



Evaluation Report



OIG-CA-26-037

CYBERSECURITY/INFORMATION TECHNOLOGY

**The Gulf Coast Ecosystem Restoration Council Federal
Information Security Modernization Act of 2014
Evaluation Report for Fiscal Year 2026**

August 10, 2026

**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 10, 2026

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 2026 (OIG-CA-26-037)

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 2026*, dated August 4, 2026. 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, 2025, through March 31, 2026. 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 appropriate and effective for the period April 1, 2025, through March 31, 2026.

Appendix I of the attached RMA report includes the Fiscal Year 2026 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

**The Gulf Coast Ecosystem Restoration Council
Federal Information Security Modernization Act of 2014
Evaluation Report for Fiscal Year 2026**

August 4, 2026

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 2026

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) 2026. 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, 2025, through March 31, 2026.

For FY 2026, 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 v2.0¹* dated April 3, 2025. The IG was required to assess the maturity levels of those metrics. We conducted an evaluation of the FY 2026 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 2026 IG FISMA Reporting Metrics.

In summary, we found the Council's information security program and practices were effective for the period April 1, 2025, through March 31, 2026.

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

¹ Based on a joint message from OMB and CIGIE received on March 17, 2026, on the FY 2026 IG FISMA Metrics and Implementation Guidance, IG's and independent external auditors, as appropriate, are directed to use the *FY 2025 IG FISMA Reporting Metrics*.

Table of Contents

Abbreviations.....	1
Introduction.....	2
Summary of Evaluation Results.....	2
Background.....	3
Federal Information Security Modernization Act of 2014.....	3
Evaluation Results.....	5
Objective, Scope, and Methodology	11
Appendix I: FY 2026 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Results	16
Appendix II: Management’s Response.....	28

Abbreviations

BOD	Binding Operational Directive
CIO	Chief Information Officer
CASB	Cloud Access Security Broker
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
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
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

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)² 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 for collecting annual FISMA responses to the Department of Homeland Security (DHS).

The Department of the Treasury's Office of Inspector General engaged RMA Associates, LLC (RMA) to conduct the Fiscal Year (FY) 2026 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, 2025, through March 31, 2026.

As part of our evaluation, we responded to the FY 2026 metrics from OMB's *FY 2025 Inspector General (IG) FISMA Reporting Metrics v2.0* dated April 3, 2025.³ For FY 2026, five Supplemental Metrics were evaluated in addition to the 20 Core Metrics. These six 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. It provides Inspector General (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 Areas⁴ and ten FISMA Metric Domains⁵ 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

² Public Law 113-283, Federal Information Security Modernization Act of 2014, December 18, 2014.

³ Based on a joint message from OMB and CIGIE received on March 17, 2026, on FY 2026 IG FISMA Metrics and Implementation Guidance, IG's and independent external auditors, as appropriate, are directed to use the *FY 2025 IG FISMA Reporting Metrics*.

⁴ 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.

⁵ 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.

Measurable. We found the Council's information security program and practices were appropriate and effective for the period April 1, 2025, through March 31, 2026.

We provided the Council with a draft of this report for comments. 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 comprises the following Federal agencies: the U.S. Departments of Agriculture, the Army, Commerce, Homeland Security, and 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 the 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 agencies' compliance, and produced reports that highlighted issues caused by security incidents.

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

FISMA reestablished the oversight authority of the Director of the OMB with respect to agency information security policies and practices and set forth the authority of the Secretary of DHS to administer the implementation of such policies and practices for information systems.⁶

FISMA requires the Secretary of DHS to develop and oversee the implementation of operational directives requiring agencies to implement the 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.⁷

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.⁸

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.⁹

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.¹⁰

FY 2026 Core and Supplemental Metrics

OMB's *FY 2025 IG FISMA Reporting Metrics v2.0*, dated April 3, 2025, specified the FY 2026 20 Core and five Supplemental Metrics (refer to Appendix I). The FY 2026 FISMA Metrics were aligned with six Function Areas:

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

⁶ Federal Information Security Modernization Act of 2014, Public Law No. 113-283, December 2014, <https://www.congress.gov/bill/113th-congress/senate-bill/2521>.

⁷ Ibid, *Summary*.

⁸ Ibid, *Summary*.

⁹ Ibid, *Summary*.

¹⁰ Ibid, *Summary*.

- Recover, which includes questions pertaining to Contingency Planning Domain.

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 2026 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 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.

The scope of our evaluation was conducted for the period between April 1, 2025, and March 31, 2026. 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, in which Core and Supplemental Metrics are averaged independently to determine a domain’s maturity and to provide data points for the assessed program and function effectiveness. For example, if the calculated Core Metric maturity of two of the function areas was Level 3 (Consistently Implemented) (i.e., 3.0) and the computed Core Metric maturity of the remaining three function areas was Level 4 (Managed and Measurable) (i.e., 4.0), the information security program rating would average a 3.60 (3+3+4+4+4)/5.

Core and Supplemental Metrics were averaged independently to determine a domain's maturity and to provide data points on the assessed program and function effectiveness. The Council's overall program calculation is shown in [Table 2](#). The Council's FY 2026 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 2026

Function Area	Core Metrics	FY 2026 Supplemental Metrics ¹¹	FY 2026 Assessed Maturity Average ¹²	FY 2026 Assessed Maturity
Govern ¹³	4	4.67	4.5	Managed and Measurable
Identify	3.8	3	3.67	Consistently Implemented
Protect	4.13	N/A	4.13	Managed and Measurable
Detect	4	5	4.33	Managed and Measurable
Respond	3.5	N/A	3.5	Consistently Implemented
Recover	3.5	N/A	3.5	Consistently Implemented
Overall Maturity	3.82	4.22	4	Managed and Measurable¹⁴

Table 3: The Council's FY 2026 Maturity Levels

Function Area ¹⁵	Core Metrics	FY 2026 Supplemental Metrics	FY 2026 Assessed Maturity	RMA's FY 2026 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 Measurable¹⁴	Managed and Measurable	Managed and Measurable¹⁴	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 data points to support our risk-based determination of overall program- and function-level effectiveness. The overall maturity level of the information security program was determined as Managed and Measurable.

¹¹ Protect, Respond, and Recover only consist of Core Metrics.

¹² The FY 2026 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.

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 to be Managed and Measurable based on RMA's assessment of these activities and the calculated average scores for each domain. Our tests of effectiveness for this evaluation found no exceptions.

Although we did not find any exceptions, our evaluation identified a broader resource consideration related to the Council's IT oversight structure:

At present, oversight of the Council's IT infrastructure resides with a single individual, the CIO. For FY 2027, Council expects notable changes to its IT operating environment, including potential adjustments in responsibilities currently managed by shared service providers.

From an information security and risk management standpoint, evolving operational demands, coupled with rising cybersecurity threats, underscore the need to periodically reassess the alignment between IT responsibilities and available resources. As such, the Council should consider evaluating whether the current IT staffing model sufficiently supports effective oversight, continuity of operations, segregation of duties, and timely incident response.

This evaluation suggests that the Council could include exploring opportunities to enhance support structures or redistribute responsibilities to strengthen the security posture, reduce single points of failure, and sustain effective governance of critical IT functions. Such considerations may include the potential for additional dedicated roles - such as information security leadership (e.g., a Chief Information Security Officer function) to further enhance cybersecurity oversight and risk management capabilities. Maintaining an appropriate balance among resources, responsibilities, and risk tolerance will help the Council to better safeguard its systems and data while continuing to support its mission efficiently and resiliently.

Below is the maturity level for each domain during this evaluation.

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 is conducted to hold personnel accountable and enforce the Council's cybersecurity requirements. Our testing found no exceptions in cybersecurity governance, and the existing controls were operating as intended. We concluded that 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. In addition, they used qualitative and quantitative metrics to measure, report on, and monitor Cybersecurity Supply Chain Risk Management. 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 intended. We concluded that 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, which entails 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 that 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 used automation to maintain an up-to-date, complete, accurate, and readily available view of the security configurations of information system components connected to the Council's network. Our testing found no exceptions, and the controls were

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.

operating as intended. We concluded that 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 and were not shared; they 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 that 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 Privacy program was Managed and Measurable. The Council did not process Personally Identifiable Information (PII) data. All PII needed for human resources, and payroll was handled through agreements with third parties, which subsequently have systems approved to collect and process PII. All controls over PII were the responsibility of the Council's outsourced service providers. We concluded that the Council's Data Protection and Privacy controls in place were effective.

Security Training: We determined the Council's overall maturity level for the Security Training program was Managed and Measurable. The Council effectively allocated resources in a risk-based manner for stakeholders to implement security awareness training consistently. The Council addressed its identified knowledge, skills, and abilities gaps through talent acquisition. Our testing of the Council's workforce assessment found no exceptions, and controls were operating as intended. We concluded that 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 quantitative and qualitative 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 that the Council's Information Security and Continuous Monitoring program was effective.

Incident Response: We determined the Council's overall maturity level for the Incident Response program was Consistently Implemented. Given that 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 that 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 and measurable. 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, 2025, through March 31, 2026.

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, 2025, through March 31, 2026.

Scope

The scope of our work included the Council's Office Support Network (OSN) and the 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, 2025, and March 31, 2026.

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) 2026 20 Core and five Supplemental Inspector General (IG) Metrics specified by the 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 2026 20 Core and five Supplemental Metrics, we indicated whether the Council achieved each maturity level by stating “MET” or “NOT MET.” Core and Supplemental Metrics were averaged independently to determine a domain’s maturity calculation and provide data points for the assessed program and function effectiveness. Appendix I shows the FISMA questions followed by the narrative of the maturity level.

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 whether the controls were designed and operated effectively and whether there were any issues that could impact the user’s entity environment.

We based our FY 2026 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 2026 FISMA evaluation.

NIST FIPS and SPs

- FIPS Publication 199, *Standards for Security Categorization of Federal Information, and Information Systems*
- FIPS Publication 200, *Minimum Security Requirements for Federal Information, and Information Systems*
- FIPS Publication 201-3, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
- NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*
- 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 800-50, Revision 1, *Building a Cybersecurity and Privacy Learning Program*
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*
- NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*
- NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*
- NIST SP 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-61, Revision 3, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile*
- NIST SP 800-63-4, *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, Revision 1, *Integrating Cybersecurity and Enterprise Risk Management*

OMB Policy Directives

- OMB Memorandum M-26-14, *Ensuring Effective and Efficient Agency Logging and Network Visibility to Defend Against Evolving Cyber Threats*
- OMB Memorandum M-26-05, *Adopting a Risk-based Approach to Software and Hardware Security*

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

DHS

- *FY 2025 IG FISMA Reporting Metrics*
- DHS Emergency Directives 26-01 (v1), *Mitigate Vulnerabilities in F5 Devices*
- DHS Emergency Directives 26-03: *Mitigate Vulnerabilities in Cisco SD-WAN Systems*
- DHS Emergency Directives 25-03, *Identity and Mitigate Potential Compromise of Cisco Devices*
- DHS Emergency Directives 25-02, *Mitigate Microsoft Exchange Vulnerability*
- DHS Emergency Directives 24-01, *Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities*
- DHS Binding Operational Directive 26-02, *Mitigating Risk From End-of-Support Edge Devices*
- DHS Binding Operational Directive 25-01, *Implementing Secure Practices for Cloud Services*
- DHS Binding Operational Directive 23-02, *Mitigating the Risk from Internet-Exposed Management Interfaces*
- DHS Binding Operational Directive 23-01, *Improving Asset Visibility and Vulnerability Detection on Federal Networks*
- DHS Binding Operational Directive 20-01, *Develop and Publish Vulnerability Disclosure Policy*
- DHS Binding Operational Directive 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*
- DHS Binding Operational Directive 18-02, *Securing High Value Assets*

- DHS Binding Operational Directive 18-01, *Enhance Email and Web Security*
- DHS Binding Operational Directive 17-01, *Removal of Kaspersky-branded Products*
- DHS Binding Operational Directive 16-03, *2016 Agency Cybersecurity Reporting Requirements*
- DHS Binding Operational Directive 16-02, *Threat to Network Infrastructure Devices*

The CIO Council's FISMA's policies and procedures

- Council Information Technology Policy and Procedures, April 2025

**Appendix I: FY 2026 Inspector General Federal Information Security
Modernization Act of 2014 (FISMA) Reporting Metrics Results**

FY 2026 FISMA 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 the FY 2026 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: System Inventory
- Question 8: Asset Management – Hardware Inventory Listing
- Question 9: Asset Management – Software Inventory Listing
- Question 10: Data Management (*Supplemental Metric*)
- Question 11: Cybersecurity Risk Management and Enterprise Risk Management Integration
- Question 12: Automated View of 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

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)**¹⁷

Evaluation: Managed and Measurable (Level 4)

Comments: Cybersecurity Risk Management activities were formally established, consistently implemented, and monitored through defined processes and governance practices. The Council maintains documented cybersecurity objectives and utilizes performance measures to evaluate the effectiveness of its cybersecurity risk management program. Management oversight and periodic reviews supported informed decision-making and continuous refinement of cybersecurity practices. Given the Council’s size and organizational structure, cybersecurity activities were managed in a structured and repeatable manner, providing measurable assurance that risk management objectives were being achieved and aligned with organizational needs. As such, the maturity level was “Managed and Measurable.”

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)**¹⁸

Evaluation: Optimized (Level 5)

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

¹⁷ Abbreviation: (OMB): Office of Management and Budget.

¹⁸ Abbreviations: (NIST): National Institute of Standards and Technology, (FIPS): Federal Information Processing Standards.

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 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)**¹⁹

Evaluation: Managed and Measurable (Level 4)

Comments: The Council uses qualitative and quantitative performance metrics (e.g., those defined within SLAs) to measure, report on, and monitor the C-SCRM performance of organizationally defined products, systems, and services provided by external providers. In addition, the Council has incorporated supplier risk evaluations, based on criticality, into its continuous monitoring practices to maintain situational awareness into the cyber-related supply chain risks. 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)**²⁰

Evaluation: Managed and Measurable (Level 4)

Comments: The Council has information systems and is most effectively managed by a third party via an interagency agreement. In addition, the Council has developed a continuous monitoring plan that incorporates the ISCM strategy, the monitoring process of performing an annual review of its information system inventory is consistent. As such, 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)**²¹

Evaluation: Managed and Measurable (Level 4)

Comments: The Council maintains an inventory of its hardware assets and monitors its assets on a real-time basis. The hardware assets are connected to the network and its

¹⁹ Abbreviation: (EO): Executive Order.

²⁰ Abbreviations: (FISMA): Federal Information Security Modernization Act of 2014, (FITARA): Federal Information Technology Acquisition Reform Act.

²¹ Abbreviations: (DHS): Department of Homeland Security, (BOD): Binding Operational Directive.

internet and subject to the monitoring processes defined within its ISCM strategy. 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 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)**

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: The Council evaluates the risk based on the system level for the potential impact on an organization should certain events jeopardize the information and information systems needed by the Council to accomplish its assigned mission, protect its assets, and maintain its day-to-day functions, and protect individuals. The Council monitors and analyzes its defined qualitative and quantitative performance measures through its risk register. In addition, the Council performs the risk profile that depicts the assessment results determining the Council's Risk Profile and Critical Risk Mitigation highlights. 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)**

Evaluation: Consistently Implemented (Level 3)

Comments: The Council 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. As such, 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 had implemented Continuous Diagnostics and Mitigation capabilities for real-time reporting and dashboard views. The automated tool reporting helps the Council maintain an up-to-date, complete, accurate, and readily available view of the security configurations. As such, 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)**

Evaluation: Managed and Measurable (Level 4)

Comments: The Council utilizes automated tools for the patch compliance and vulnerability scanning that generate a monthly report summary to determine the Council’s compliance, as well as providing details of patch compliance for each device the Council possesses. The automated tool provides a dashboard view of the Council’s open vulnerabilities (critical, high, medium) and whether 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],

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)**²²

Evaluation: Managed and Measurable (Level 4)

Comments: The Council's non-privileged users use strong authentication mechanisms to authenticate applicable organizational systems and facilities. They centrally implement support for non-PIV authentication mechanisms in their enterprise identity management system. 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: The Council centrally implements support for non-PIV authentication mechanisms in their enterprise identity management system. All privileged users, even though they do not have control to make changes to Domain Name System records, use strong authentication mechanisms to authenticate to applicable organizational systems. 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: Optimized (Level 5)

Comments: The Council has made progress towards implementing event logging (EL) 3's advanced requirements for user behavior monitoring to detect and alert privileged user compromise. As such, the maturity level was "Optimized."

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 18-02.²³

²² Abbreviations: (PIV): Personal Identity Verification, (FIDO2) Fast Identity Online 2, (HSPD) Homeland Security Presidential Directive, (ED): Emergency Directive.

²³ Abbreviation: (PII): Personally Identifiable Information.

- 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 collect PII and therefore, the related monitoring processes defined within its ISCM strategy were not applicable. However, the Council has capabilities in place to protect PII and other agency-sensitive data, as appropriate. As such, 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)**²⁴

Evaluation: Managed and Measurable (Level 4)

Comments: The Council is consistently capturing test activities and procedures and sharing lessons learned on the effectiveness of its data exfiltration. The Council has assessed its current EDR capabilities, identified any gaps, and is coordinating with Cybersecurity and Infrastructure Security Agency for future EDR solution deployments. As such, 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)**

²⁴ 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)**²⁵

Evaluation: Managed and Measurable (Level 4)

Comments: The Council monitors and analyzes measures on the effectiveness of its ISCM policies and procedures and make updates as necessary. The Council has transitioned to ongoing control and system authorization through the implementation of its continuous monitoring policies and strategy. As such, 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 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: The Council utilizes the results of security control assessments and monitoring to maintain ongoing authorizations of information systems. The Council's authorization

²⁵ Abbreviation: (ISCM): Information Security Continuous Monitoring.

process included automated analysis tools and manual expert analysis as evidenced in the risk register. As such, 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 has implemented an automated tool within the Continuous Diagnostics Mitigation program to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents. In addition, they are meeting logging requirements at maturity EL2 (intermediate), in accordance with M-21-31. As such, 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 26; therefore, we cannot validate whether the Council manages and measures the impact of successful incidents and can quickly mitigate related vulnerabilities in 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 27, 2026

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 2026

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 2026*.

The Council agrees with the results of the evaluation for Fiscal Year 2026, which found that the Council's information security program and practices were effective for the period April 1, 2025 through March 31, 2026.

In Fiscal Year 2027, 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: 2026.07.27
14:44:11 -05'00'

Mary S. Walker
Executive Director
Gulf Coast Ecosystem Restoration Council



REPORT WASTE, FRAUD, AND ABUSE

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

TREASURY OIG WEBSITE

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