Evaluation Report

OIG-CA-25-053

CYBERSECURITY/INFORMATION TECHNOLOGY

The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2025

August 1, 2025

Office of Inspector General
Department of the Treasury

This Page Intentionally Left Blank

OFFICE OF
INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

August 1, 2025

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

Re: Evaluation Report – The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2025 (OIG-CA-25-053)

Dear Ms. Walker:

We hereby transmit the attached report, *The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2025*, dated July 30, 2025. The Federal Information Security Modernization Act of 2014 (FISMA) requires that Federal agencies have an annual independent evaluation performed of their information security programs and practices to determine the effectiveness of such programs and practices, and to report the results to the Office of Management and Budget (OMB). OMB delegated its responsibility to the Department of Homeland Security for the collection of annual FISMA responses. FISMA also requires that the agency Inspector General (IG) or an independent external auditor perform the annual evaluation as determined by the IG.

To meet our FISMA requirements, we contracted with RMA Associates, LLC (RMA), an independent certified public accounting firm, to perform this year's annual FISMA evaluation of the Gulf Coast Ecosystem Restoration Council's (Council) security program and practices for the period April 1, 2024, through March 31, 2025. 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 the Council's information security program and practices were established and maintained for the six Cybersecurity Function Areas and ten FISMA Metric Domains consistent with applicable FISMA requirements,

OMB policy and guidance, and the National Institute of Standards and Technology standards and guidelines. RMA found that the Council's information security program and practices were effective for the period April 1, 2024, through March 31, 2025.

Appendix I of the attached RMA report includes the Fiscal Year 2025 IG FISMA Reporting Metrics Results.

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

Sincerely,

/s/

Larissa Klimpel
Director, Cyber/Information Technology Audits

Attachment

RMA | Associates
Auditors. Consultants. Advisors.

The Gulf Coast Ecosystem Restoration Council
Federal Information Security Modernization Act of 2014
Evaluation Report for Fiscal Year 2025

RMA | Associates
Auditors. Consultants. Advisors.

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

July 30, 2025

Loren Sciurba
Deputy Inspector General
Department of the Treasury
875 15th St. NW
Washington, DC 20005

Re: The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2025

Dear Mr. Sciurba:

RMA Associates, LLC is pleased to submit the Gulf Coast Ecosystem Restoration Council (Council) Federal Information Security Modernization Act of 2014 (FISMA) Evaluation Report for fiscal year (FY) 2025. We conducted the evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* issued in December 2020. The objective of this evaluation was to evaluate the effectiveness of the Council's information security program and practices for the period April 1, 2024, through March 31, 2025.

For FY 2025, the Office of Management and Budget (OMB) identified 20 Core and 5 Supplemental Inspector General (IG) FISMA Reporting Metrics to evaluate. These metrics are outlined in OMB's *FY 2025 Inspector General FISMA Reporting Metrics v2.0* dated April 3, 2025. The IG was required to assess the maturity levels of those metrics. We conducted an evaluation of the FY 2025 Core and Supplemental Metrics on behalf of the Department of the Treasury's Office of Inspector General. The results of this evaluation are presented in Appendix I: FY 2025 IG FISMA Reporting Metrics.

In summary, we found the Council's information security program and practices were effective for the period April 1, 2024, through March 31, 2025.

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.

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

Table of Contents

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

Abbreviations

BOD	Binding Operational Directive
CIO	Chief Information Officer
CIS	Center for Internet Security
CASB	Cloud Access Security Broker
CISO	Chief Information Security Officer
CIGIE	Council of the Inspectors General on Integrity and Efficiency
Council	Gulf Coast Ecosystem Restoration Council
CSF	Cybersecurity Framework
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DNS	Domain Name System
ED	Emergency Directive
EL	Event Logging
EO	Executive Order
EDR	Endpoint Detection and Response
FIDO2	Fast Identity Online 2
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAO	Government Accountability Office
HSPD	Homeland Security Presidential Directive
IG	Inspector General
IT	Information Technology
IDPS	Intrusion Detection and Prevention Systems
ISCM	Information Security Continuous Monitoring
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OSN	Office Support Network
PII	Personally Identifiable Information
PIV	Personal Identity Verification
RESTORE Act	Resources and Ecosystems Sustainability, Tourist Opportunities, and Revived Economies of the Gulf Coast States Act of 2012
RMA	RMA Associates, LLC
SIEM	Security Information and Event Management
SP	Special Publication
ZTA	Zero Trust Architecture

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

Introduction

This report presents 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 independently evaluate their information security program and practices to determine the effectiveness of such programs and practices and report results to the Office of Management and Budget (OMB). OMB delegated its responsibility to the Department of Homeland Security (DHS) for the collection of annual FISMA responses.

The Department of the Treasury's Office of Inspector General engaged RMA Associates, LLC (RMA) to conduct the Fiscal Year (FY) 2025 FISMA evaluation of the Council's information security program and practices. The objective of this evaluation was to evaluate the effectiveness of the Council's information security program and practices for the period April 1, 2024, through March 31, 2025.

As part of our evaluation, we responded to the FY 2025 metrics from OMB's *FY 2025 Inspector General (IG) FISMA Reporting Metrics v2.0* dated April 3, 2025.[2] For FY 2025, five Supplemental Metrics were evaluated in addition to the 20 Core Metrics. These metrics aligned with function areas in *The National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0*: Govern, Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks. This evaluation was performed in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) *Quality Standards for Inspection and Evaluation* issued in December 2020.

Summary of Evaluation Results

We concluded that the Council's information security program and practices were established and maintained for the six Function Areas[3] and ten FISMA Metric Domains[4] consistent with FISMA requirements, OMB policy and guidance, and NIST standards and guidelines. The overall maturity of the Council's information security program was determined to be Level 4, Managed and Measurable. We found the Council's information security program and practices were appropriate and effective for the period April 1, 2024 through March 31, 2025.

[1] Public Law 113-283, Federal Information Security Modernization Act of 2014, December 18, 2014.
[2] OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency developed the IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officers Council.
[3]The six Function Areas as defined in *The NIST Cybersecurity Framework* are: (1) Govern, (2) Identify, (3) Protect, (4) Detect, (5) Respond, and (6) Recover.
[4] As described in the FISMA Reporting Metrics, the ten FISMA Metric Domains, which are aligned with the six Function Areas are: (1) cybersecurity governance, (2) cybersecurity supply chain risk management, (3) risk and asset management, (4) configuration management, (5) identity and access management, (6) data protection and privacy, (7) security training, (8) information security continuous monitoring, (9) incident response, and (10) contingency planning.

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

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

Background

Gulf Coast Ecosystem Restoration Council

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

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

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

Federal Information Security Modernization Act of 2014

On December 18, 2014, the President signed FISMA, which amended the Federal Information Security Management Act of 2002 and provided several modifications that modernized Federal security practices to address evolving security concerns. These changes strengthened the use of continuous monitoring in systems, increased focus on the agencies' compliance, and produced reports that focused on issues caused by security incidents.

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

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

FISMA reestablished the oversight authority of the Director of the OMB with respect to agency information security policies and practices; and set forth authority for the Secretary of DHS to administer the implementation of such policies and practices for information systems.[5]

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

The Director of OMB directs the Secretary of DHS to consult with and consider guidance developed by NIST to ensure operational directives do not conflict with NIST information security standards.[7]

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

Further, FISMA requires OMB to ensure the development of guidance for evaluating the effectiveness of information security programs and practices and determining what constitutes a major incident.[9]

FY 2025 Core and Supplemental Metrics

OMB's *FY 2025 IG FISMA Reporting Metrics v2.0*, dated April 3, 2025, specified the FY 2025 20 Core and five Supplemental Metrics (refer to Appendix I). It directed IGs to report the assessed maturity levels of these metrics in CyberScope[10] no later than August 1, 2025. The FY 2025 FISMA Metrics were aligned with six Function Areas:

- Govern, which includes questions pertaining to Cybersecurity Governance and Cybersecurity Supply Chain Risk Management;
- Identify, which includes questions pertaining to Risk and Asset Management;
- Protect, which includes questions pertaining to Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training;

[5] Federal Information Security Modernization Act of 2014, Public Law No. 113-283, December 2014, https://www.congress.gov/bill/113th-congress/senate-bill/2521.
[6] Ibid.
[7] Ibid.
[8] Ibid.
[9] Ibid.
[10] CyberScope is an online reporting tool, established by OMB, developed to streamline the collection of cybersecurity performance data, including FISMA metric results, from federal agencies.

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

- Detect, which includes questions pertaining to Information Security Continuous Monitoring;
- Respond, which includes questions pertaining to Incident Response; and
- Recover, which includes questions pertaining to Contingency Planning.

We evaluated the effectiveness of the Council's information security programs and practices on a maturity model spectrum, in which the foundation levels ensure the development of sound policies and procedures. The FY 2025 IG Reporting Metrics classify information security programs and practices into five maturity model levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized (**Table 1**). Within the context of the maturity model, Level 4, Managed and Measurable, represents an effective level of security. IGs may determine that a particular domain, function area, and/or the agency's information security program is effective at a calculated maturity level lower than Level 4.

Table 1: IG Evaluation Maturity Levels

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

The scope of our evaluation was conducted for the period between April 1, 2024, and March 31, 2025. It consisted of testing the 20 Core and five Supplemental Metrics as shown in Appendix I, which reflects the results of our assessment of the Council's information security program and practices.

Evaluation Results

In previous years, IGs were directed to use a mode-based scoring approach to assess agency maturity levels. Under this approach, ratings throughout the reporting domains were determined by a simple majority, where the most frequent level (i.e., the mode) across the questions served as the domain rating. Since FY 2023, a calculated average scoring model has been used, where Core and Supplemental Metrics are averaged independently to determine a domain's maturity calculation and provide data points for the assessed program and function effectiveness. For example, if the calculated Core Metric maturity of two of the function areas was Level 3 (Consistently Implemented) (i.e., 3.0) and the computed Core Metric maturity of the remaining

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

three function areas was Level 4 (Managed and Measurable) (i.e., 4.0), the information security program rating would average a 3.60 (3+3+4+4+4)/5).

Core and Supplemental Metrics were averaged independently to determine a domain's maturity calculation and provide data points for the assessed program and function effectiveness. The Council's overall program calculation is shown in **Table 2**. The Council's FY 2025 corresponding maturity levels for the six function areas and the overall level are presented in **Table 3**.

Table 2: The Council's Overall Calculated Averages Maturity Calculation in FY 2025

Function Area	Core Metrics	FY 2025 Supplemental Metrics[11]	FY 2025 Assessed Maturity Average[12]	FY 2025 Assessed Maturity
Govern[13]	4.00	4.33	4.17	Managed and Measurable
Identify	3.80	3.00	3.40	Consistently Implemented
Protect	4.00	N/A	4.00	Managed and Measurable
Detect	4.00	5.00	4.50	Managed and Measurable
Respond	3.50	N/A	3.50	Consistently Implemented
Recover	3.50	N/A	3.50	Consistently Implemented
Overall Maturity	**3.80**	**4.11**	**3.84**	**Managed and Measurable[14]**

Table 3: The Council's FY 2025 Maturity Levels

Function Area[15]	Core Metrics	FY 2025 Supplemental Metrics	FY 2025 Assessed Maturity	RMA's FY 2025 Assessed Maturity Level
Govern	Managed and Measurable	Managed and Measurable	Managed and Measurable	Effective
Identify	Consistently Implemented	Consistently Implemented	Consistently Implemented	Effective
Protect	Managed and Measurable	N/A	Managed and Measurable	Effective
Detect	Managed and Measurable	Optimized	Managed and Measurable	Effective
Respond	Consistently Implemented	N/A	Consistently Implemented	Effective
Recover	Consistently Implemented	N/A	Consistently Implemented	Effective
Overall Maturity	**Managed and Measurable[14]**	**Managed and Measurable**	**Managed and Measurable[14]**	**Effective**

RMA focused on the results of the Core Metrics to determine the maturity level and used the calculated averages of the Supplemental Metrics as a data point to support our risk-based

[11] Protect, Respond, and Recover only consist of Core Metrics.
[12] The FY 2025 Assessed Maturity Average was calculated by averaging the Core and Supplemental Metrics. The calculated averages were truncated to determine the maturity level. In determining maturity levels and the overall effectiveness of Council's information security program, RMA focused on the results of the Core Metric and made a risk-based determination of overall program and function level effectiveness.
[13] The Govern Function Area was introduced in FY 2025.
[14] RMA used their judgement and made a risk-based determination of overall program and function level effectiveness.
[15] Protect, Respond, and Recover only consist of Core Metrics.

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

determination of overall program and function level effectiveness. The overall maturity level of the information security program was determined as Consistently Implemented.

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

NOTE: Based on Council's risk tolerance and threat models, RMA used discretion to determine the overall effectiveness of Council's information security program, in accordance with Cybersecurity Framework Function Area effectiveness (e.g., Identify, Protect), and the individual domain ratings (e.g., risk and asset management, configuration management). Using this approach, RMA determined that a particular domain, function area, and/or the Council's information security program was effective even though the overall calculated maturity level was lower than 4.0.

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

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

Below is the maturity level for each domain.

Cybersecurity Governance: We determined the Council's overall maturity level for the Cybersecurity Governance domain was Managed and Measurable. The Council monitored its cybersecurity risk management program in near real-time, leveraging predictive analytics and threat intelligence to proactively adjust strategies. In addition, regular training conducted to hold personnel accountable and enforced Council's cybersecurity requirements. Our testing found no exceptions in cybersecurity governance, and the existing controls were operating as intended. We concluded the Council's Cybersecurity Governance controls in place were effective.

Cybersecurity Supply Chain Risk Management: We determined the Council's overall maturity level for the Supply Chain Risk Management domain was Managed and Measurable. The Council defined supply chain policies and procedures. The Council managed its supply chain risks by purchasing products from trusted and approved manufacturers. The Council's OSN was considered a server-less network with a Federal Information Processing Standards (FIPS) Publication 199 low rating.[16] Our testing found no exceptions, and the controls were operating as

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

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

intended. We concluded the Council's Supply Chain Risk Management controls in place were effective.

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

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

Identity and Access Management: We determined the Council's overall maturity level for the Identity and Access Management domain was Managed and Measurable. The Council managed the Identity and Access Management protocols for its employees and contractors. Due to the Council's size and structure with all systems, except the OSN, being cloud-based and housed by third parties, account changes could only be made on local machines. All accounts are local accounts that were not shared and could only be modified by a privileged user logging into each machine. Our testing found no exceptions, and controls were operating as intended. We concluded the Council's Identity and Access Management controls in place were effective.

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

Security Training: We determined the Council's overall maturity level for the Security Training program was Managed and Measurable. The Council effectively allocated resources in a risk-based manner for stakeholders to implement security awareness training consistently. The Council

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

addressed its identified knowledge, skills, and abilities gaps through talent acquisition. Our testing of the Council's workforce assessment found no exceptions, and controls were operating as intended. We concluded the Council's Security Training controls in place were effective.

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

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

Contingency Planning: We determined the Council's overall maturity level for the Contingency Planning program was Consistently Implemented. Since the Council does not own any network servers, it developed contingency planning policies and procedures that were consistently implemented. Through our control testing for this domain, we found no exceptions and determined the controls were operating as intended. We concluded the Council's Contingency Planning controls in place were effective.

Summary: Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, we concluded that the Council's information security program and practices were established. They were maintained for the six Function Areas and ten FISMA Metric Domains with an overall maturity level of Managed and Measurable. We found the Council's information security program, and practices were effective for the period April 1, 2024, through March 31, 2025.

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

Objective, Scope, and Methodology

Objective

The objective of this evaluation was to determine the effectiveness of the Council's information security program and practices for the period of April 1, 2024, through March 31, 2025.

Scope

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

The Council's OSN was technically not a computer network as it included no network servers. OSN was a stand-alone group of laptops connected to a leased wireless access point that provides a leased Virtual Private Network connection to the Trusted Internet Connection portal. Our evaluation scope covered the period between April 1, 2024, and March 31, 2025.

We determined the effectiveness of the Council's security program and practices by evaluating the following six Function Areas as follows:

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

As part of our evaluation, we evaluated and responded to the fiscal year (FY) 2025 20 Core and five Supplemental Inspector General (IG) Metrics specified by Office of Management and Budget (OMB) in the *FY 2025 IG Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0* (issued on April 3, 2025). We assessed the maturity levels on behalf of the Department of the Treasury's Office of Inspector General. See Appendix I for the results of each metric and assessed maturity level.

Methodology

The overall strategy of our evaluation considered the following: (1) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5.1.1, *Security and Privacy Controls for Information Systems and Organizations*; (2) NIST SP 800-53A, Revision 5.1.1, *Assessing Security and Privacy Controls in Information Systems and Organizations*; (3) *FY 2025 IG FISMA Reporting Metrics v2.0*; and (4) the Council's policies and procedures. Our testing procedures were developed from NIST SP 800-53A, Revision 5.1.1. For each of the FY 2025 20 Core and five Supplemental Metrics, we indicated whether the Council achieved each maturity

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

level by stating "MET" or "NOT MET." Core and Supplemental Metrics were averaged independently to determine a domain's maturity calculation and provide data points for the assessed program and function effectiveness. Appendix I shows the FISMA questions followed by the narrative of the maturity level.

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

In testing the effectiveness of the security controls relevant to the 20 Core and five Supplemental Metrics specified in OMB's *FY 2025 IG FISMA Reporting Metrics v2.0*, we tested the Council's entire population of administrative controls. The application controls were the responsibility of the Council's service providers. For the non-Department of the Treasury service providers, we examined the applicable service level agreements to gain an understanding of the terms and conditions and agreed-upon procedures for delivering enterprise services to the Council. For the Department of the Treasury-based service provider, we examined the relevant System and Organization Controls 1 report, to determine if the controls were designed and operating effectively and if there were any issues that could impact the user's entity environment.

We conducted the FISMA evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* issued in December 2020; and other evaluation requirements contained in the following: (1) OMB Circular No. A-130, *Managing Information as a Strategic Resource*; (2) OMB M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*; (3) NIST SP 800-53, Revision 5.1.1, *Security and Privacy Controls for Information Systems and Organizations* dated November 7, 2023; (4) NIST *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, dated April 16, 2018, and (5) *FY 2025 IG FISMA Reporting Metrics v2.0* criteria.

We based our FY 2025 FISMA evaluation approach on Federal information security guidelines developed by NIST, OMB, and the Council. NIST SPs provide guidelines considered essential to developing and implementing the Council's security programs. We applied the following criteria in performing the Council's FY 2025 FISMA evaluation.

NIST FIPS and SPs

- *NIST Cybersecurity Framework (CSF 2.0)*
- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
- FIPS Publication 201-3, *Personal Identity Verification (PIV) of Federal Employees and Contractors*

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

- NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*
- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*
- NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- NIST SP 800-40, Revision 4, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*
- NIST SP 800-53, Revision 5.1.1, *Security and Privacy Controls for Information Systems and Organizations*
- NIST SP 800-53A, Revision 5.1.1, *Assessing Security and Privacy Controls in Information Systems and Organizations*
- NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*
- NIST SP 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-61, Revision 3, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile*
- NIST SP 800-63-3, *Digital Identity Guidelines*
- NIST SP 800-83, Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*
- NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*
- NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*
- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
- NIST SP 800-161, Revision 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*
- NIST SP 800-181, Revision 1, *Workforce Framework for Cybersecurity* (*NICE Framework)*
- NIST SP 800-207, *Zero Trust Architecture*
- NIST SP 800-218, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*
- NIST Interagency Report 8011, *Automation Support for Security Control Assessments: Volume 1: Overview*
- NIST Interagency Report 8011, *Automation Support for Security Control Assessments: Volume 2: Hardware Asset Management*
- NIST Interagency Report 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*

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

OMB Policy Directives

- *FY 2025 IG FISMA Reporting Metrics v2.0*
- OMB M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*
- OMB M-24-15, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP)*
- OMB M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*
- OMB M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*
- OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*
- OMB M-21-30, *Protecting Critical Software Through Enhanced Security Measures*
- OMB M-20-32, *Improving Vulnerability Identification, Management, and Remediation*
- OMB M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative*
- OMB M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*
- OMB M-17-26, *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda*
- OMB M-17-09, *Management of Federal High Value Assets*
- OMB M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*
- OMB Circular No. A-130, *Managing Information as a Strategic Resource*

GAO

- Standards for Internal Control in the Federal Government, September 2014

Cybersecurity and Infrastructure Security Agency

- Binding Operational Directive (BOD) 25-01, *Implementing Secure Practices for Cloud Services*
- BOD 23-02, *Mitigating the Risk from Internet-Exposed Management Interfaces*
- BOD 23-01, *Improving Asset Visibility and Vulnerability Detection on Federal Networks*
- BOD 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*
- BOD 20-01, *Develop and Publish a Vulnerability Disclosure Policy*
- BOD 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*
- BOD 18-02, *Securing High Value Assets*
- BOD 18-01, *Enhance Email and Web Security*
- BOD 17-01, *Removal of Kaspersky-Branded Products*
- BOD 16-03, *2016 Agency Cybersecurity Reporting Requirements*
- BOD 16-02, *Threat to Network Infrastructure Devices*
- Emergency Directive (ED) 24-02, *Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System*

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

- ED 24-01 *Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities*
- ED 22-03 *Mitigate VMware Vulnerabilities*
- ED 21-04, *Mitigate Windows Print Spooler Service Vulnerability*
- ED 21-03, *Mitigate Pulse Connect Secure Product Vulnerabilities*
- ED 21-02, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*
- ED 21-01, *Mitigate SolarWinds Orion Code Compromise*
- ED 20-04, *Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday*
- ED 20-03, *Mitigate Windows DNS Server Remote Code Execution Vulnerability from July 2020 Patch Tuesday*
- ED 20-02, *Mitigate Windows Vulnerabilities from January 2020 Patch Tuesday*
- ED 19-01, *Mitigate DNS Infrastructure Tampering*

The CIO Council's FISMA's policies and procedures

- Council Information Technology Policy and Procedures, April 2025

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

Appendix I: FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Results

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

Key Changes to the FY 2025 IG FISMA Reporting Metrics

One of the goals of the annual FISMA evaluations is to assess agencies' progress toward achieving objectives that strengthen Federal cybersecurity. The IG FISMA Reporting Metrics have been updated to determine the agency progress in achieving the objectives, as follows:

- NIST Cybersecurity Framework (CSF) 2.0. NIST published CSF Version 2.0, highlighting the critical role that governance plays in managing cybersecurity risks and incorporating cybersecurity into an organization's broader enterprise risk management strategy. As such, a new Function Area (*Govern*) has been created that includes a new domain (*Cybersecurity Governance*). In addition, new Supplemental Metrics are designed to assess the maturity of an organization's:
    - Use of cybersecurity profiles to understand, tailor, assess, prioritize and communicate cybersecurity objectives.
    - Cybersecurity risk management strategy, which establishes an organization's priorities, constraints, risk tolerance and appetite statements and is used to support operational risk decisions.
    - Processes and authorities to foster cybersecurity accountability, performance assessment, and continuous improvement.

  In addition, to align with the CSF 2.0, the supply chain risk management (SCRM) domain moved from the *Identify* Function Area to the *Govern* Function Area and renamed to Cybersecurity SCRM (C-SCRM) to better reflect the cybersecurity environment. Furthermore, a new domain in the Identify Function Area (Risk and Asset Management) has been established to group metrics on system inventory and hardware, software, and data management.

- Zero Trust Architecture (ZTA) Implementation. The FY 2025 metrics include two new Supplemental Metrics that are critical to achieving ZTA objectives. These new metrics assess the maturity of an organization's (1) data management capabilities, and (2) ability to monitor and measure the integrity and security posture of all owned and associated assets.[17]

- Supplemental metrics for FY 2025. Five new Supplemental Metrics are in scope for the FY 2025 IG FISMA evaluation.

- Information System Level Risk Management. The Core Metric on information system level risk management (*Metric 11, formerly Metric 5*) has been revised to focus on the maturity of agencies' implementation of the NIST risk management framework.

- Unique IG FISMA Metric identifier. Each metric question has a unique identifier, indicated in bold text, to assist with tracking metric revisions or moves.

[17] For the FY 2026 IG FISMA review cycle, OMB and CIGIE will consider including additional Core or Supplemental Metrics that focus on measuring the maturity of agencies implementation of ZTA, as necessary.

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

FY 2025 Core and Supplemental Metrics

In addition to the 20 FISMA Core Metrics that must be evaluated annually, OMB and CIGIE issued five Supplemental Metrics to assess in FY 2025 FISMA evaluation.

Govern – Cybersecurity Governance

- Question 1: Organizational Context (*Supplemental Metric*)
- Question 2: Risk Management Strategy (*Supplemental Metric*)
- Question 3: Roles, Responsibilities, and Authorities (*Supplemental Metric*)

Govern – C-SCRM

- Question 5: SCRM Oversight

Identify – Risk and Asset Management

- Question 7: Information Technology (IT) Inventory
- Question 8: Asset Management – Hardware Inventory Listing
- Question 9: Asset Management – Software Inventory Listing
- Question 10: Data Management (*Supplemental Metric*)
- Question 11: Information System Risk Governance
- Question 12: Enterprise View of Cybersecurity Risk

Protect – Configuration Management

- Question 14: Security Configuration Settings
- Question 15: Flaw Remediation

Protect – Identity and Access Management

- Question 17: Strong Authentication Mechanisms for Non-Privileged Users
- Question 18: Strong Authentication Mechanisms for Privileged Users
- Question 19: Least Privilege and Separation of Duties

Protect – Data Protection and Privacy

- Question 21: Personally Identifiable Information Security Controls
- Question 22: Data Exfiltration

Protect – Security Training

- Question 24: Assessment of Skills, Knowledge, and Abilities of Organization Workforces

Detect – Information Security Continuous Monitoring (ISCM)

- Question 26: ISCM Strategy
- Question 27: Monitor Assets (*Supplemental Metric*)
- Question 28: Ongoing System Authorizations

Respond – Incident Response

- Question 30: Incident Detection and Analysis
- Question 31: Incident Handling

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

Recover – Contingency Planning

- Question 33: Business Impact Analysis
- Question 34: IT Contingency Plan Testing

GOVERN – Cybersecurity Governance

Question 1: To what extent does the organization develop and maintain cybersecurity profiles that are used to understand, tailor, assess, prioritize, and communicate its cybersecurity objectives? OMB Circular A-123, OMB Circular A-130, FISMA 2014 (**Supplemental)**[18]

Evaluation: Consistently Implemented (Level 3)

Comments: The Council has not refined its organizational profiles periodically based on known risk exposure and residual risk. In addition, the Council's risk strategy was not used to align security architectures and investments. As such, the maturity level was "Consistently Implemented."

Question 2: To what extent does the organization use a cybersecurity risk management strategy to support operational risk decisions? OMB Circular A-123, OMB Circular A-130, FISMA 2014. **(Supplemental)**

Evaluation: Optimized (Level 5)

Comments: The Council continuously monitors its cybersecurity risk management program in near real-time, leveraging predictive analytics and threat intelligence to proactively adjust strategies. Governance structures ensure near real-time decision-making.

The cybersecurity risk management program is fully integrated at the Council, mission/business process, and information system levels, as well as with the Council's enterprise risk management program. As such, the maturity level was "Optimized."

Question 3: To what extent do cybersecurity roles, responsibilities, and authorities foster accountability, performance assessment, and continuous improvement? OMB Circular A-123, OMB Circular A-130, FISMA 2014, NIST FIPS 200. **(Supplemental)**[19]

Evaluation: Optimized (Level 5)

Comments: The Council holds personnel accountable and enforces the Council's cybersecurity requirements. As such, the maturity level was "Optimized."

GOVERN – Cybersecurity Supply Chain Risk Management

Question 5: To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity

[18] Abbreviation: (OMB): Office of Management and Budget.
[19] Abbreviations: (NIST): National Institute of Standards and Technology, (FIPS): Federal Information Processing Standards.

and supply chain requirements? OMB Circular A-130, OMB M-19-03, M-22-18, Executive Order (EO) 14028, The Federal Acquisition Supply Chain Security Act of 2018. **(Core)**[20]

Evaluation: Managed and Measurable (Level 4)

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

IDENTIFY – Risk and Asset Management

Question 7: 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? FISMA 2014, Federal Information Technology Acquisition Reform Act (FITARA) of 2014, OMBs M-16-12, M-19-03, M-21-31, M-25-04, OMB Circulars A-130, A-123, NIST FIPs 199, 200. **(Core)**[21]

Evaluation: Managed and Measurable (Level 4)

Comments: The Council did not use automation to develop and maintain a centralized information system inventory that included hardware and software components from all organizational information systems. Also, the centralized inventory was not updated on a near real-time basis. Recognizing the unique size and structure of the Council's information systems, the Council's maturity level for this metric was "Managed and Measurable."

Question 8: To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including Government Furnished Equipment (GFE), Internet of Things [IoT], and Bring Your Own Device [BYOD] mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting? FISMA 2014, FITARA 2014, OMB Circulars A-130, A-123, OMB-M-25-04, DHS Binding Operational Directive (BODs) 23-01, 23-02. **(Core)**

Evaluation: Managed and Measurable (Level 4)

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

Question 9: 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

[20] Abbreviation: (EO): Executive Order.
[21] Abbreviations: (FISMA): Federal Information Security Modernization Act of 2014.

organization with the detailed information necessary for tracking and reporting? FISMA 2014, FITARA 2014, OMB M-25-04, A-130, M-21-30, EO 14028, M-22-18. **(Core)**[22]

Evaluation: Managed and Measurable (Level 4)

Comments: The Council did not employ automation to track the life cycle of the organization's software assets (and their associated licenses) with processes that limit the manual/procedural methods for asset management. However, software inventories were regularly updated as part of the organization's enterprise architecture in current and future states. The only software assets the Council was responsible for were the operating system installed on its laptops. It should be noted that the Council was a user (stakeholder) of all its information systems. Recognizing the unique size and structure of the Council's information systems, the Council's maturity level for this metric was "Managed and Measurable."

Question 10: To what extent does the organization develop and maintain inventories of data and corresponding metadata for designated data types, as appropriate throughout the data lifecycle? FISMA 2014, Privacy Act, Federal Records Act, EO 14028. **(Supplemental)**

Evaluation: Consistently Implemented (Level 3)

Comments: We determined that, although Council uses data centric security tools, they have not ensured that the data and corresponding metadata in its inventories are subject to the monitoring processes defined within the Council's ISCM strategy. As such, the Council's maturity level for this metric was "Consistently Implemented."

Question 11: To what extent does the organization ensure that information system security risks are adequately managed? FISMA 2014, EO 13800, EO 14028, OMB Circulars A-123, A-130, OMB M-25-04, OMB M-19-03. **(Core)**

Evaluation: Managed and Measurable (Level 4)

Comments: Based on the examination of the evidence, the Council has not fully integrated its organizational and business processes at all levels of the agency or established a Cybersecurity Framework profile to align cybersecurity outcomes with mission requirements, risk tolerance, and resources of the organization to ensure that continuous identification and monitoring of all risk remains at acceptable levels. However, we determined the Council is a micro-agency with a unique organizational size and structure. As such, we assessed the maturity level as "Managed and Measurable."

Question 12: To what extent does the organization use technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboard? EO 14028, OMB Circulars A-123, A-130. **(Core)**

[22] Abbreviation: (FITARA): Federal Information Technology Acquisition Reform Act.

Evaluation: Consistently Implemented (Level 3)

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

PROTECT – Configuration Management

Question 14: To what extent does the organization use configuration settings/common secure configurations for its information systems? FISMA 2014, OMB Circular A-130, M-25-04, M-21-31. **(Core)**

Evaluation: Managed and Measurable (Level 4)

Comments: The Council did not deploy system configuration management tools that automatically enforce and redeploy configuration settings to systems at frequent intervals as defined by the organization, or on an event-driven basis. However, due to the unique structure of the Council's information systems, the maturity level was "Managed and Measurable."

Question 15: To what extent does the organization use flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management, to manage software vulnerabilities on all network addressable IP assets? OMB M-25-04, Circular A-130, FIPS 200, DHS BODs 18-02, 19-02, 22-01, 23-01. **(Core)**[23]

Evaluation: Managed and Measurable (Level 4)

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

PROTECT – Identity and Access Management

Question 17: To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO2, or web authentication) for non- privileged users to access the organization's physical and logical assets [organization-defined entry/exit points],

[23] Abbreviations: (DHS) Department of Homeland Security, (BOD): Binding Operational Directive.

networks, and systems, including for remote access? Cybersecurity Enhancement Act 2016, FIPS 201-2, HSPD-12, EO 14028, OMB M-19-17, M-25-04. **(Core)**[24]

Evaluation: Managed and Measurable (Level 4)

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

Question 18: To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO2, or web authentication) for privileged users to access the organization's physical and logical assets [organization-defined entry/exit points], networks, and systems, including for remote access? FIPS 201-2, HSPD-12, EO 14028, OMB M-19-17, M-25-04, DHS ED 19-01. **(Core)**

Evaluation: Managed and Measurable (Level 4)

Comments: Due to the unique structure of the council information systems, having 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 (privilege) accounts and privileges centrally and report on the effectiveness on a near real-time basis will require financial commitment and cost-benefits that may not be justifiable in the Council environment. As such, the maturity level was "Managed and Measurable."

Question 19: 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? Cybersecurity Enhancement Act 2016, EO 14028, OMB A-130, M-19-17, M-21-31, DHS ED 19-01. **(Core)**

Evaluation: Managed and Measurable (Level 4)

Comments: The Council has not made progress towards implementing event logging (EL) 3's advanced requirements for user behavior monitoring to detect and alert privileged user compromise. However, due to the unique organizational structure of the Council's information systems, the maturity level was "Managed and Measurable."

[24] Abbreviations: (PIV): Personal Identity Verification, (FIDO2) Fast Identity Online 2, (HSPD) Homeland Security Presidential Directive, (ED): Emergency Directive.

PROTECT – Data Protection and Privacy

Question 21: To what extent has the organization implemented the following security controls to protect the confidentiality, integrity, and availability of its PII and other agency sensitive data, as appropriate, throughout the data lifecycle? OMB Circular A-130, EO 14028, DHS BOD 18-02.[25]

- 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
- Backups of data are created, protected, maintained, and tested
- Access to personal email, external file sharing and storage sites, and personal communication applications are blocked, as appropriate. **(Core)**

Evaluation: Managed and Measurable (Level 4)

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

Question 22: To what extent has the organization implemented security controls (e.g., DLP, IDPS, CASB, User and Entity Behavior Analytic tools, SIEM and EDR) to prevent data exfiltration and enhance network defenses? DHS BOD 18-01, ED 19-01, OMB M-21-07, M-22-01. **(Core)**[26]

Evaluation: Managed and Measurable (Level 4)

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

PROTECT – Security Training

Question 24: To what extent does the organization use an assessment of the skills, knowledge, and abilities of its workforce to provide specialized security training within the functional areas of: govern, identify, protect, detect, respond, and recover? Cyber Workforce Assessment Act 2015, EO 13870. **(Core)**

[25] Abbreviation: (PII): Personally Identifiable Information.

[26] Abbreviations: (DLP): Data Loss Prevention, (IDPS): Intrusion Detection and Prevention Systems, (CASB): Cloud Access Security Blocker, (SIEM): Security Information and Event Management, (EDR): Endpoint Detection and Response.

Evaluation: Managed and Measurable (Level 4)

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

DETECT – Information Security Continuous Monitoring

Question 26: To what extent does the organization use information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier? FISMA 2014, OMB A-130, M-25-04, NIST FIPS 200. **(Core)**

Evaluation: Managed and Measurable (Level 4)

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

Question 27: To what extent does the organization monitor and measure the integrity and security posture of all owned and associated assets? EO 14028, OMB A-130, M-21-31. **(Supplemental)**

Evaluation: Optimized (Level 5)

Comments: The Council has institutionalized the implementation of advanced ISCM technologies for analysis of trends and identification of potentially adverse events and adjusts its ISCM processes and security measures accordingly.

The Council continuously verifies insights and enforces compliance throughout the lifetime of devices and virtual assets. The Council integrates device, software, configuration, and vulnerability management across all Council environments, including for virtual assets. The Council employs more sophisticated approaches to continuous monitoring. As such the maturity level was "Optimized."

Question 28: To what extent does the organization perform ongoing (continuous monitoring) information system assessments to grant system authorizations, including developing and maintaining system security plans, and monitoring system security controls? [ISCM.03] OMB A-130, M-14-03, M-19-03, EO 14028. **(Core)**

Evaluation: Managed and Measurable (Level 4)

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

RESPOND – Incident Response

Question 30: To what extent does the organization implement processes related to incident detection and analysis? OMB M-20-04, M-21-31, M-22-01, M-25-04. **(Core)**

Evaluation: Managed and Measurable (Level 4)

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

Question 31: To what extent has the organization implemented processes related to incident handling? EO 14028, OMB M-21-31, OMB M-25-04. **(Core)**

Evaluation: Consistently Implemented (Level 3)

Comments: The Council did not experience any incidents in FY 25, and hence, we cannot validate if the Council manages and measures the impact of successful incidents and can quickly mitigate related vulnerabilities on other systems so that they are not subject to exploitation of the same vulnerability. Recognizing the unique size and structure of the Council's information systems, the Council's maturity level for this metric was "Consistently Implemented."

RECOVER – Contingency Planning

Question 33: To what extent does the organization ensure that the results of BIAs are used to guide contingency planning efforts? OMB A-130, M-19-03, FIPS 199. **(Core)**

Evaluation: Managed and Measurable (Level 4)

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

Question 34: To what extent does the organization perform tests/exercises of its information system contingency planning processes? OMB A-130, M-19-03. **(Core)**

Evaluation: Consistently Implemented (Level 3)

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

Appendix II: Management's Response

Gulf Coast Ecosystem Restoration Council

July 28, 2025

Loren Sciurba
Deputy Inspector General
Department of the Treasury
875 15th St. NW
Washington, DC 20005

Re: The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2025

Thank you for the opportunity to review The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2015 Evaluation Report for Fiscal Year 2025.

The Council agrees with the results of the evaluation for Fiscal Year 2025 that the Council's information security program and practices were effective for the period April 1, 2024 through March 31, 2025.

In Fiscal Year 2026, 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 ecosystem restoration in the Gulf Coast region.

Sincerely,

MARY WALKER Digitally signed by MARY WALKER Date: 2025.07.28 10:00:25 -05'00'

Mary S. Walker
Executive Director
Gulf Coast Ecosystem Restoration Council

This Page Intentionally Left Blank

REPORT WASTE, FRAUD, AND ABUSE

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

TREASURY OIG WEBSITE

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