MERLIN) for metadata hosted by U.S. Geological Survey;
4. GrantSolutions for awards management hosted by U.S. Department of Health and Human Services and Restoration Assistance and Award Management System (RAAMS) hosted by U.S. Geological Survey;
5. Program Information Platform for Ecosystem Restoration (PIPER) for program data management hosted by U.S. Geological Survey;
6. Electronic records management hosted by National Archives and Records Administration to record management transactions in Electronic Record Archives (ERA);
7. email and G Suite hosted by U.S Department of Commerce's National Oceanic and Atmospheric Administration (NOAA); and
8. Continuous Diagnostic Monitoring and EINSTEIN capabilities hosting services by the Department of Homeland Security (DHS).

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, 2020, and June 30, 2021.

We determined the effectiveness of the Council's security program and practices by evaluating the following five Cybersecurity Framework security functions (key performance areas) outlined in the annual *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.1* (May 12, 2021) (FISMA Reporting Metrics) as follows:

- Identify, which includes questions pertaining to Risk Management and Supply Chain Risk Management (SCRM);

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

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

Methodology

The overall strategy of our evaluation considered the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53 Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations,* NIST SP 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations,* the FISMA Reporting Metrics from the Council of the Inspectors General on Integrity and Efficiency (CIGIE), Office of Management and Budget (OMB), and Department of Homeland Security (DHS), and the Council's policies and procedures. Appendix I shows the FISMA questions followed by the narrative of the maturity level, the criteria, and our test procedures. Our testing procedures were developed from NIST SP 800-53A Revision 4. For each of the FISMA questions, 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[15], in accordance with the FISMA Reporting Metrics.

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 (IT) 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 66 metric questions, we tested the entire population of administrative controls of the Council. The application controls were the responsibility of the Council's service providers.

We conducted the FISMA evaluation in accordance with the *Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation*, issued January 2012,

[15] Per the FISMA Reporting Metrics, we assessed the maturity levels of the Supply Chain Risk Management metrics, but this domain was not considered in the overall maturity results used in determining the effectiveness of the Identify function rating and the overall security program.

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

and subsequent revisions, OMB guidance,[16] FISMA Reporting Metrics, NIST guidance,[17] and the Council's policies and procedures.

[16] OMB Circular No. A-130, "*Managing Information as a Strategic Resource"* and OMB Memorandum M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirement.*
[17] NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations dated April, 2013;* and NIST *Framework for Improving Critical Infrastructure Cybersecurity version 1.1, dated April 16, 2018.*

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

Criteria

We focused our *FY 2021 Inspector General Federal Information Security Modernization Act of 2014* (FISMA) evaluation approach on Federal information security guidelines developed by the Gulf Coast Ecosystem Restoration Council (Council), National Institute of Standards and Technology (NIST), and Office of Management and Budget (OMB). NIST Special Publications (SPs) provide guidelines that were considered essential to the development and implementation of the Council's security programs. The following is a listing of the criteria used in the performance of the Fiscal Year 2021 FISMA evaluation:

Council

- Gulf Coast Council (GCC)-IT-06-AC-Access Control Policy
- GCC-IT-07-AU-Audit and Accountability Procedures
- GCC-IT-08-AT-Awareness and Training Procedures
- GCC-IT-09-CM-Configuration Management Procedures
- GCC-IT-10-CP-Contingency Planning Procedures
- GCC-IT-11-IA-Identification and Authentication Procedure
- GCC-IT-12-IR-Incident Response Procedures
- GCC-IT-13-MA-System Maintenance Policy and Procedures
- GCC-IT-14-MP-Media protection Procedures
- GCC-IT-15-PP-Personnel Security
- GCC-IT-16-PE-Physical and Environmental Protection
- GCC-IT-17-PL-Security Planning Policy and Procedures
- GCC-IT-19-RA-Risk Assessment Procedures
- GCC-IT-20-CC-Security Assessment and Authorization Procedures
- GCC-IT-21-SC Security Assessment and Authorization
- GCC-IT-22-SI System and Information Integrity Procedures
- GCC-IT-23-SA-System and Services Acquisitions
- GCC-IT-24-Mobile Device Policy
- GCC-IT-25-Mobile Code Technologies
- GCC-IT-26-Sanitization Procedures

NIST Federal Information Processing Standards (FIPS) and Special Publications

- 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 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
- NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*

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

- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*
- NIST SP 800-37, Revision 2, *Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- 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 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-53 Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*
- NIST SP 800-60, Revision 1, *Volume I: 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, *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)
- NIST Interagency Report 8286, Integrating Cybersecurity and Enterprise Risk Management (ERM)

OMB Policy Directives

- OMB Memorandum M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*
- OMB Memorandum M-20-32, *Improving Vulnerability Identification, Management, andRemediation*
- OMB Memorandum M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative*

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

- OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies byEnhancing the High Value Asset Program*
- 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 Memorandum M-17-26, *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda*
- OMB Circular No. A-123, *Management Responsibility for Internal Control*
- OMB Circular No. A-130, *Managing Information as a Strategic Resource*

DHS

- FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.1 May 12, 2021
- DHS Binding Operational Directive 20-01, *Develop and Publish a Vulnerability Disclosure Policy*

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

Appendix I: FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics

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

Key Changes to the FY 2021 IG FISMA Metrics

One of the goals of the annual *Federal Information Security Modernization Act of 2014* (FISMA) evaluations is to assess agencies' progress toward achieving outcomes that strengthen Federal cybersecurity, including implementing priorities and best practices. One such area is increasing the maturity of the Federal Government's Supply Chain Risk Management (SCRM) practices. As noted in the *Federal Acquisition Supply Chain Security Act of 2018*, agencies are required to assess, avoid, mitigate, accept, or transfer supply chain risks. The *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (FISMA Reporting Metrics) include a new domain on SCRM within the Identify function. This new domain focuses on the maturity of agency SCRM strategies, policies and procedures, plans, and processes to ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain risk management requirements. The new domain references SCRM criteria in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*. To provide agencies with sufficient time to fully implement NIST SP 800-53, Revision 5, in accordance with Office of Management and Budget (OMB) Circular No. A-130, these new metrics should not be considered for the purposes of the Identify framework function rating. However, NIST SP 800-53, Revision 5 would be applicable for any selected systems that are undergoing a major change or an Authorization to Operate during the performance audit period.

Also, within the Identify function, specific metric questions have been reorganized and reworded to focus on the degree to which cyber risk management processes are integrated with enterprise risk management (ERM) processes. As an example, Inspectors General (IG) are directed to evaluate how cybersecurity risk registers are used to communicate information at the information system, mission/business process, and organizational levels. These changes are consistent with NIST Interagency Report 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*, which provides guidance to help organizations improve the cybersecurity risk information they provide as inputs to their enterprise ERM programs.

Furthermore, OMB has issued guidance on improving vulnerability identification, management, and remediation. Specifically, OMB M-20-32, *Improving Vulnerability Identification, Management, and Remediation*, September 2, 2020, provides guidance to federal agencies on collaborating with members of the public to find and report vulnerabilities on federal information systems. In addition, Department of Homeland Security (DHS) Binding Operational Directive 20-01, *Develop and Publish a VulnerabilityDisclosure Policy*, September 2, 2020, provides guidance on the development and publishing of an agency's vulnerability disclosure policy and supporting handling procedures. The FISMA Reporting Metrics include a new question (#24) to measure the extent to which agencies utilize a vulnerability disclosure policy (VDP) as part of their vulnerability management program for internet-accessible federal systems.

In addition, the FISMA Reporting Metrics related to the implementation of policies and procedures have been reorganized and streamlined to reduce duplication and redundancies. Furthermore, a new Frequently Asked Question (FAQ) section provides additional guidance to IGs.

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

Risk Management

Identify Function Area

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. 4: CA-3, PM-5, and CM-8; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2021 CIO FISMA Metrics: 1.1, 1.1.5 and 1.4, OMB A-130, NIST SP 800-37, Rev. 2: Task P-18).[18]
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 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 (TIC) 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 used eight cloud-based systems and services that were hosted by third parties 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.

[18] Abbreviations: (CA) Security Assessment and Authorization, (PM) Program Management, (CM) Configuration Management, (ID.AM) Asset Management, and (CIO) Chief Information Officer.

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

Risk Management

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. 4: CA-7 and CM-8; NIST SP 800-137; NIST IR 8011; Federal Enterprise Architecture (FEA) Framework, v2; FY2021 CIO FISMA Metrics: 1.2, 1.3, 2.2, 3.9, CSF: ID.AM-1; NIST SP 800-37, Rev. 2: Task P-10)?[19]
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 for 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 CIO tracks and maintains an inventory of its hardware assets and monitors its assets monthly. As the Council had very few information technology (IT) assets, it was more cost-effective to maintain a list of hardware assets 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 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.

[19] Abbreviations: (GFE) Government Furnished Equipment and (NISTIR) National Institute of Standards and Technology Interagency or Internal Report.

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

Risk Management

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. 4: CA-7, CM-8, and CM-10; NIST SP 800-137; NIST IR 8011; FEA Framework, v2; FY 2021 CIO FISMA Metrics: 1.2.5, 1.3.3, 1.3.9, 3.10; CSF: ID.AM-2; NIST SP 800-37, Rev. 2: Task P-10)?[20]
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 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 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.

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

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

Risk Management

Question 4
To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets (NIST SP 800-53 Rev. 4: RA-2, PM-7, and PM-11; NIST SP 800-60; NIST SP 800-37 (Rev. 2); CSF: ID.BE-3, ID.AM-5, and ID.SC-2; FIPS 199; FY 2021 CIO FISMA Metrics: 1.1; OMB M-19-03; NIST SP 800-37, Rev. 2: Task C-2, C-3, P-4, P-12, P-13, S-1, S-3, NIST IR 8170)?[21]
Consistently Implemented
The organization consistently implements its policies, procedures, and processes for system categorization, review, and communication, including for high value assets, as appropriate. Security categorizations consider potential adverse impacts to organization operations, organizational assets, individuals, other organizations, and the Nation. System categorization levels are used to guide risk management decisions, such as the allocation, selection, and implementation of appropriate control baselines. **MET –** The Council had a small organizational structure without high value assets, and other agencies host and support its cloud-based systems through interagency agreements except for the Council's OSN which was managed by the CIO. The third party system service providers were responsible for evaluating the risk to information systems from the supporting business functions and mission impacts.
Managed and Measurable
The organization ensures the risk-based allocation of resources based on system categorization, including for the protection of high value assets, as appropriate, through collaboration and data-driven prioritization. **NOT MET –** The Council did not have high value assets. As such, this maturity level was not applicable to the Council's environment.

[21] Abbreviations: (RA) Risk Assessment, (ID.BE) Business Environment, (ID.SC) Supply Chain Risk Management, and (FIPS) Federal Information Processing Standards.

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

Risk Management

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. 4: RA-3, 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?[22]
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 serve as an input into the organization's enterprise risk management program. The organization consistently monitors the effectiveness of risk responses to ensure that risk tolerances are maintained at an appropriate level. ***The organization ensures that information in cybersecurity risk registers is obtained accurately, consistently, and in a reproducible format and is used to (i) quantify and aggregate security risks, (ii) normalize cybersecurity risk information across organizational units, and (iii) prioritize operational risk response*** **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 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 is obtained accurately and consistently.

[22] Abbreviation: (ID.RM) Risk Management Strategy.

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

Risk Management

Question 5
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, based on our examination of the evidence, the Council did not fully integrate its organizational and business processes at all levels of the agency, nor have they 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

Risk Management

Question 6
To what extent does the organization utilize an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain (*Federal Information Technology Acquisition Reform Act* (FITARA), NIST SP 800-39; NIST SP 800-160; NIST SP 800-37 (Rev. 2) Task P-16; OMB M-19-03; OMB M-15-14, FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-163, Rev. 1 CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?[23]
Consistently Implemented
The organization has consistently implemented its security architecture across the enterprise, business process, and system levels. System security engineering principles are followed and include assessing the impacts to the organizations information security architecture prior to introducing information system changes into the organization's environment. ***In addition, the organization employs a software assurance process for mobile applications.*** **MET –** The Council is a micro-agency with a unique organizational size and structure. The Council relied on third party system service providers and only controlled its 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 TIC portal. The Council relied on third party system service providers to provide security functionality and allocation of security controls. The Council had stand-alone mobile devices that were not connected to the Council's OSN; therefore, they did not employ a software assurance process for mobile applications.
Managed and Measurable
The organization's information security architecture is integrated with its systems development lifecycle and defines and directs implementation of security methods, mechanisms, and capabilities to both the Information and Communications Technology (ICT) supply chain and the organization's information systems. **NOT MET –** The Council's information security architecture was not integrated with its systems development lifecycle and did not define and direct the implementation of security methods, mechanisms, and capabilities to both the ICT supply chain and its information systems.

[23] Abbreviations: (PL) Planning, (SA) System and Service Acquisition, and (PR.IP) Information Protection Processes and Procedures.

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

Risk Management

Question 7
To what extent have the roles and responsibilities of internal and external stakeholders involved in cybersecurity risk management processes been defined, communicated, and implemented across the organization (NIST SP 800-39: Section 2.3.1, 2.3.2, and Appendix D; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID. GV-2; OMB A-123; NIST SP 800-37 (Rev. 2) Section 2.8 and Task P-1; OMB M-19-03)?[24]
Managed and Measurable
Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement cybersecurity risk management activities and integrate those activities with enterprise risk management processes, as appropriate. Further, stakeholders involved in cybersecurity risk management are held accountable for carrying out their roles and responsibilities effectively. **MET** - The Council had a unique organizational size and structure. The Council CIO was the only employee responsible for all IT related activities. The CIO was intimately involved in all aspects of the Council's risk management program and was aware of every important decision involving its IT operations and its risk management program. The CIO communicated to the management to address the risk management capabilities of the Council. Additionally, the Council had documented the identified risks and developed a defined strategy to mitigate those risks. As such, we determined the maturity level as met based on the above information.
Optimized
The organization utilizes an integrated governance structure, in accordance with A-123, and associated review processes (e.g., ERM councils or IT investment review boards) to support the integration of roles and responsibilities for cybersecurity risk management and ERM. **NOT MET** – The Council's risk management program did not address the full spectrum of an agency's risk portfolio across all organizational (major units, offices, and lines of business) and business (agency mission, programs, projects, etc.) aspects. Due to the unique organizational size and structure of the Council, it may be misleading to state the maturity level of the Council as Optimized.

[24] Abbreviation: (ID.GV) Governance.

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

Risk Management

Question 8
To what extent has the organization ensured that plans of action and milestones (POA&Ms) are utilized for effectively mitigating security weaknesses (NIST SP 800-53 Rev. 4: CA-5; NIST SP 800-37 (Rev. 2) Task A-6, R-3; OMB M-04-14, M-19-03, CSF v1.1, ID.RA-6)?[25]
Managed and Measurable
The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its POA&M activities and uses that information to make appropriate adjustments, as needed, to ensure that its risk posture is maintained. **MET –** The Council tracked POA&Ms on a spreadsheet and had developed a mitigation plan to monitor and analyze qualitative and quantitative performance measures on the effectiveness of its POA&M activities. The Council used the tracker to make appropriate adjustments, as needed, to ensure that its risk posture is maintained.
Optimized
The organization employs automation to correlate security weaknesses amongst information systems and identify enterprise-wide trends and solutions in a near real- time basis. Furthermore, processes are in place to identify and manage emerging risks, in addition to known security weaknesses. **NOT MET -** Given the unique structure of the Council, the Council did not employ automation to correlate security weaknesses amongst information systems and identify enterprise-wide trends and solutions in a near real-time basis. Furthermore, processes were not in place to identify and manage emerging risks, in addition to known security weaknesses.

[25] Abbreviation: (ID.RA) Risk Assessment.

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

Risk Management

Question 9
To what extent does the organization ensure that information about cybersecurity risks is communicated in a timely and effective manner to appropriate internal and external stakeholders (OMB A-123; OMB Circular A-11 and OMB M-19-03; CSF: Section 3.3; NIST SP 800-37 (Rev. 2) Task M-5; SECURE Technology Act: s. 1326, NIST IR 8170 and 8286)?
Managed and Measurable
The organization employs robust diagnostic and reporting frameworks, including dashboards that facilitate a portfolio view of cybersecurity risks across the organization. The dashboard presents qualitative and quantitative metrics that provide indicators of cybersecurity risk. ***Cybersecurity risks are integrated into enterprise level dashboards and reporting frameworks.*** ***To facilitate timely, consistent, and effective communication of cybersecurity risks, the organization ensures that data supporting the cybersecurity risk register, or other comparable mechanism, are obtained accurately, consistently, and in a reproducible format and is used to*** • ***Quantify and aggregate security risks*** • ***Normalize information across organizational units*** • ***Prioritize operational risk response activities*** **MET–** The Council employed robust diagnostic and reporting frameworks, including dashboards which facilitated a portfolio view of interrelated risks across the organization. The dashboards presented qualitative and quantitative metrics that provided indicators of risk. Cybersecurity risks were integrated into enterprise level dashboards and reporting frameworks.
Optimized
Using risk profiles and dynamic reporting mechanisms, cybersecurity risk information is incorporated into the organization's enterprise risk management program and utilized to provide a fully integrated, prioritized, enterprise-wide view of organizational risks to drive strategic and business decisions. ***Cyber risks are normalized and translated at the organizational level to support a fully integrated, prioritized, enterprise-wide view of organizational risks to drive strategic and business decisions.*** **NOT MET –** Due to the unique organizational structure, the Council's cybersecurity risk information was not incorporated into the organization's enterprise risk management program and was not utilized to provide a fully integrated, prioritized, enterprise-wide view of organizational risks to drive strategic and business decisions. Cyber risks were not normalized and translated at the organizational level to support a fully integrated, prioritized, enterprise-wide view of organizational risks to drive strategic and business decisions.

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

Risk Management

Question 10
To what extent does the organization utilize technology/ automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123 and NIST IR 8286)?
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 to organizational systems and data. ***In addition, the organization ensures that cybersecurity risk management information is integrated into ERM reporting tools, such as a governance, risk management, and compliance tool), as appropriate.*** **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 impact on organizational systems and data. In addition, the cybersecurity risk management information was not integrated into ERM reporting tools.

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

Risk Management

Question 11
Provide any additional information on the effectiveness (positive or negative) of the organization's risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?
Question 1 – Maturity Level: Managed and Measurable
Question 2 – Maturity Level: Managed and Measurable
Question 3 – Maturity Level: Managed and Measurable
Question 4 – Maturity Level: Consistently Implemented
Question 5 – Maturity Level: Managed and Measurable
Question 6 – Maturity Level: Consistently Implemented
Question 7 – Maturity Level: Managed and Measurable
Question 8 – Maturity Level: Managed and Measurable
Question 9 – Maturity Level: Managed and Measurable
Question 10 – Maturity Level: Consistently Implemented
OVERALL: Managed and Measurable
Based on the maturity levels generated from the questions and all testing performed in the Risk Management domain, we concluded the Council's overall maturity level for the Risk Management program was Managed and Measurable. Due to the small organizational structure, the Council had the ability to operate more efficiently and effectively compared to larger Federal agencies. The CIO was intimately involved in all aspects of the Council's risk management program and was aware of every important decision involving its IT operations and its risk management program. The Council defined the priority levels for its information systems 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 help to improve and continuously update the Council's risk management policies, procedures, and strategy, including methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk.

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

Supply Chain Risk Management
NOTE: This section was not considered in the Identity framework function rating per FY21 IG FISMA Reporting Metrics.

Question 12
To what extent does the organization utilize an organization wide SCRM strategy to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services? (The Federal Acquisition Supply Chain Security Act of 2018 (H.R. 7327, 41 USC Chap. 13 Sub chap. III and Chap. 47, P.L. 115-390) (Dec. 21, 2018), NIST SP 800-53, Rev. 5, PM-30, NIST IR 8276)?[26]
Ad Hoc
The organization has not defined and communicated an organization wide SCRM strategy. **MET -** The Council had developed SCRM policies and procedures that described the supply chain process. However, the Council did not define and communicate an organization wide SCRM strategy.
Defined
The organization has defined and communicated an organization wide SCRM strategy. The strategy addresses: - ***SCRM risk appetite and tolerance*** - ***SCRM strategies or controls*** - ***Processes for consistently evaluating and monitoring supply chain risk*** - ***Approaches for implementing and communicating the SCRM strategy*** - ***Associated roles and responsibilities*** **NOT MET –** The Council did not define and communicate an organization wide SCRM strategy that addressed the above elements.

[26] Abbreviations: (P.L.) Public Law and (USC) U.S. Code.

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

Supply Chain Risk Management

Question 13
To what extent does the organization utilize SCRM policies and procedures to manage SCRM activities at all organizational tiers (*The Federal Acquisition Supply Chain Security Act of 2018*, NIST 800-53, Rev. 5, SR-1, NIST CSF v1.1, ID.SC-1 and ID.SC-5, NIST IR 8276)?[27]
Consistently Implemented
The organization consistently implements its policies, procedures, and processes for managing supply chain risks for [organizationally-defined] products, systems, and services provided by third parties. ***Further, the organization utilizes lessons learned in implementation to review and update its SCRM policies, procedures, and processes in an organization defined timeframe.*** **MET -** The Council has laptops and mobile devices as part of its inventory. The CIO directly purchases those laptops and mobile devices from the manufacturer. All purchases were reviewed by either the Director of Administration (DoA) or the CIO, or both. Both CIO and DoA attended training on purchasing, including on prohibited items or vendors. The CIO reviews all IT purchases and ensures that authorized vendors are used. The Council's OSN is considered a server-less network, with a FIPS 199 rating of 'low'.[28] As such, purchasing from trusted and approved manufacturers does not increase the threat of risks to the system. The Council implements its policies, procedures, and processes by buying supply chain components directly from the manufacturer and manages its supply chain risk. The Council did not develop any lessons learned for FY 21 as this is a new requirement based on FY 21 FISMA Reporting Metrics.
Managed and Measurable
The organization monitors, analyzes, and reports on the qualitative and quantitative performance measures used to gauge the effectiveness of its SCRM policies and procedures and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format. ***The organization has integrated SCRM processes across its enterprise, including personnel security and physical security programs, hardware, software, and firmware development processes, configuration management tools, techniques, and measures to maintain provenance (as appropriate); shipping and handling procedures; and programs, processes, or procedures associated with the production and distribution of supply chain elements.*** **NOT MET -** The Council did not monitor, analyze, and report on the qualitative and quantitative performance measures used to gauge the effectiveness of its SCRM policies and procedures. In addition, the Council did not integrate SCRM processes across its enterprise.

[27] Abbreviation: (SR) Supply Chain Risk Management.
[28] FIPS 199, *Federal Information Processing Standards Publication, 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

Supply Chain Risk Management

Question 14
To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements. (The Federal Acquisition Supply Chain Security Act of 2018, NIST SP 800-53 REV. 5: SA-4, SR-3, SR-5, 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)?[29]
Ad Hoc
The organization has not defined and communicated policies, procedures, and processes to ensure that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and supply chain risk management requirements. **MET –** The Council did not define and communicate policies, procedures, and processes to ensure that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and supply chain risk management requirements.
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 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 described its process of supply chain policies and procedures in its OSN System Security Plan. However, the Council did not define the minimum above components as required by the Defined maturity level.

[29] Abbreviation: (FedRAMP) Federal Risk and Authorization Management Program.

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

Supply Chain Risk Management

Question 15
To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization's systems? (800-53 rev 5 SR-11, 11 (1), and 11(2)
Consistently Implemented
The organization consistently implements its component authenticity policies and procedures. Further, the organization: • ***Provides component authenticity/anti-counterfeit training for designated personnel.*** • ***Maintains configuration control over organizationally defined system components that are awaiting repair and service or repaired components awaiting return to service.*** **MET -** The Council consistently implemented its component authenticity policies and procedures by providing component authenticity/anti-counterfeit training for designated personnel. The CIO is the lone designated personnel who takes the component authenticity/anti-counterfeit and had taken the training through third party provider. In addition, the Council maintains configuration control over organizationally defined system components that are awaiting repair and service.
Managed and Measurable
The organization monitors, analyzes, and reports on the qualitative and quantitative performance measures used to gauge the effectiveness of its component authenticity policies and procedures and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format. ***In addition, the organization has incorporated component authenticity controls into its continuous monitoring practices.*** **NOT MET -** The Council did not monitor, analyze, and report on the qualitative and quantitative performance measures to gauge the effectiveness of its component authenticity policies and procedures. However, the Council had incorporated component authenticity controls into its continuous monitoring practices through its System Security Plan.

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

Supply Chain Risk Management

Question 16
Provide any additional information on the effectiveness (positive or negative) of the organization's supply chain risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?
Question 12 – Maturity Level: Ad Hoc
Question 13 – Maturity Level: Consistently Implemented
Question 14 – Maturity Level: Ad Hoc
Question 15 – Maturity Level: Consistently Implemented
OVERALL: Consistently Implemented
Based on the maturity levels generated from the questions and all testing performed in the Supply Chain Risk Management domain, we determined the Council's overall maturity level for the Supply Chain Risk Management program as Consistently Implemented. Per the guidance in the FISMA Reporting Metrics, if there is a tie between two maturity levels the highest maturity level applies. The Council has a simple, flat organizational structure without formal departments and layers of management typically found in larger organizations. As a result, the CIO was the lone IT personnel and was directly responsible for monitoring all IT assets. This allowed the Council to operate more quickly, efficiently, and effectively than larger organizations, because ideas or requests did not need to climb up the levels of management before approval.

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

Configuration Management

Protect Function Area

Question 17
To what extent have the roles and responsibilities of configuration management stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: CM-1; NIST SP 800-128: Section 2.4)?
Managed and Measurable
Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively perform information system configuration management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively. **MET** – The Council CIO was the lone IT personnel and was directly responsible for managing all information assets in the organization. The Council is a micro-agency with a unique organizational structure. The Council's resources (people, processes, and technology) were allocated in a risk-based manner for stakeholders to effectively perform information system configuration management activities. Further, stakeholders were held accountable for carrying out their roles and responsibilities effectively.
Optimized
Per the FISMA Reporting Metrics, this maturity level was not applicable to this question.

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

Configuration Management

Question 18
To what extent does the organization utilize an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems (NIST SP 800-128: Section 2.3.2; NIST SP 800-53 REV. 4: CM-9)?[30]
Managed and Measurable
The organization monitors, analyzes, and reports to stakeholders qualitative and quantitative performance measures on the effectiveness of its configuration management plan, uses this information to take corrective actions when necessary, and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format. **MET –** The Council monitored, analyzed, and reported to stakeholders qualitative and quantitative performance measures on the effectiveness of its configuration management plan, and used this information to take corrective actions when necessary, and ensured data supporting the metrics were obtained accurately, consistently, and in a reproducible format. The Council reviewed the baseline configuration and system component inventory annually. The Council's contractor provided monthly reports to the Council's management that included patch management, hardware, and software scans.
Optimized
The organization utilizes automation to adapt its configuration management plan and related processes and activities to a changing cybersecurity landscape on a near real-time basis (as defined by the organization). **NOT MET –** Due to the unique structure of the Council's information systems, the Council did not utilize automation to adapt its configuration management plan and related processes and activities to a changing cybersecurity landscape on a near real-time basis (as defined by the organization).

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

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

Configuration Management

Question 19
To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53 REV. 4: CM-2 and CM-8; FY 2021 CIO FISMA Metrics: 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7 and PR. IP-1)?[31]
Managed and Measurable
The organization employs automated mechanisms (such as application whitelisting and network management tools) to detect unauthorized hardware, software, and firmware and unauthorized changes to hardware, software, and firmware. **MET –** The Council employed automated mechanism through the use of dashboards to detect unauthorized hardware, software, and firmware and unauthorized changes to hardware, software, and firmware. The Council's contractor provided monthly reports to the Council's management that included patch management, hardware, and software scans.
Optimized
The organization utilizes technology to implement a centralized baseline configuration and information system component inventory process that includes information from all organization systems (hardware and software) and is updated in a near real-time basis. **NOT MET –** Due to the unique structure of the Council's information system, the Council did not utilize technology to implement a centralized baseline configuration and information system component inventory process that includes information from all organization systems (hardware and software) and is updated in a near real-time basis.

[31] Abbreviations: (DE.CM) Security Continuous Monitoring and (PR.IP) Information Protection Processes and Procedures.

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

Configuration Management

Question 20
To what extent does the organization utilize configuration settings/common secure configurations for its information systems? (NIST SP 800-53 REV. 4: CM-6, CM-7, RA-5, and SI-2; NIST SP 800-70, Rev. 4, FY 2021 CIO FISMA Metrics: 2.1, 2.2, 4.3; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1 and DE.CM-8)?[32]
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.

[32] Abbreviations: (SI) System and Information Integrity, (SANS) SysAdmin, Audit, Network and Security, and (CIS) Center for Internet Security.

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

Configuration Management

Question 21
To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53 REV. 4: CM-3, RA-5, SI-2, and SI-3; NIST SP 800-40, Rev. 3; SANS/CIS Top 20, Control 4.5; FY 2021 CIO FISMA Metrics: 1.3.7, 1.3.8, 2.13, 2.14; CSF: ID.RA-1; DHS Binding Operational Directive (BOD)18-02 and 19-02)?
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 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,such as through patch sourcing and testing.

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

Configuration Management

Question 22
To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-19-26, DHS-CISA TIC 3.0 Core Guidance Documents)?[33]
Managed and Measurable
The organization, in accordance with OMB M-19-26, DHS guidance, and its cloud strategy is ensuring that its TIC implementation remains flexible and that its policies, procedures, and information security program are adapting to meet the security capabilities outlined in TIC initiative, consistent with OMB M-19-26. ***The organization monitors and reviews the implemented TIC 3.0 use cases to determine effectiveness and incorporates new/different use cases, as appropriate.*** **MET –** The Council has implemented the TIC initiative per OMB M-19-26, DHS guidance. The Council monitors and reviews the implemented TIC 3.0 use cases to determine the effectiveness of TIC and incorporates new/different use cases, as appropriate.
Optimized
Per the FISMA Reporting Metrics, this maturity level was not applicable to this question.

[33] Abbreviation: (CISA) Cybersecurity and Infrastructure Security Agency.

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

Configuration Management

Question 23
To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, as appropriate (NIST SP 800-53 REV. 4: CM-2, CM-3 and CM-4;CSF: PR.IP-3)?
Managed and Measurable
The organization monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its change control activities and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format. ***In addition, the organization implements [organizationally defined security responses] if baseline configurations are changed in an unauthorized manner.*** **MET –** The Council monitored, analyzed, and reported qualitative and quantitative performance measures on the effectiveness of its change control activities and ensured that data supporting the metrics is obtained accurately, consistently, and in a reproducible format. In addition, the Council implemented security responses if baseline configurations are changed in an unauthorized manner.
Optimized
The organization utilizes automation to improve the accuracy, consistency, and availability of configuration change control and configuration baseline information. ***Automation is also used to provide data aggregation and correlation capabilities, alerting mechanisms, and dashboards on change control activities to support risk-based decision making across the organization.*** **NOT MET –** Due to the unique structure of the Council's information systems, the Council did not utilize automation to improve the accuracy, consistency, and availability of configuration change control and configuration baseline information.

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

Configuration Management

Question 24
To what extent does the organization utilize a vulnerability disclosure policy (VDP) as part of its vulnerability management program for internet-accessible federal systems (OMB M- 20-32 and DHS BOD 20-01)?
Defined
The organization has developed, documented, and publicly disseminated a comprehensive VDP. The following elements are addressed: • ***The systems in scope;*** • ***Types of testing allowed;*** • ***Reporting mechanisms;*** • ***Timely feedback; and*** • ***Remediation.*** ***In addition, the organization has updated its vulnerability disclosure handling procedures to support the implementation of its VDP.*** **MET -** The Council has developed, documented, and publicly disseminated a comprehensive VDP. In addition, the Council has updated its vulnerability disclosure handling procedures to support the implementation of its VDP.
Consistently Implemented
The organization consistently implements its VDP policy. In addition, the organization: • ***Has updated the relevant fields at the .gov registrar to ensure appropriate reporting by the public;*** • ***Ensures that newly launched internet accessible systems and services, and at least 50% of internet-accessible systems, are included in the scope of its VDP; and*** • ***Increases the scope of systems covered by its VDP, in accordance with DHS BOD 20-01.*** **NOT MET –** The Council did not own or host its systems. These are hosted with the third party providers through interagency agreements. As such, the Council is not responsible for this maturity level.

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

Configuration Management

Question 25
Provide any additional information on the effectiveness (positive or negative) of the organization's configuration management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?
Question 17 – Maturity Level: Managed and Measurable
Question 18 – Maturity Level: Managed and Measurable
Question 19 – Maturity Level: Managed and Measurable
Question 20 – Maturity Level: Managed and Measurable
Question 21 – Maturity Level: Managed and Measurable
Question 22 – Maturity Level: Managed and Measurable
Question 23 – Maturity Level: Managed and Measurable
Question 24 – Maturity Level: Defined
OVERALL: Managed and Measurable
Based on the maturity levels generated from the questions and all testing performed in the Configuration Management domain, we concluded the overall maturity level for the Council's Configuration Management program was Managed and Measurable. The Council had a simple, flat organizational structure without formal departments and layers of management typically found in larger organizations. As a result, the CIO was the lone IT personnel and was directly responsible for monitoring all IT assets. Further, no IT decisions were made without the CIO's direct involvement and approval. This allowed the Council to operate more efficiently and effectively than larger organizations because ideas or requests did not need to climb up the levels of management before approval.

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

Identity and Access Management

Question 26
To what degree have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: AC-1, IA-1, and PS-1; NIST SP 800-63-3 and 800-63A, B, and C; Federal Identity, Credential, and Access Management (FICAM) playbooks and guidance (see idmanagement.gov), OMB M-19-17)?[34]
Managed and Measurable
Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement identity, credential, and access management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively. **MET –** Due to the Council's organizational structure without formal departments and layers of management typically found in larger organizations, we determined the Council had adequate resources (people, processes, and technology) to consistently implement ICAM activities. Furthermore, we determined the CIO submitted quarterly reports to the senior official of the Council to discuss about IT program.
Optimized
In accordance with OMB M-19-17, the agency has implemented an integrated agency-wide ICAM office, team, or other governance structure in support of its ERM capability to effectively govern and enforce ICAM efforts. **NOT MET –** 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.

[34] Abbreviations: (AC) Access Control, (IA) Identification and Authentication, and (PS) Personnel Security.

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

Identity and Access Management

Question 27
To what extent does the organization utilize a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities (FICAM, OMB M- 19-17; NIST SP 800-53 REV. 4: AC-1 and IA-1; OMB M-19-17; SANS/CIS Top 20: 14.1. DHS ED 19-01; CSF: PR.AC-4 and 5)?[35]
Consistently Implemented
The organization is consistently implementing its ICAM policy, strategy, process, and technology solution road map and is on track to meet milestones. The strategy encompasses the entire organization, aligns with the FICAM and CDM requirements, and incorporates applicable Federal policies, standards, playbooks, and guidelines. ***Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its ICAM policy, strategy, and road map and making updates as needed.*** **MET –** The Council consistently implemented its ICAM policy, strategy, process, and technology solution road map and is on track to meet milestones. In addition, the Council captured, and shared lessons learned on the effectiveness of its ICAM policy, strategy, and road map and makes updates as needed.
Managed and Measurable
The organization integrates its ICAM strategy and activities with its enterprise architecture and the Federal ICAM architecture. ***The organization uses automated mechanisms (e.g. machine-based, or user-based enforcement), where appropriate, to manage the effective implementation of its ICAM policies, procedures, and strategy. Examples of automated mechanisms include network segmentation based on the label/classification of information stored; automatic removal/disabling of temporary/emergency/ inactive accounts; and use of automated tools to inventory and manage accounts and perform segregation of duties/least privilege reviews.*** **NOT MET –** The Council did not have an enterprise architecture like those available in a large organization. As such, the Council did not integrate its ICAM strategy and activities with its enterprise architecture and the Federal ICAM architecture. The Council did not use automated mechanisms (e.g., machine-based or user-based enforcement) to manage the effective implementation of its policies and procedures. Deployment of automated mechanisms may not be cost-effective considering the structure of the Council environment.

[35] Abbreviation: (ED) Emergency Directive and (PR.AC) Identity Management and Access Control.

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

Identity and Access Management

Question 28
To what extent has the organization developed and implemented processes for assigning position risk designations and performing appropriate personnel screening prior to granting access to its systems (NIST SP 800-53 REV. 4: PS-2 and PS-3; National Insider Threat Policy; CSF: PR. IP-11, OMB M-19-17)?
Consistently Implemented
The organization ensures that all personnel are assigned risk designations, appropriately screened prior to being granted system access, and rescreened periodically. **MET –** The CIO was the lone IT personnel and was directly responsible for implementing all identity, credential, and access management activities, including ensuring all new users were assigned an ID and initial passwords to login to their laptops. As his responsibility, the CIO ensured all personnel were assigned risk designations and were appropriately screened prior to being granted access to the system and rescreened periodically.
Managed and Measurable
The organization employs automation to centrally document, track, and share risk designations and screening information with necessary parties. **NOT MET –** Due to the unique structure of the Council's information systems, the Council did not employ automation to centrally document, track, and share risk designations and screening information with necessary parties.

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

Identity and Access Management

Question 29
To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non-privileged users) that access its systems are completed and maintained (NIST SP 800-53 REV. 4: AC-8, PL-4, and PS-6)?
Consistently Implemented
The organization ensures that access agreements for individuals are completed prior to access being granted to systems and are consistently maintained thereafter. The organization utilizes more specific/detailed agreements for privileged users or those with access to sensitive information, as appropriate. **MET** – The Council had a 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 and was directly responsible for implementing all identity, credential, and access management activities. He ensured access agreements for individuals were completed prior to access being granted to systems and were consistently maintained thereafter. Additionally, there was no sensitive information on the network. As such, the Council did not find it necessary to utilize more specific or detailed agreements. Given the small size of the organization and limited complexity of the IT environment, we determined the Council met the maturity level of Consistently Implemented for this question.
Managed and Measurable
The organization uses automation to manage and review user access agreements for privileged and non-privileged users. To the extent practical, this process is centralized. **NOT MET –** Due to the unique structure of the Council's information systems, the Council did not use automation to manage and review user access agreements for privileged and non-privileged users. To the extent practical, this process was not centralized.

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

Identity and Access Management

Questions 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 (HSPD-12; NIST SP 800-53 REV. 4:AC-17, IA-2, IA-5, IA-8, and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63, 800-157; FY 2021 CIO FISMA Metrics: 2.4, 2.7, CSF: PR.AC-1 and 6; OMB M-19-17, NIST SP 800-157)?[36]
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 the solution and all of the organization's systems interface with the solution, resulting in an ability to manage user (non-privileged) accounts and privileges centrally and report on 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 which 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.

[36] Abbreviations: (HSPD) Homeland Security Presidential Directive, (PIV) Personal Identity Verification and (PE) Physical and Environmental Protection.

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

Identity and Access Management

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 (HSPD-12; NIST SP 800-53 REV. 4: AC-17, PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63 and 800-157; OMB M-19-17, FY 2021 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; DHS ED 19-01)?
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 and was assigned a moderate-risk designation. The Council did not make changes to Domain Name System (DNS) records as it did not host 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 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.

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

Identity and Access Management

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 (FY 2021 CIO FISMA Metrics: 2.3, 2.5, 2.6, and 2.7; OMB M-19-17, NIST SP 800-53 REV. 4: 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).[37]
Consistently Implemented
The organization ensures that its processes for provisioning, managing, and reviewing privileged accounts are consistently implemented across the organization. The organization limits the functions that can be performed when using privileged accounts; limits the duration that privileged accounts can be logged in; limits the privileged functions that can be performed using remote access; and ensures that privileged user activities are logged and periodically reviewed. **MET–** The Council CIO was the lone IT personnel and was directly responsible for implementing all identity, credential, and access management activities. Given the small size of the organization and limited complexity of the IT environment, we determined the Council met the maturity level of Consistently Implemented for this question.
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. **NOT MET –** The Council did not employ 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.

[37] Abbreviation: (AU) Audit and Accountability.

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

Identity and Access Management

Question 33
To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions (NIST SP 800-53 REV. 4: AC-11, AC-12, AC-17, AC-19, AU-2, IA-7, SC-10, SC-13, and SI-4; CSF: PR.AC-3; and FY2021 CIO FISMA Metrics: 2.10 and 2.11).[38]
Consistently Implemented
The organization ensures that FIPS 140-2 validated cryptographic modules are implemented for its remote access connection method(s), remote access sessions time out after 30 minutes (or less), and that remote users' activities are logged and reviewed based on risk. **MET –** There were no permanent/continuous/ongoing remote access connections, only on-demand/transient access. Such a connection was only created when users requested assistance. The help desk employee could only gain access when the user had already logged in to their laptops. The connections used appropriate encryption, and users were automatically logged out after 30 minutes (or less) of inactivity.
Managed and Measurable
The organization ensures that end user devices have been appropriately configured prior to allowing remote access and restricts the ability of individuals to transfer data accessed remotely to non-authorized devices. **NOT MET –** The Council is a small organization that did not have the infrastructure, risks, or resources needed to employ processes to ensure end-user devices were appropriately configured prior to allowing remote access and did not restrict the ability of individuals to transfer data accessed remotely to non-authorized devices.

[38] Abbreviation: (SC) System and Communications Protection.

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

Identity and Access Management

Question 34
Provide any additional information on the effectiveness (positive or negative) of the organization's identity and access management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?
Question 26 – Maturity Level: Managed and Measurable
Question 27 – Maturity Level: Consistently Implemented
Question 28 – Maturity Level: Consistently Implemented
Question 29 – Maturity Level: Consistently Implemented
Question 30 – Maturity Level: Managed and Measurable
Question 31 – Maturity Level: Managed and Measurable
Question 32 – Maturity Level: Consistently Implemented
Question 33 – Maturity Level: Consistently Implemented
OVERALL: Consistently Implemented
Based on the maturity levels generated from the questions and all testing performed in the Identity and Access Management domain, we concluded the overall maturity level for the Council's Identity and Access Management program was Consistently Implemented. 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 Identity and Access Management program controls in place were effective**.** The Council had a simple, flat organizational structure without formal departments and layers of management typically found in larger organizations. As a result, the CIO was the lone IT personnel and was directly responsible for monitoring all IT assets. Further, no ICAM decisions were made without the CIO's direct involvement and approval. This allowed the Council to operate more efficiently and effectively than larger organizations because ideas or requests did not need to climb up the levels of management before approval.

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

Data Protection and Privacy

Question 35
To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems (NIST SP 800-122; NIST SP 800-37 (Rev. 2) Section 2.3, Task P-1; OMB M-20-04; OMB M-19-03; OMB A-130, Appendix I; CSF: ID. GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J, FY 2020 SAOP FISMA metrics, Sections 1 through 4, 5(b), NIST Privacy Framework)?[39]
Consistently Implemented
The organization consistently implements its privacy program by: • ***Dedicating appropriate resources to the program.*** • ***Maintaining an inventory of the collection and use of PII.*** • ***Conducting and maintaining privacy impact assessments and system of records notices for all applicable systems.*** • ***Reviewing and removing unnecessary PII collections on a regular basis (i.e., SSNs).*** • ***Using effective communications channels for disseminating privacy policies and procedures.*** • ***Ensuring that individuals are consistently performing the privacy roles and responsibilities that have been defined across the organization.*** **MET –** According to the Council's *Privacy Program Plan,* "None of the GCERC Systems create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII." The Council staff were trained to not store PII on laptops or Google Drive. In addition, the CIO performed searches of Google Drive on a quarterly basis to discover and remove any PII. The Council ensured each laptop had encryption enabled on the hard drive. The Council only had OSN directly under its control and other Council systems were managed by third party. Hence, the third party is responsible for its privacy controls.
Managed and Measurable
The organization monitors and analyses quantitative and qualitative performance measures on the effectiveness of its privacy activities and uses that information to make needed adjustments. The organization conducts an independent review of its privacy program and makes necessary improvements. **NOT MET –** The Council did not manage any systems that handle PII. As such, they did not monitor and analyze quantitative and qualitative performance measures on the effectiveness of its privacy activities and did not use the information to make needed adjustments. Furthermore, the Council did not conduct an independent review of its privacy program and make necessary improvements.

[39] Abbreviations: (AR) Accountability, Audit, and Risk Management and (SAOP) Senior Agency Official for Privacy.

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

Data Protection and Privacy

Question 36
To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle (NIST SP 800-53 REV. 4; Appendix J, SC-8, SC-28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2020 CIO FISMA Metrics: 2.8, 2.12; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR. IP-6)?[40] • Encryption of data at rest • Encryption of data in transit • Limitation of transfer to removable media • Sanitization of digital media prior to disposal or reuse
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 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 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.

[40] Abbreviations: (MP) Media Protection, (PR.DS) Data Security, and (PR.PT) Protective Technology.

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

Data Protection and Privacy

Question 37
To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses (NIST SP 800-53 REV. 4: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2021 CIO FISMA Metrics: 3.8; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5)?
Consistently Implemented
The organization consistently monitors inbound and outbound network traffic, ensuring that all traffic passes through a web content filter that protects against phishing, malware, and blocks against known malicious sites. Additionally, the organization checks outbound communications traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of PII. Also, suspected malicious traffic is quarantined or blocked. ***In addition the organization 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 DHS' 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 on the performance of its data exfiltration and enhanced network defenses. The organization also conducts exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses. ***Further, the organization monitors its DNS infrastructure for potential tampering, in accordance with its ISCM strategy. In addition, the organization audits its DNS records.*** **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

Data Protection and Privacy

Question 38
To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events (NIST SP 800-122; NIST SP 800-53 REV. 4: Appendix J, SE-2; FY 2019 SAOP FISMA metrics, Section 12; OMB M-17-12; and OMB M-17-25)?[41]
Consistently Implemented
The organization consistently implements its Data Breach Response plan. Additionally, the breach response team participates in table-top exercises and uses lessons learned to make improvements to the plan as appropriate. Further, the organization is able to scan the specific individuals affected by a breach, send notice to the affected individuals, and provide those individuals with credit monitoring and repair services, as necessary. **MET –** The Council did not have network servers to store PII and did not allow PII on stand-alone laptops. According to the Council's *Privacy Program Plan,* "none of the GCERC Systems create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII." The Council had a Data Breach Response Plan implemented by the CIO, but the Council did not store PII information.
Managed and Measurable
The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. **NOT MET –** The Council conducted table-top exercises to review the effectiveness of its Data Breach Response Plan; however, as the Council did not suffer from a breach, it had not analyzed qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan.

[41] Abbreviation: (SE) Security.

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

Data Protection and Privacy

Question 39
To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training (NIST SP 800-53 REV. 4: AR-5, FY 2020 SAOP FISMA Metrics, Sections 9 10, and 11)?
Consistently Implemented
The organization ensures that all individuals receive basic privacy awareness training and individuals having responsibilities for PII or activities involving PII receive role-based privacy training at least annually. Additionally, the organization ensures that individuals certify acceptance of responsibilities for privacy requirements at least annually. **MET –** The Council ensured all individuals receive basic privacy awareness training and individuals having responsibilities for PII or activities involving PII received role-based privacy training at least annually. Additionally, the Council ensured individuals certify acceptance of responsibilities for privacy requirements at least annually.
Managed and Measurable
The organization measures the effectiveness of its privacy awareness training program by obtaining feedback on the content of the training and conducting targeted phishing exercises for those with responsibility for PII. Additionally, the organization make updates to its program based on statutory, regulatory, mission, program, business process, information system requirements, and/or results from monitoring and auditing. **NOT MET –** The Council updated its training program based on statutory, regulatory, mission, program, business process, and information system requirements. The Council did not perform targeted phishing exercises for those with responsibility for PII as they do not collect any PII. However, they perform phishing training for all users. In addition, the CIO tracks the responses of the users received from the training so that the CIO may review and gauge feedback on how well topics are understood and determine effectiveness. However, Council did not have a process of collecting feedback from its users. As such, we determined the Council did not meet this maturity level.

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

Data Protection and Privacy

Question 40
Provide any additional information on the effectiveness (positive or negative) of the organization's data protection and privacy program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the data protection and privacy program effective?
Question 35 – Maturity Level: Consistently Implemented
Question 36 – Maturity Level: Consistently Implemented
Question 37 – Maturity Level: Consistently Implemented
Question 38 – Maturity Level: Consistently Implemented
Question 39 – Maturity Level: Consistently Implemented
OVERALL: Consistently Implemented
Based on the maturity levels generated from the questions and all testing performed in the Data Protection and Privacy domain, we concluded the overall maturity level for the Council's Data Protection and Privacy program was Consistently Implemented. 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 Data Protection and Privacy program controls in place were effective. Due to the small organizational size and limited internal IT systems, the duties of positions were very limited, and multiple roles and responsibilities were accomplished by both the CIO and Chief Financial Officer. The agency did not process any PII data. PII data needed for human resources and payroll were handled through agreements with a Federal Shared Service Provider whose systems were approved to collect and process PII data. It should be noted, due to the unique organizational structure of the Council, some of the areas which determine the maturity level of the Council's Data Protection and Privacy domain may not be applicable.

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

Security Training

Question 41
To what extent have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced? (Note: this includes the roles and responsibilities for the effective establishment and maintenance of an organization wide security awareness and training program as well as the awareness and training related roles and responsibilities of system users and those with significant security responsibilities (NIST SP 800-53 REV. 4: AT-1; and NIST SP 800-50).[42]
Managed and Measurable
*Re**sources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to consistently implement security awareness and training responsibilities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.***   **MET -** The Council had a unique organizational structure with the CIO as the only person responsible for all day-to-day activities of the Council's IT security awareness and training program. As a result, we determined resources were allocated in a risk-based manner as the CIO was the lone IT personnel in the organization.
Optimized
Per the FISMA Reporting Metrics, this maturity level was not applicable to this question.

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

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

Security Training

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 (NIST SP 800-53 REV. 4: AT-2 and AT-3; 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/SANS Top 20: 17.1)?
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 small size of the organization 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. As such, we could not determine the Council's personnel collectively possessed a training level such that the Council could demonstrate security incidents resulting from personnel actions or inactions were being reduced over time.

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

Security Training

Question 43
To what extent does the organization utilize a security awareness and training strategy/plan that leverages its skills assessment and is adapted to its mission and risk environment? (Note: the strategy/plan should include the following components: the structure of the awareness and training program, priorities, funding, the goals of the program, target audiences, types of courses/material for each audience, use of technologies (such as email advisories, intranet updates/wiki pages/social media, web based training, phishing simulation tools), frequency of training, and deployment methods (NIST SP 800-53 REV. 4: AT-1; NIST SP 800-50: Section 3; CSF: PR.AT-1).
Managed and Measurable
The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. **MET–** The Council monitored and analyzed qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. The Council ensured data supporting metrics were obtained accurately, consistently, and in a reproducible format. The CIO reviewed all results of testing and made updates to quarterly training based on the analysis as applicable.
Optimized
The organization's security awareness and training activities are integrated across other security-related domains. For instance, common risks and control weaknesses, and other outputs of the agency's risk management and continuous monitoring activities inform any updates that need to be made to the security awareness and training program. **NOT MET –** The Council did not integrate security awareness and training activities across other security-related domains. For instance, common risks, control weaknesses, and other outputs of the agency's risk management and continuous monitoring activities did not inform any updates which need to be made to the security awareness and training program.

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

Security Training

Question 44
To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting (NIST SP 800-53 REV. 4: AT-1, AT-2; FY 2021 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; CSF: PR.AT-2; SANS Top 20: 17.4).
Consistently Implemented
The organization ensures that its security awareness policies and procedures are consistently implemented. ***The organization ensures that all appropriate users complete the organization's security awareness training (or a comparable awareness training for contractors) [within organizationally defined timeframes] and periodically thereafter and maintains completion records.*** ***The organization obtains feedback on its security awareness and training program and uses that information to make improvements.*** **MET –** The Council ensured all systems users completed its security awareness training (or a comparable awareness training for contractors) prior to system access and periodically thereafter and maintained completion records. The Council obtained feedback on its security awareness and training program and used the information to make improvements.
Managed and Measurable
The organization measures the effectiveness of its awareness training program by, for example, conducting phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate. ***The organization monitors and analyzes qualitative and quantitative performance measures on theeffectiveness of its security awareness policies, procedures, and practices. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.*** **NOT MET –** As a small organization with limited IT infrastructure, the Council did not have much exposure to risk. While the Council conducted phishing awareness training, the Council did not conduct a phishing exercise to measure the effectiveness of the training. In addition, the Council did not monitor and analyze qualitative and quantitative performance measure on the effectiveness of its security awareness policies, procedures, and practices.

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

Security Training

Question 45
To what extent does the organization ensure that specialized security training is provided to individuals with significant security responsibilities (as defined in the organization's security policies and procedures and in accordance with 5 Code of Federal Regulation 930.301) (NIST SP 800-53 REV. 4: AT-3 and AT-4; FY 2021 CIO FISMA Metrics: 2.15, and 5 Code of Federal Regulation 930.301)?
Consistently Implemented
The organization ensures that its security training policies and procedures are consistently implemented. ***The organization ensures that individuals with significant security responsibilities complete the organization's defined specialized security training (or comparable training for contractors) [within organizationally defined timeframes] and periodically thereafter. The organization also maintains completion records for specialized training taken by individuals with significant security responsibilities.*** ***The organization obtains feedback on its security training program and uses that information to make improvements.*** **MET–** The Council CIO completes the specialized security training by maintaining certification which requires 40 hours of continuing professional education per year. The transcript details various specialized courses the CIO has taken to comply with maintaining his certification. All training is reviewed by the CIO, and in addition, the CIO contacts the staff to ensure they understand the requirements. Training is updated yearly to ensure that new threats are included in the training. This way Council obtains feedback on its security training program and uses that information to make improvements.

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

Security Training

Question 45
Managed and Measurable
The organization obtains feedback on its security training content and makes updates to its program, as appropriate. In addition, the organization measures the effectiveness of its specialized security training program by, for example, conducting targeted phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate. ***The organization monitors and analyzes qualitative and quantitative performance measures on theeffectiveness of its security training policies, procedures, and practices. The organization ensuresthat data supporting metrics are obtained accurately, consistently, and in a reproducible format.*** **NOT MET –** The Council is a small organization and did not measure the effectiveness of its specialized security training program by, for example, conducting targeted phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate. The Council conducted phishing awareness training but did not perform phishing exercises. The Council did not monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security training policies, procedures, and practices.

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

Security Training

Question 46
Provide any additional information on the effectiveness (positive or negative) of the organization's security training program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the security training program effective?
Question 41 – Maturity Level: Managed and Measurable
Question 42 – Maturity Level: Managed and Measurable
Question 43 – Maturity Level: Managed and Measurable
Question 44 – Maturity Level: Consistently Implemented
Question 45 – Maturity Level: Consistently Implemented
OVERALL: Managed and Measurable
Based on the maturity levels generated from the questions and all testing performed in the Security Training domain, we concluded the overall maturity level for the Council's Security Training program was Managed and Measurable. The Council had a simple, flat organizational structure without formal departments and layers of management typically found in larger organizations. As a result, the CIO was the lone IT personnel and is directly responsible for monitoring all IT security training.

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

ISCM

Detect Function Area

Question 47
To what extent does the organization utilize information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier (NIST SP 800-37 (Rev. 2) Task P-7; NIST SP 800-137: Sections 3.1 and 3.6)?
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

ISCM

Question 48
To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization (NIST SP 800-53REV. 4: CA-1; NIST SP 800-137; CSF: DE. DP-1; NIST 800-37, Rev. 2 Task P-7 and S-5)?[43]
Managed and Measurable
Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement ISCM activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively. **MET –** The Council had a small organizational structure without the typical network available in a large organization, and the CIO was the lone IT personnel. The Council relied on third party service providers to manage its information systems. As such, the Council's service providers were responsible for implementing ISCM activities on those systems. It would be inaccurate to state the Council did not meet the Managed and Measurable maturity level.
Optimized
Per the FISMA Reporting Metrics, this maturity level was not applicable to this question.

[43] Abbreviation: (DE. DP) Detection Process.

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

ISCM

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. 4: CA-2, CA-6, and CA-7; 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)?
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.

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

ISCM

Question 50
How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137)?
Managed and Measurable
The organization is able to integrate metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations and security domains. The Council's small organizational structure and size enable it to integrate metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations and security domains. The Council has established procedures for reviewing and modifying all aspects of its ISCM strategy, including the relevance of the overall strategy, accuracy in reflecting organizational risk tolerance, accuracy/correctness of measurements, and applicability of metrics, reporting requirements, and monitoring and assessment frequencies.
Optimized
On a near real-time basis, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner. **NOT MET –** Although the Council has established procedures and processes for continuous monitoring to provide situation awareness across many areas of its organization, the Council did not actively adapt its ISCM program to a changing cybersecurity landscape and respond to evolving and sophisticated threats in a timely manner.

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

ISCM

Question 51
Provide any additional information on the effectiveness (positive or negative) of the organization's ISCM program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?
Question 47 – Maturity Level: Managed and Measurable
Question 48 – Maturity Level: Managed and Measurable
Question 49 – Maturity Level: Managed and Measurable
Question 50 – Maturity Level: Managed and Measurable
OVERALL: Managed and Measurable
Based on the maturity levels generated from the questions and the testing performed in the ISCM domain, we concluded the overall maturity level of the Council's ISCM program was Managed and Measurable. The Council's simple, flat organizational structure, which did not have any formal departments or layers of management, allowed the Council to operate more efficiently and effectively than larger organizations. Decisions regarding IT operations were made with the direct involvement and approval of the Council's CIO allowing the leadership to easily monitor and analyze qualitative and quantitative performance measures across the organization and the effectiveness of its ISCM program. The direct involvement of the CIO and leadership allowed the Council to achieve cost-effective IT security objectives and goals which helped facilitate decision-making and minimize cost, risk, and impact on the Council's mission.

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

Incident Response

Respond Function Area

Question 52
To what extent does the organization utilize an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents (NIST SP 800-53 REV. 4: IR-8; NIST SP 800-61 Rev. 2, section 2.3.2; CSF, RS.RP-1, Presidential Policy Directive (PPD) 8 – National Preparedness)?[44]
Consistently Implemented
The organization consistently implements its incident response plan. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident response plan and making updates as necessary. **MET –** The Council monitor's threats through a third-party application. The threats were not deemed significant that could classify as incidents. The Council did not experience any successful incidents during the FISMA reporting period July 1, 2020 through June 30, 2021. The Council did not have an opportunity to perform lessons learned since they did not have any successful incidents.
Managed and Measurable
The organization monitors and analyzes the qualitative and quantitative performance measures that have been defined in its incident response plan to monitor and maintain the effectiveness of its overall incident response capability. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. **NOT MET –** The Council did not experience any incidents during the FISMA reporting period July 1, 2020 through June 30, 2021. As such, the Council did not monitored and analyzed the qualitative and quantitative performance measures that have been defined in its incident response plan to monitor and maintain the effectiveness of its overall incident response capability.

[44] Abbreviation: (RS.RP) Response Planning.

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

Incident Response

Question 53
To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization (NIST SP 800-53 REV. 4: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; CSF, RS.CO-1, OMB M-20-04; FY 2021 CIO FISMA Metrics: Section 4. CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?[45]
Consistently Implemented
Individuals are performing the roles and responsibilities that have been defined across the organization. **MET –** Individuals performed the roles and responsibilities that have been defined across the organization. The Council complied with Federal requirements to establish, implement, and enforce an incident management policy to continually manage risks to the Council's information resources. The Council's Incident Response Plan serves as the foundation for the Council to develop and implement cybersecurity incident management procedures and plans that comply with Federal and agency requirements.
Managed and Measurable
Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement incident response activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively. **NOT MET –** Due to the small organizational structure of the Council, and its reliance on third party service providers which gives the Council limited exposure to the possibility of security incidents, the Council only had part-time incident response team members, serving as more of a virtual incident response team. As such, we could not determine if resources were allocated in a risk-based manner for shareholders to implement incident response activities.

[45] Abbreviations: (IR) Incident Response and (RS.CO) Communications.

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

Incident Response

Question 54
How mature are the organization's processes for incident detection and analysis (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; OMB M-20-04; CSF: DE.AE-1, DE.AE-2 –5, PR.DS-6, RS.AN-1 and 4, and PR.DS-8; and US-CERT Incident Response Guidelines)?[46]
Managed and Measurable
The organization monitors and analyzes qualitative and quantitative performance measures on theeffectiveness of its incident detection and analysis policies and procedures. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. ***The organization utilizes profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents. Examples of profiling include running file integrity checking software on hosts to derive checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times. Through profiling techniques, the organization maintains a comprehensive baseline of network operations and expected data flows for users and systems.*** **MET –** The Council has conducted table-top exercises and used third party provider 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 FISMA Reporting Metrics, this maturity level was not applicable to this question.

[46] Abbreviations: (DE.AE) Anomalies and Events and (RS.AN) Analysis.

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

Incident Response

Question 55
How mature are the organization's processes for incident handling (NIST 800-53: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 2)?[47]
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 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 on 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 correct.
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 are hosted by third party providers, the Council has limited exposure to vulnerabilities and security incidents on its information systems. The Council had not reported any incident during the audit period. The Council relies on third party service providers for its information system's needs. Since the Council did not experience any incidents during the FISMA period July 1, 2020 through June 30,

[47] Abbreviation: (RS.MI) Mitigation.

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

Incident Response

Question 55
2021, 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

Incident Response

Question 56
To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; OMB M-20-04; NIST SP 800-53 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 5; DHS Cyber Incident Reporting Unified Message)?
Consistently Implemented
The organization consistently shares information on incident activities with internal stakeholders. The organization ensures that security incidents are reported to US-CERT, law enforcement, the Office of Inspector General, and the Congress (for major incidents) in a timely manner. ***Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident reporting policies and procedures and making updates as necessary.*** **MET –** The Council had a simple, flat organizational structure, without formal departments or layers of management like larger organizations. No incidents occurred at the Council during FY 21. As such, there was no means to verify information regarding sharing information on incident activities and reporting incidents in a timely manner. However, it would be inaccurate to state the Council had not met the Consistently Implemented maturity level because they have processes and controls in place for incidents that requires incidents to be reported to United States Computer Emergency Readiness Team within one hour of discovery/detection and contact OIG and law enforcement. In addition, no lessons learned were developed as they did not experience any incidents.
Managed and Measurable
Incident response metrics are used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. **NOT MET –** The Council did not experience any incidents for FY 21. The Council's incident response is managed by third parties. Since there were no incidents reported, we cannot determine that the Council's Incident response metrics are used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.

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

Incident Response

Question 57
To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents, including through contracts/agreements, as appropriate, for incident response support (NIST SP 800-86; NIST SP 800-53 REV. 4: IR-4; OMB M-20-04; PPD-41)?
Managed and Measurable
The organization utilizes Einstein 3 Accelerated, and/or other comparable tools or services, to detect and proactively block cyber-attacks or prevent potential compromises. **MET –** The Council utilized EINSTEIN 3 Accelerated to detect and proactively block cyber-attacks or prevent potential compromises.
Optimized
Per the FISMA Reporting Metrics, this maturity level was not applicable to this question.

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

Incident Response

Question 58
To what extent does the organization utilize the following technology to support its incident response program? • Web application protections, such as web application firewalls; • Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools; • Aggregation and analysis, such as security information and event management (SIEM) products; • Malware detection, such as antivirus and antispam software technologies; • Information management, such as data loss prevention; and • File integrity and endpoint and server security tools (NIST SP 800-137; NIST SP 800-61, Rev. 2; NIST SP 800-44).
Managed and Measurable
The organization evaluates the effectiveness of its incident response technologies and makes adjustments to configurations and toolsets, as appropriate. **MET –** The Council did not use these technologies since it relied on its service providers. Therefore, we determined this maturity level was not applicable to the Council's environment. However, the Council's third party service providers are responsible for monitoring and evaluating the effectiveness of their incident response technologies. Therefore, we determined the Council's maturity level as Managed and Measurable for this metric.
Optimized
The organization has institutionalized the implementation of advanced incident response technologies for analysis of trends and performance against benchmarks (e.g., simulation-based technologies to continuously determine the impact of potential security incidents to its IT assets) and adjusts incident response processes and security measures accordingly. **NOT MET –** The Council is a micro-agency with a unique organizational structure that relies on third party providers for its information systems. The Council did not institutionalize the implementation of advanced incident response technologies for analysis of trends and performance against benchmarks (e.g., simulation-based technologies to continuously determine the impact of potential security incidents to its IT assets) and did not adjust its incident response processes and security measures accordingly.

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

Incident Response

Question 59
Provide any additional information on the effectiveness (positive or negative) of the organization's incident response program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the incident response program effective?
Question 52 – Maturity Level: Consistently Implemented
Question 53 – Maturity Level: Consistently Implemented
Question 54 – Maturity Level: Managed and Measurable
Question 55 – Maturity Level: Consistently Implemented
Question 56 – Maturity Level: Consistently Implemented
Question 57 – Maturity Level: Managed and Measurable
Question 58 – Maturity Level: Managed and Measurable
OVERALL: Consistently Implemented
Based on the maturity levels generated from the questions and the testing performed in the Incident Response domain, we concluded the overall maturity level of the Council's Incident Response program was Consistently Implemented. Since the Council did not own any servers or general support systems, and they depended on third party providers, the Council had limited exposure to the possibility of security incidents and only had part-time incident response team members who served more as a virtual incident response team. The small organizational structure enabled the Council to respond to and address security incidents promptly. As a result, the Council's Computer Security Incident Response Center could be assembled quickly to meet the required reporting timelines and help the Council expedite reporting of incidents that could help serve to mitigate or prevent damage to the Council's information systems.

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

Contingency Planning

Recover Function Area

Question 60
To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined, communicated, and implemented across the organization, including appropriate delegations of authority (NIST SP 800-53 REV. 4: CP-1, CP-2, and CP-3; NIST SP 800- 34; NIST SP 800-84; FCD-1: Annex B)?[48]
Optimized
The organization incorporates simulated events into contingency training to facilitate effective response by stakeholders (internal and external) involved in information systems contingency planning and to measure the extent to which individuals are equipped to perform their roles and responsibilities. **MET** – Since the Council has a very simplified system (OSN) that consists of laptops, the contingency table-top exercise that was conducted incorporated simulated events into contingency training. The exercise report included the contingency activities, testing results, and action items, as appropriate. We determined the Council had ensured its stakeholders are equipped to perform their roles and responsibilities accordingly.

[48] Abbreviations: (CP) Contingency Planning and (FCD) Federal Continuity Directive.

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

Contingency Planning

Question 61
To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34, Rev. 1, 3.2; NIST IR 8286; FIPS 199; FCD-1; OMB M-19-03; FY 2021 CIO FISMA Metrics, Section 5; CSF: ID.RA-4)?
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 Business Impact Analysis (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 results of the organizational and system level BIA are integrated with enterprise risk management processes, for consistently evaluating, recording, and monitoring the criticality and sensitivity of enterprise assets.

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

Contingency Planning

Question 62
To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST SP 800-53 REV. 4:CP-2; NIST SP 800-34; FY 2021 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?
Consistently Implemented
Information system contingency plans are consistently developed and implemented for systems, as appropriate, and include organizational and system level considerations for the following phases: activation and notification, recovery, and reconstitution. In addition, system level contingency planning development/maintenance activities are integrated with other continuity areas including organization and business process continuity, disaster recovery planning, incident management, insider threat implementation plan (as appropriate), and occupant emergency plans. **MET –** The Council is a small organization that relied on third party service providers to manage its information systems, except for the OSN managed by the CIO, and the Council had developed an Information Systems Contingency Plan for its OSN. The plan considered activation and notification, recovery, and reconstitution. Each system managed by the service provider received a FISMA certification ensuring it complied with contingency plans and NIST guidelines were met.
Managed and Measurable
The organization is able to integrate metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related plans, such as organization and business process continuity, disaster recovery, incident management, insider threat implementation, and occupant emergency, as appropriate to deliver persistent situational awareness across the organization. ***The organization coordinates the development of ISCP's with the contingency plans of external service providers.*** **NOT MET –** The Council did not integrate metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related plans. The Council owned few IT assets and had contracts with third party service providers for its information processing needs and therefore did not have integrated metrics on the effectiveness of those information system contingency plans as the third parties had the responsibility to do so. In addition, the Council did not coordinate the development of Information System Contingency Plans (ISCP) with the contingency plans of external service providers.

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

Contingency Planning

Question 63
To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST SP 800-34; NIST SP 800-53 REV. 4: CP-3 and CP-4; FY 2021 CIO FISMA Metrics, Section 5; CSF: ID.SC-5 and CSF: PR. IP-10)?
Consistently Implemented
Information system contingency plan testing and exercises are consistently implemented. ISCP testing and exercises are integrated, to the extent practicable, with testing of related plans, such as incident response plan/COOP/BCP. **MET –** 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.*** **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.

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

Contingency Planning

Question 64
To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST SP 800-53 REV. 4: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD-1; NIST CSF: PR. IP-4; FY2021 CIO FISMA Metrics, Section 5; and NARA guidance on information systems security records)?[49]
Consistently Implemented
The organization consistently implements its policies, procedures, processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites and RAID, as appropriate. ***Alternate processing and storage sites are chosen based upon risk assessments that ensure the potential disruption of the organization's ability to initiate and sustain operations is minimized. In addition, the organization ensures that these sites and are not subject to the same risks as the primary site.*** ***Furthermore, the organization ensures that alternate processing and storage facilities are configured with information security safeguards equivalent to those of the primary site, including applicable ICT supply chain controls. Furthermore, backups of information at the user- and system-levels are consistently performed, and the confidentiality, integrity, and availability of this information is maintained.*** **MET –** Though the Council defined the policies, procedures, processes, strategies, and technologies for information system backup and storage, the Council did not have a typical network as found in larger organizations. Given the small size of the organization, limited complexity of the IT environment, the fact the Council's information systems were managed by third parties and were therefore not subjected to the same physical and cybersecurity risks, we determined the Council met the maturity level of Consistently Implemented for this question. In addition, we examined each of the service provider's service level agreements and determined they addressed contingency planning or continuity of operations.
Managed and Measurable
The organization ensures that its information system backup and storage processes, including the use of alternate storage and processing sites, and related supply chain controls, are assessed, as appropriate, as part of its continuous monitoring program. ***As part of its continuous monitoring processes, the organization demonstrates that its system backup and storage and alternate storage and processing sites are configured to facilitate recovery operations in accordance with recovery time and recover point objectives.*** **NOT MET -** The Council has a simple organizational structure and system. OSN has no alternate processing facility established, and the backup data of the Council is responsible of third party provider.

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

Contingency Planning

Question 65
To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk based decisions (CSF: RC.CO-3; NIST SP 800-53 REV. 4: CP-2and IR-4)?
Consistently Implemented
Information on the planning and performance of recovery activities is consistently communicated to relevant stakeholders and executive management teams, who utilize the information to make risk-based decisions. **MET –** The Council had a small organizational structure without a typical network available in larger organizations. As a result, the CIO was the lone IT personnel and was directly responsible for monitoring all IT assets. Further, no IT decisions were made without the CIO's direct involvement and approval. The Council did not experience any incidents, therefore there was no evidence of any recovery activities performed.
Managed and Measurable
Metrics on the effectiveness of recovery activities are communicated to relevant stakeholders and the organization has ensured that the data supporting the metrics are obtained accurately, consistently, and in a reproducible format. **NOT MET –** The Council did not experience any incidents, and no recovery activities were performed. As such, we assessed the maturity level as Consistently Implemented.

[49] Abbreviation: (NARA) National Archives and Records Administration.

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

Contingency Planning

Question 66
Provide any additional information on the effectiveness (positive or negative) of the organization's contingency planning program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the contingency program effective?
Question 60 – Maturity Level: Optimized
Question 61 – Maturity Level: Consistently Implemented
Question 62 – Maturity Level: Consistently Implemented
Question 63 – Maturity Level: Consistently Implemented
Question 64 – Maturity Level: Consistently Implemented
Question 65 – Maturity Level: Consistently Implemented
OVERALL: Consistently Implemented
Based on the maturity levels generated from the questions and the testing performed in the Contingency Planning domain, we concluded the overall maturity level of the Council's Contingency Planning program was Consistently Implemented. The Council had a simple, flat organizational structure without formal departments and layers of management typically found in larger organizations. As a result, the CIO was the lone IT personnel and is directly responsible for monitoring all IT assets. Further, no IT decisions were made without the CIO's direct involvement and approval. The CIO's direct control allowed the Council to operate more efficiently and effectively than larger organizations because ideas or requests did not need to climb up the levels of management before approval.

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

Appendix II: Management Response

RMA | Associates
Auditors. Consultants. Advisors.

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

Gulf Coast Ecosystem Restoration Council

October 15, 2021

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

Re: The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2021

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 2021.

The Council agrees with the report that the Council's information security program and practices were effective for the period July 1, 2020 through June 30, 2021. The Council works to ensure the information assurance program meets the key performance areas for the five Cybersecurity Functions and nine FISMA Metric Domains.

In fiscal year 2022, 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: 2021.10.15 12:37:05 -04'00'

Mary S. Walker
Executive Director
Gulf Coast Ecosystem Restoration Council

REPORT WASTE, FRAUD, AND ABUSE

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

TREASURY OIG WEBSITE

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