Independent Audit of the Council of the Inspector General on Integrity and Efficiency Compliance with the Federal Information Security Modernization Act of 2014

COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY

Fiscal Year 2025
August 18, 2025

Prepared by

Brown & Company Certified Public Accountants and Management Consultants, PLLC
6401 Golden Triangle Drive, Suite 310
Greenbelt, Maryland 20770

Mr. Andrew Cannarsa, Executive Director
Council of the Inspectors General on Integrity and Efficiency
1750 H Street, NW Suite 400
Washington, DC 20006

Dear Mr. Cannarsa:

Enclosed is the audit report on the Council of the Inspector General on Integrity and Efficiency Compliance with the Federal Information Security' (CIGIE) compliance with the Federal Information Security Modernization Act of 2014 (FISMA). The CIGIE contracted with the independent certified public accounting firm, Brown & Company CPAs and Management Consultants, PLLC (Brown & Company), to conduct the audit in support of the FISMA requirement for an annual evaluation of the CIGIE Office of Information Chief Information Officer (OCIO) information security program.

The objective of this performance audit was to determine whether CIGIE OCIO implemented selected security controls for certain information systems in support of FISMA. The audit included the testing of selected management, technical, and operational controls outlined in the National Institute of Standards and Technology Special Publication 800-53, Revision 5.1.1, *Security and Privacy Controls for Information Systems and Organizations*.

We reviewed selected controls from CIGIE's general support system for this audit. The selected controls included 20 Core and 5 Supplemental Inspector General FISMA Reporting Metrics in six security function areas — Govern, Identify, Protect, Detect, Respond, and Recover — to determine the effectiveness of the agency's information security program and the maturity level of each function area. We conducted our performance audit during the period from March 19, 2025, to August 18, 2025.

Our performance audit was performed in accordance with generally accepted government auditing standards (GAGAS) and Government Auditing Standards issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

In addition to GAGAS, we conducted this performance audit in accordance with Consulting Services Standards established by the American Institute of Certified Public Accountants (AICPA). This performance audit did not constitute an audit of financial statements, or an attestation level report as defined under GAGAS and the AICPA standards for attestation engagements.

The audit concluded that CIGIE generally complied with FISMA requirements by implementing selected security controls for tested systems; therefore, the overall controls are effective. Also, sixteen recommendations from the prior year were closed and implemented. We found CIGIE OCIO's selected controls effective.

This report is for the purpose of concluding on the audit objective described above. Accordingly, this report is not suitable for any other purpose.

We appreciate the assistance we received from the staff of CIGIE OCIO and the opportunity to serve you.

Brown & Company

Greenbelt, M aryland
August 18, 2025

Table of Contents

Summary of Results

The Federal Information Security Modernization Act of 2014[1] (FISMA) requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems[2], including those provided or managed by another agency, contractor, or other sources. Because the Council of the Inspector General on Integrity and Efficiency Compliance with the Federal Information Security (CIGIE) is a federal agency, it is required to comply with federal information security requirements.

FISMA also requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capabilities are established, and (3) information security management processes are integrated with the agency's strategic and operational planning processes. All agencies must also report annually to the U.S. Office of Management and Budget (OMB) and to congressional committees on their information security program's effectiveness. FISMA has also established that the standards and guidelines issued by the National Institute of Standards and Technology (NIST) are mandatory for federal agencies.

The CIGIE engaged Brown & Company CPAs and Management Consultants, PLLC (Brown & Company) to conduct an audit in support of the FISMA requirement for an annual evaluation of the CIGIE Office Chief Information Officer’s (OCIO) program. This performance audit's objective was to determine whether CIGIE OCIO implemented certain security controls for selected information systems in support of FISMA during fiscal year (FY) 2025. For this audit, we reviewed selected controls from CIGIE OCIO’s general support system.

Our audit was performed in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

According to OMB FY 2025 Inspector General (IG) FISMA Reporting Metrics, a security program is considered effective if the calculated average of the FY 2025 IG FISMA Reporting Metrics is at least Managed and Measurable (Level 4) overall for the six domains: Govern, Identify, Protect, Detect, Respond and Recover. Based on OMB's guidance and CyberScope results, we found that the calculated average of the Cybersecurity Functions was assessed as Managed and Measurable (Level 4), and therefore effective. Based on FISMA effectiveness standards, we found CIGIE OCIO's selected controls effective or operating as intended. Result details are provided in the following section.

[1] The FISMA Act of 2014 (Public Law 113–283— December 18, 2014) amends the FISMA Act of 2002.
[2] According to NIST, an information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Audit Results

To be considered effective, CIGIE OCIO's information security program must be rated Managed and Measurable (Level 4). We concluded that CIGIE OCIO's information system program received an overall Level 4 maturity level; therefore, the CIGIE OCIO information security program is effective.

Table-1 below details the five maturity model levels: ad hoc, defined, consistently implemented, managed and measurable, and optimized.

Table-1 Assessment Maturity Levels

Maturity Level	Maturity Level Description
Level 1: Ad-hoc	Policies, procedures, and strategies are not formalized; activities are 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 are 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.

*Within the context of the maturity model, OMB believes that achieving a Level 4 or above represents an effective level of security.

Table-2 below summarizes the overall assessed maturity levels for each function area and domain in the FY 2025 IG FISMA Reporting Metrics. Five out of six functions met the managed and measurable level, and one is optimized.

Table-2 Summary of Overall Calculated Average Maturity Levels

Function and Domain Areas	FY 25 FISMA Maturity Levels
Govern: Organizational Context; Risk Management Strategy; Roles, Responsibilities, and Authorities; Policy; Oversight; and Cybersecurity Supply Chain Risk Management	Level 4: Managed and Measurable
Identify: Asset Management, Risk Assessment, and Risk Management Strategy	Level 4: Managed and Measurable
Protect: Technology Infrastructure Resilience; Identity Management; Authentication, and Access Control; Data Security; Platform Security; and Awareness and Training	Level 4: Managed and Measurable
Detect: Continuous Monitoring and Adverse Event Analysis	Level 4: Managed and Measurable
Respond: Incident Response: Incident Management; Incident Analysis; Incident Response Reporting and Communication; and Incident Mitigation	Level 5: Optimized
Recover: Incident Recovery Plan Execution; and Incident Recovery Communication	Level 4: Managed and Measurable
Overall Effectiveness Rating – Effective	**Level 4: Managed and Measurable**

Appendix I – Scope, Methodology and Criteria

Scope

We conducted this audit in accordance with GAGAS, as specified in the Government Accountability Office's *Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. The audit was designed to determine whether CIGIE OCIO implemented selected security controls for certain information systems in support of the FISMA Act of 2014. The audit fieldwork was from March 19, 2025, through August 18, 2025 at Brown & Company in Greenbelt, Maryland, and CIGIE's headquarters in Washington, DC.

In FY 2025, the IG FISMA Reporting Metrics were revised to align with the NIST Cybersecurity Framework 2.0. A new IG FISMA function, Govern, was introduced, which includes a new domain, Cybersecurity Governance. Additionally, the Supply Chain Risk Management (SCRM) domain was moved from the Identify function to the Govern function and renamed Cybersecurity SCRM (C-SCRM). Finally, a new domain, Risk and Asset Management, was added under the Identify function to consolidate metrics related to system inventory as well as hardware, software, and data management.

Our overall objective was to evaluate CIGIE OCIO's security program and practices, as required by FISMA. Specifically, we reviewed 20 Core and 5 Supplemental IG FISMA Reporting Metrics in six security function areas — Govern, Identify, Protect, Detect, Respond, and Recover — to determine the effectiveness of the agencies' information security program and the maturity level of each function area.

Function (Domains)

- Govern (Cybersecurity Governance)
- Govern (Cybersecurity SCRM)
- Identify (Risk and Asset Management)
- Protect (Configuration Management)
- Protect (Identity and Access Management)
- Protect (Data Protection and Privacy)
- Protect (Security Training)
- Detect (Information Security Continuous Monitoring)
- Respond (Incident Response)
- Recover (Contingency Planning)

The maturity levels range from lowest to highest — Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

We also followed up on outstanding recommendations from the prior FISMA audit report (see Appendix III) and performed audit procedures on CIGIE OCIO's internal and external systems. The audit also included a review of vulnerability assessments of CIGIE OCIO-managed internal systems and an evaluation of the CIGIE OCIO process for identifying and mitigating technical vulnerabilities.

Methodology

We reviewed CIGIE OCIO's general FISMA compliance efforts in the specific areas defined in OMB guidance[3] and the corresponding reporting instructions. We considered the internal control structure for CIGIE OCIO's systems in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objectives. Accordingly, we obtained an understanding of the internal controls over CIGIE OCIO's internal system and contractor-owned and managed systems through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. Our understanding of these systems' internal controls was used to evaluate the degree to which the appropriate internal controls were designed and implemented. When appropriate, we conducted compliance tests using judgmental sampling to determine the extent to which established controls and procedures are functioning as required.

We assessed internal controls deemed significant to our audit, which include the following:

- Risk Assessment:
  - Define Objectives and Risk Tolerances
  - Identify, Analyze, and Respond to Risks
  - Identify, Analyze, and Respond to Change

- Control Activities:
  - Design Control Activities
  - Implement Control Activities

- Information and Communication:
  - Communicate Internally
  - Communicate Externally

- Monitoring:
  - Perform Monitoring Activities
  - Evaluate Issues and Remediate Deficiencies.

To accomplish our audit objective, we:

- Interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA;
- Reviewed documentation related to the CIGIE OCIO information security program, such as security policies and procedures, system security plans, and risk assessments;
- Tested system processes to determine the adequacy and effectiveness of selected controls;
- Reviewed the status of recommendations in the prior FISMA audit report; and
- Reviewed the network vulnerability assessment of the CIGIE OCIO internal system.

Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the set of internal controls for CIGIE OCIO's systems taken as a whole. There were no internal control weaknesses identified that affected the audit objective.

[3] OMB Memorandum M-24-04, Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements, December 4, 2023.

Criteria

The criteria used in conducting this audit included:

- NIST Special Publication (SP) 800-30, Revision (Rev.) 1, *Guide for Conducting Risk Assessments,* September 17, 2012;
- NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems,* November 11, 2010;
- NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* December 20, 2018;
- NIST SP 800-39, *Managing Information Security Risk Organization, Mission, and Information System View,* March 1, 2011;
- NIST SP 800-50, Rev. 1, *Building a Cybersecurity and Privacy Learning Program,* September 12, 2024*;*
- NIST SP 800-53, Rev. 5.1.1, *Security and Privacy Controls for Information Systems and Organizations, September* 2020; updated as of December 10, 2020;
- NIST SP 800-61*, Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A Cybersecurity Framework 2.0 Community Profile,* April 2025*;*
- NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information,* April 6, 2021;
- NIST SP 800-128*, Guide for Security-Focused Configuration Management of Information Systems,* October 10, 2019*;*
- NIST SP 800-137*, Information Security for Continuous Monitoring for Federal Information Systems and Organizations,* September 30, 2011;
- NIST Framework for Improving Critical I*nfrastructure Cybersecurity, V 1.1, April 16, 2018;*
- *Federal Acquisition Regulation (FAR); FAR Case 2007-004, Common Security Configurations;*
- *Department of Homeland Security Binding Operational Directive 23-01, Improving Asset Visibility and Vulnerability Detection on Federal Networks,* October 03, 2022;
- *OMB Memorandum M-25-04, Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements,* January 15, 2025*;*
- *OMB Memorandum 24-15, Modernizing the Federal Risk and Authorization Management Program,* July 25, 2024*;*
- *OMB Memorandum 23-16, Update to OMB 22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, September 14, 2022,* June 9, 2023*;*
- *OMB Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,* January 26, 2022*;*
- *OMB Memorandum M-22-01, Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response,* October 8, 2021*;*
- *OMB Memorandum M-21-30, Protecting Critical Software through Enhanced Security Measures,* August 10, 2021*; and*
- *OMB Memorandum M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incident, August 27, 2021.*

Appendix II – Response to 2025 CyberScope Questionnaire

Inspector General Section Report	2025 FISMA Annual IG

Council of the Inspectors General on Integrity and Efficiency

Function 0: Overall

0.1 Please provide an overall IG self-assessment rating (Effective/Not Effective)

Effective

0.2 Please provide an overall assessment of the agency's information security program. The narrative should include a description of the assessment scope, a summary on why the information security program was deemed effective/ineffective and any recommendations on next steps. Please note that OMB will include this information in the publicly available Annual FISMA Report to Congress to provide additional context for the Inspector General's effectiveness rating of the agency's information security program. OMB may modify the response to conform with the grammatical and narrative structure of the Annual Report.

The CIGIE contracted with an independent auditor to determine the degree of compliance for CIGIE's information security programs and practices with FISMA requirements, DHS reporting requirements, and applicable OMB and NIST guidance. This audit assessed the maturity of CIGIE's information security program using the FY 2025 FISMA Reporting Metrics, and was performed with CIGIE oversight. In FY 2025, the independent auditor reviewed the CIGIE's GSS and determined the majority of cybersecurity framework functions were rated Managed and Measurable (Level 4), which is how OMB, DHS, and CIGIE define an effective program. As a result, the CIGIE information security program was defined as effective. Detailed audit results are available in the CIGIE OIG audit report of CIGIE's FY 2025 compliance with FISMA.

Function 1A: Govern - Cybersecurity Governance

1 **FY25 Supplemental.** To what extent does the organization develop and maintain cybersecurity profiles that are used to understand, tailor, assess, prioritize and communicate its cybersecurity objectives?
[CG.01]

Optimized (Level 5)

2 **FY25 Supplemental.** To what extent does the organization use a cybersecurity risk management strategy to support operational risk decisions?
[CG.02]

Managed and Measurable (Level 4)

3 **FY25 Supplemental.** To what extent do cybersecurity roles, responsibilities, and authorities foster accountability, performance assessment, and continuous improvement?
[CG.03]

Managed and Measurable (Level 4)

4.1 Please provide the assessed maturity level for the agency's Govern - Cybersecurity Governance program.

Managed and Measurable (Level 4)

4.2 Provide any additional information on the effectiveness (positive or negative) of the organization's cybersecurity governance program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the cybersecurity governance program effective?
[CG.SUM]

The CIGIE has achieved the rating of Managed and Measurable (Level 4) for its Govern metrics evaluation. The controls are effective.

Function 1B: Govern - Cybersecurity Supply Chain Risk Management (C-SCRM)

5 **FY25 Core.** 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?
[C-SCRM.01]

Managed and Measurable (Level 4)

6.1 Please provide the assessed maturity level for the agency's Govern - Cybersecurity Supply Chain Risk Management (C-SCRM) program.
[GV.SUM]

Managed and Measurable (Level 4)

6.2 Please provide the assessed maturity level for the agency's Govern program.

Managed and Measurable (Level 4)

6.3 Provide any additional information on the effectiveness (positive or negative) of the organization's supply chain risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the supply chain risk management program effective?
[C-SCRM.SUM]

The CIGIE has achieved the rating of Managed and Measurable (Level 4) for its Cybersecurity Supply Chain Risk Management metrics evaluation. The controls are effective.

Function 2: Identify - Risk and Asset Management (RAM)

7 **FY25 Core.** 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?
[RAM.01]

Optimized (Level 5)

8 **FY25 Core.** 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?
[RAM.02]

Managed and Measurable (Level 4)

9 **FY25 Core.** 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?
[RAM.03]

Optimized (Level 5)

10 **FY25 Supplemental.** 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?
[RAM.04]

Optimized (Level 5)

11 **FY25 Core.** To what extent does the organization ensure that information system security risks are adequately managed?
[RAM.05]

Managed and Measurable (Level 4)

12 **FY25 Core.** To what extent does the organization use technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?
[RAM.06]

Managed and Measurable (Level 4)

13.1 Please provide the assessed maturity level for the agency's Identify program.

Managed and Measurable (Level 4)

13.2 Provide any additional information on the effectiveness (positive or negative) of the organization's RAM program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the RAM program effective?
[RAM.SUM]

The CIGIE has achieved the rating of Managed and Measurable (Level 4) for its Risk Management metrics evaluation. The controls are effective.

Function 3A: Protect - Configuration Management

14 **FY25 Core.** To what extent does the organization use configuration settings/common secure configurations for its information systems?
[CM.01]

Managed and Measurable (Level 4)

15 **FY25 Core.** 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?
[CM.02]

Optimized (Level 5)

16.1 Please provide the assessed maturity level for the agency's Protect - Configuration Management program.

Managed and Measurable (Level 4)

16.2 Provide any additional information (positive or negative) of the organization's configuration management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?
[CM.SUM]

The CIGIE has achieved the rating of Managed and Measurable (Level 4) for its Configuration Management metrics evaluation. The control is effective.

Function 3B: Protect - Identity and Access Management (IDAM)

17 **FY25 Core.** 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?
[IDAM-01]

Managed and Measurable (Level 4)

18 **FY25 Core.** 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?
[IDAM-02]

Managed and Measurable (Level 4)

19 **FY25 Core.** 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?
[IDAM-03]

Managed and Measurable (Level 4)

20.1 Please provide the assessed maturity level for the agency's Protect - Identity and Access Management (IDAM) program.

Managed and Measurable (Level 4)

20.2 Provide any additional information (positive or negative) of the organization's IDAM program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the IDAM program effective?
[IDAM.SUM]

The CIGIE has achieved the rating of Managed and Measurable (Level 4) for its Identity and Access Management metrics evaluation. The control is effective.

Function 3C: Protect - Data Protection and Privacy

21 **FY25 Core.** 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?
• 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.
[DPP.01]

Managed and Measurable (Level 4)

22 **FY25 Core.** 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?
[DPP.02]

Optimized (Level 5)

23.1 Please provide the assessed maturity level for the agency's Protect - Data Protection and Privacy program.

Managed and Measurable (Level 4)

23.2 Provide any additional information (positive or negative) of the organization's data protection and privacy program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the data protection and privacy program effective?
[DPP.SUM]

The CIGIE has achieved the rating of Managed and Measurable (Level 4) for its Data Protection & Privacy metrics evaluation. The control is effective.

Function 3D: Protect - Security Training

24 **FY25 Core.** 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? [ST.01]?

Optimized (Level 5)

25.1 Please provide the assessed maturity level for the agency's Protect - Security Training program.

Optimized (Level 5)

25.2 Please provide the assessed maturity level for the agency's Protect program.

Optimized (Level 5)

25.3 Provide any additional information (positive or negative) of the organization's security training program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the security training program effective? [ST.SUM]

The CIGIE has achieved the rating of Optimized (Level 5) for its Security Training metrics evaluation. The control is effective.

Function 4: Detect - Information Security Continuous Monitoring (ISCM)

26 **FY25 Core.** 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?
[ISCM.01]

Managed and Measurable (Level 4)

27 **FY25 Supplemental.** To what extent does the organization monitor and measure the integrity and security posture of all owned and associated assets?
[ISCM.02]

Managed and Measurable (Level 4)

28 **FY25 Core.** To what extent does the organization performing ongoing (continuous monitoring) information system assessments to grant system authorizations, including developing and maintaining system security plans, and monitoring system security controls?
[ISCM.03]

Optimized (Level 5)

29.1 Please provide the assessed maturity level for the agency's Detect program.

Managed and Measurable (Level 4)

29.2 Provide any additional information (positive or negative) of the organization's ISCM program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the ISCM program effective? [ISCM.SUM]

The CIGIE has achieved the rating of Managed and Measurable (Level 4) for its Information Security Continuous Monitoring metrics evaluation. The controls are effective.

Function 5: Respond - Incident Response

30 **FY25 Core.** To what extent has the organization implemented processes related to incident detection and analysis?
[IR.01]

Optimized (Level 5)

31 **FY25 Core.** To what extent has the organization implemented processes related to incident handling?
[IR.02]

Optimized (Level 5)

32.1 Please provide the assessed maturity level for the agency's Respond program.

Optimized (Level 5)

32.2 Provide any additional information (positive or negative) of the organization's incident response program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the incident response program effective?
[IR.SUM]

The CIGIE has achieved the rating of Managed and Measurable (Level 4) for its Incident Response metrics evaluation. The controls are effective.

Function 6: Recover - Contingency Planning

33 **FY25 Core.** To what extent does the organization ensure that the results of BIAs are used to guide contingency planning efforts?
[CP.01]

Optimized (Level 5)

34 **FY25 Core.** To what extent does the organization perform tests/exercises of its information system contingency planning processes?
[CP.02]

Managed and Measurable (Level 4)

***Comments*:** Auditor's Comment: The next level is not met because CIGIE OCIO did not employ automated mechanisms to test its system contingency plan and did not coordinate its plan testing with external stakeholders.

35.1 Please provide the assessed maturity level for the agency's Recover program.

Managed and Measurable (Level 4)

35.2 Provide any additional information (positive or negative) of the organization's contingency planning program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the contingency planning program effective?
[CP.SUM]

The CIGIE has achieved the rating of Managed and Measurable (Level 4) for its Contingency Planning metrics evaluation. The controls are effective.

APPENDIX A: Maturity Model Scoring

A.1 Please provide the assessed maturity level for the agency's Overall status.

Function	FY25 Core	FY25 Supplemental	FY25 Weighted Average	FY25 Assessed Maturity	FY25 Effectiveness	Explanation
Govern	4	4.33	4.29	Managed and Measurable (Level 4)	Effective	
Identify	4.4	5	4.6	Managed and Measurable (Level 4)	Effective	
Protect	4.38		4.38	Optimized (Level 5)	Effective	
Detect	4.5	4	4.5	Managed and Measurable (Level 4)	Effective	
Respond	5		5	Optimized (Level 5)	Effective	
Recover	4.5		4.67	Managed and Measurable (Level 4)	Effective	
Overall Maturity	**4.46**	**4.44**	**4.57**	**Managed and Measurable (Level 4)**	**Effective**	

Appendix III – Status of Prior Year Audit Recommendations

The following table provides the status of the FY 2024 open audit recommendations. Sixteen recommendations from the prior year were fully implemented.

No.	Cyber Security Framework Section	FY 2024 Audit Recommendations[4]	Status
1	Risk Management	**FY 2024 FISMA audit recommendation No. 1:** We recommend the CIGIE OCIO implement a governance, risk, and compliance solution to manage and monitor cybersecurity risk activities required by NIST SP 800-39 and to provide a centralized enterprise-wide view of all risks across the Agency.	Closed
2	Risk Management	**FY 2024 FISMA Audit Recommendation No. 2:** We recommend the CIGIE OCIO develop and implement a supply risk chain management strategy that aligns with NIST SP 800-53, Rev. 5.1, PM-30 *Supply Chain Risk Management Strategy* as required by OMB.	Closed
3	Risk Management	**FY 2024 FISMA audit recommendation No. 3:** We recommend the CIGIE OCIO develop and implement comprehensive anti-counterfeit policies and procedures and provide appropriate training for personnel.	Closed
4	Configuration Management	**FY 2024 FISMA audit recommendation No. 4:** We recommended CIGIE OICO remediate vulnerabilities in its information systems in a timely manner as required by the agency's policy.	Closed
5	Configuration Management	**FY 2024 FISMA audit recommendation No. 5:** We recommend the CIGIE OCIO scan all information products to assess configuration settings, resolve unsecured configuration and provide appropriate training for personnel.	Closed
6	Access Management	**FY 2024 FISMA audit recommendation No. 6:** We recommend the CIGIE OCIO ensures physical and environmental protection access controls are in place and regularly monitored.	Closed
7	Access Management	**FY 2024 FISMA audit recommendation No. 7:** We recommend the CIGIE OCIO implement controls to mitigate the risks associated with inadequate temperature and high humidity to protect the agency's information systems and ensure continuous and efficient operations.	Closed
8	Access Management	**FY 2024 FISMA audit recommendation No. 8:** We recommend the CIGIE OCIO ensure that all visitors' access to the facility and network area is recorded, including entry and exit times, purpose of visit, and areas accessed.	Closed
9	Security Training	**FY 2024 FISMA audit recommendation No. 9:** We recommended that CIGIE OCIO ensure security awareness	Closed

[4] CIGIE, FISMA Act of 2014, Fiscal Year 2024 Audit, (October 28, 2024).

No.	Cyber Security Framework Section	FY 2024 Audit Recommendations[4]	Status
		and privacy training is provided to all system users as required by the agency's policy, and track performance.	
10	Security Training	**FY 2024 FISMA audit recommendation No. 10:** We recommend the CIGIE OCIO develop a cybersecurity workforce assessment plan that aligns with the NIST SP 800-181 Rev. 1, *Workforce Framework for Cybersecurity (National Initiative for Cybersecurity Education Framework).*	Closed
11	Security Training	**FY 2024 FISMA audit recommendation No. 11:** We recommend the CIGIE OCIO conduct a cybersecurity workforce assessment of its workforce's knowledge, skills, and abilities to identify any skill gaps and specialized training needs.	Closed
12	Information System Continuous Monitoring	**FY 2024 FISMA audit recommendation No. 12:** We recommend the CIGIE OCIO update its System Security Plan, policies, and procedures to align with the NIST control families, specifically focusing on Program Management, Supply Chain Risk Management, and privacy-related controls for Personally Identifiable Information Processing and Transparency.	Closed
13	Information System Continuous Monitoring	**FY 2024 FISMA audit recommendation No. 13:** We recommend the CIGIE OCIO monitor its Information Security Continuous Monitoring (ISCM) program and document lessons learned to make improvements to the ISCM policies and strategy.	Closed
14	Response	**FY 2024 FISMA audit recommendation No. 14:** We recommend the CIGIE OCIO implement logging requirements as required by OMB M-21-31.	Closed
15	Contingency Planning	**FY 2024 FISMA audit recommendation No. 15:** We recommend the CIGIE OCIO develop an organizational-level and system-level Business Impact Analyses (BIA) that aligns with the applicable NIST controls and updates its contingency plan.	Closed
16	Contingency Planning	**FY 2024 FISMA audit recommendation No. 16:** We recommend the CIGIE OCIO review and approve its contingency plan ensuring the results of the BIAs are consistently used to determine contingency planning requirements and priorities, including mission essential functions and high-value assets.	Closed

Appendix IV - Acronyms

Acronyms	
CIGIE	Council of the Inspector General on Integrity and Efficiency
C-SCRM	Cybersecurity Supply Chain Risk Management
FAR	Federal Acquisition Regulation
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
IG	Inspector General
ISCM	Information Security Continuous Monitoring
NIST	National Institute of Standards and Technology
OCIO	Office of Chief Information Officer
OMB	U.S. Office of Management and Budget
REV	Revision
SCRM	Supply Chain Risk Management
SP	Special Publication

Appendix V – Management's Comments

COUNCIL OF THE INSPECTORS GENERAL
ON INTEGRITY AND EFFICIENCY

DATE: August 18, 2025

TO: Gail Jenifer, Member, Brown & Company

FROM: Andrew Cannarsa, Executive Director

SUBJECT: Independent Auditor's Performance Audit Report on the Council of the Inspectors General on Integrity and Efficiency's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2025

This memorandum provides the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) management response to the Fiscal Year 2025 audit of CIGIE's compliance with the Federal Information Security Modernization Act (FISMA). We appreciate the thorough and professional assessment conducted by Brown & Company, and we are pleased to acknowledge the results of your audit.

The FY 2025 audit concluded that CIGIE's information security program is effective, with maturity ratings of "Managed and Measurable" (Level 4) and "Optimized" (Level 5) across all cybersecurity framework functions. These results reflect the continued commitment of the Office of the Chief Information Officer (OCIO) to maintaining a robust, risk-based cybersecurity program aligned with federal standards and best practices.

We are especially proud that this year's audit resulted in no findings or recommendations. This outcome is a testament to the dedication of our cybersecurity and IT teams, and to the collaborative nature of your audit process. It also reflects the maturity of our security posture and the effectiveness of our ongoing efforts to strengthen the confidentiality, integrity, and availability of CIGIE's systems and data.

CIGIE remains committed to continuous improvement and to maintaining the highest standards of cybersecurity. We thank you again for your time, diligence, and partnership throughout this engagement.

Sincerely,

ANDREW CANNARSA
Digitally signed by ANDREW CANNARSA
Date: 2025.08.18 09:54:08 -04'00'

Andrew M. Cannarsa
Executive Director
Council of the Inspectors General on Integrity and Efficiency
1750 H Street NW, Suite 400
Washington, DC 20006
andrew.cannarsa@cigie.gov