Independent Audit of the Council of the Inspector General Compliance with the Federal Information Security Modernization Act of 2014

COUNCIL OF THE INSPECTORS GENERAL
ON INTEGRITY AND EFFICIENCY

Fiscal Year 2024

For the Period Ending
September 30, 2024

Prepared by

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

October 28, 2024

BROWN & COMPANY
CERTIFIED PUBLIC ACCOUNTANTS AND MANAGEMENT CONSULTANTS, PLLC

October 28, 2024

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 Inspectors General on Integrity and Efficiency's (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 information and information system security controls (herein referred to as information security program). We conducted our performance audit during the period from January 18, 2024, through September 30, 2024.

On December 4, 2023, the Office of Management and Budget (OMB) issued Memorandum M-24-04 *Memorandum for the Heads of Executive Departments and Agencies: Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements* to provide instructions for meeting the Fiscal Year (FY) 2024 FISMA reporting requirements.

To achieve this objective, we reviewed the FY 2023-2024 Inspector General FISMA reporting metrics and performance measures selected by OMB and conducted this performance audit in accordance with Generally Accepted Government Auditing Standards, which requires that we obtain sufficient, appropriate evidence to provide a reasonable basis for our conditions and conclusions. We believe that the evidence obtained throughout the FY 2024 audit provides a reasonable basis for our conclusions and maturity ratings.

Based on the results of the audit procedures performed for the FY 2024 audit period, Brown & Company concluded that the CIGIE has not met the requirements to be operating at an effective level of security outlined within the FY 2024 FISMA reporting metrics for the subset of information system evaluated. We are reporting seven findings and making sixteen recommendations to assist CIGIE in strengthening its information security program. The details supporting our overall conclusion are found in the attached report.

Additionally, we have included CIGIE's Management Response in Appendix III for your reference. Please note that Brown & Company has not audited the statements included in the Management Response. We appreciate your cooperation and support during this audit. If you have any questions, please contact Gail Jenifer at gjenifer@brownco-cpas.com (240) 770-4903.

6401 GOLDEN TRIANGLE DRIVE, SUITE 310 • GREENBELT, MD 20770
PHONE: (240) 770-4900 • FAX: (301) 773-2090 • mail@brownco-cpas.com • www.brownco-cpas.com

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

Sincerely,

Brown & Company CPAs and
Management Consultants, PLLC

Gail Jenifer, CPA, CISA, CISM, CRISC, CGFM, CDPSE

Member

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 Inspectors General on Integrity and Efficiency (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 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 information security program. This performance audit's objective was to determine whether CIGIE implemented certain security controls for selected information systems in support of FISMA.

Our audit was performed in accordance with generally accepted 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 objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

For this audit, we reviewed selected controls from CIGIE's general support system.

---

[1] The Federal Information Security Modernization Act of 2014 (Public Law 113–283— December 18, 2014) amends the Federal Information Security Management 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.

Results

According to OMB Fiscal Year (FY) 2023-2024 Inspector General (IG) FISMA Reporting Metrics, a security program is considered effective if the calculated average of the FY 2024 IG FISMA Reporting Metrics is at least Managed and Measurable (Level 4) across the five domains: Identify, Protect, Detect, Respond and Recover. Based on OMB's guidance and CyberScope results, we found that the calculated average of the Cybersecurity Function was assessed as Consistently Implemented (Level 3), and therefore not effective.

We found CIGIE 's selected controls not effective or operating as intended. We are reporting seven findings and making 16 recommendations to assist CIGIE in strengthening its information security program. Specifically, CIGIE needs to improve its:

1. Risk Management Program
2. Configuration Management Program
3. Identity and Access Management Program
4. Security Training Program
5. Information System Continuous Monitoring (ISCM) Program
6. Incident Response Program
7. Contingency Planning Program

Detailed findings and recommendations appear in the following sections.

Audit Results

Brown & Company assessed the effectiveness of CIGIE's information security program and practices using a maturity model. The foundational levels (Levels 1-2) ensure that policies and procedures are designed to support the requirements outlined within the FISMA, while the advanced levels (Levels 3-5) focus on the implementation and operating effectiveness of the defined policies and procedures.

We concluded the CIGIE Office of the Chief Information Officer's (OCIO) information system program received an overall Level 3 – Consistently Implemented maturity level, therefore the CIGIE OCIO information security program is not effective. To be considered effective, CIGIE OCIO's information security program must be rated Managed and Measurable (Level 4).

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 (managed and measurable) 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 2024 Inspector General FISMA Reporting Metrics. Four out of five functions met consistently implemented, and one at defined.

Table-2 Summary of Overall Calculated Average Maturity Levels

Function and Domain Areas	FY 2024 Core and Supplemental FISMA Maturity Levels Rating
Identify: Risk Management and Supply Chain Risk Management	Consistently Implemented (Level 3)
Protect: Configuration Management, Identity and Access Management, Data Protection & Privacy, and Security Training	Consistently Implemented (Level 3)
Detect: Information Security Continuous Monitoring	Defined (Level 2)
Respond: Incident Response	Consistently Implemented (Level 3)
Recover: Contingency Planning	Consistently Implemented (Level 3)
Overall Effectiveness Rating – Not Effective	**Consistently Implemented (Level 3)**

Audit Findings and Recommendations

1. CIGIE OCIO Needs to Improve Its Risk Management Program.

NIST Special Publication (SP) 800-39, M*anaging Information Security Risk, Organization, Mission, and Information System View*, states that effective risk management requires an agency's mission/business process to explicitly account for information security risk when making operational decisions and that cybersecurity risk information should be shared with key stakeholders throughout the organization. Also, NIST SP 800-39 recommends automating risk management requirements for efficiency, consistency, and effectiveness of a unified platform for managing governance, risk assessment, control implementation, incident response, continuous monitoring, and reporting.

Our review of CIGIE OCIO's implementation of NIST SP 800-39 and the agency's ability to provide and share cybersecurity risk information with key stakeholders revealed that CIGIE OCIO has partially implemented automated solutions for managing and monitoring cybersecurity risks. While automated tools are utilized, the current approach still heavily relies on manual methods, such as preparing and storing risk documents in a shared portal. The CIGIE OCIO did not prioritize the resources needed to implement an automated centralized enterprise risk solution. CIGIE OCIO's hybrid approach limits the ability to provide a centralized, enterprise-wide view of cybersecurity risks across the organization, increases administrative burden, and risks of human error.

OMB Circular A-130, *Managing Information as a Strategic Resource*, requires Agencies to implement supply chain risk management (SCRM) principles to protect against supply chain risks, such as the insertion of counterfeits, unauthorized production, tampering, the insertion of malicious software, as well as poor manufacturing and development practices throughout the system development life cycle. Also, NIST SP 800-53, Revision (Rev.) 5.1, PM-30 *Supply Chain Risk Management Strategy* control requires organizations to develop, implement, and maintain an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services.

We noted that the CIGIE OCIO did not develop and implement SCRM strategies, policies, and procedures to manage supply chain risks. Also, the agency has not conducted a supplier risk assessment. The CIGIE OCIO did not prioritize the resources needed to develop and implement SCRM strategies, policies, and procedures. Not developing and implementing an SCRM strategy increases the risk of bad actors exploring unknown vulnerabilities in CIGIE OCIO's supply chain and, thus, compromises the confidentiality, integrity, or availability of the agency's systems and the information contained in the systems.

NIST SP 800-53, Rev. 5.1, SR-11(1) *Component Authenticity* | *Component Authenticity* | *Anti-Counterfeit Training* control requires organizations to train personnel to detect counterfeit system components (including hardware, software, and firmware).

We noted the CIGIE OCIO has not developed and implemented anti-counterfeit policies and procedures that include the means to detect and prevent counterfeit components from entering the system. Also, the CIGIE OCIO has not provided training for personnel to detect counterfeit system components (including hardware, software, and firmware). The CIGIE OCIO lacks controls for implementing anti-counterfeit policies and procedures. Not developing and implementing anti-counterfeit policies and procedures increases the risk of bad actors exploring unknown vulnerabilities in CIGIE's supply chain and, thus, compromises the confidentiality, integrity, or availability of the agency's systems and the information contained in the systems.

Recommendation 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.

Recommendation 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.

Recommendation 3:
We recommend the CIGIE OCIO develop and implement comprehensive anti-counterfeit policies and procedures and provide appropriate training for personnel.

2. CIGIE OCIO Needs to Improve Its Configuration Management Program.

NIST SP 800-53, Rev. 5.1, SI-2 *Flaw Remediation* control requires organizations to identify, report, and correct system flaws in its information systems. Also, the control requirements include installing security-relevant software and firmware updates within the organization's defined time period of the release of the updates.

On May 1, 2024, we conducted a vulnerability scan on CIGIE's network for 11 selected IP addresses and confirmed 49 unique vulnerabilities: 3 "Critical," 4 "High," and 42 "Medium" risk vulnerabilities related to patch and configuration management. The 49 vulnerabilities were not resolved within the agency's policies and procedure timeframes that require the remediation of critical vulnerabilities within 7 days and high vulnerabilities within 30 days. Also, the CIGIE OCIO vulnerability reports, dated October 28, 2023, through December 28, 2024, identified one high-level vulnerability relating to an SSL certificate that was not remediated within 30 days.

The CIGIE OCIO runs vulnerability scans; however, flaw remediation controls were not consistently implemented to remediate known vulnerabilities due to a lack of a remediation plan. Unmitigated vulnerabilities on the agency's network can compromise the confidentiality, integrity, and availability of the data.

NIST SP 800-53, Rev. 5.1, CM-6 *Configuration Settings* control requires organizations to Implement, document, and monitor configuration settings for information technology products employed within the agency's information systems using the most restrictive mode consistent with operational requirements. Also, NIST SP 800-53, Rev. 5.1, (CM-6(1) *Automated Management, Application, and Verification* control requires organizations to manage, apply, and verify configuration settings for system components using automated mechanisms.

Our review of *CIGIE OCIO's Windows 10* Defense Information Systems Agency *(DISA) Security Technical Implementation Guides (STIG) Scan Security Content Automation Protocol (SCAP) Report,* dated August 12, 2024, revealed secure configuration settings were not monitored to ensure settings reflected the most restrictive mode consistent with the agency's requirements for Windows devices. Specifically, the report revealed 37 secure compliance controls failed to meet the agency's requirements. As of August 15, 2024, the CIGIE OCIO has not conducted SCAP assessments for all information technology products employed within the agency's information systems. Due to the lack of training, the staff did not conduct and provide SCAP assessments for management review. The lack of production of SCAP assessment reports limits management's ability to track, audit, and verify that systems are securely configured according to the agency's policies and procedures.

Recommendation 4:
We recommend the CIGIE OCIO remediate vulnerabilities in its information systems in a timely manner as required by the agency's policy.

Recommendation 5:
We recommend the CIGIE OCIO scan all information products to assess configuration settings, resolve unsecured configuration and provide appropriate training for personnel.

3. CIGIE OCIO Needs to Improve Its Identity and Access Management Program.

NIST SP 800-53, Rev. 5.1, PE-3 *Physical Access Control* requires organizations to enforce physical access authorizations to the information system in addition to the physical access controls at entry and exit points to the facility where the information systems reside. Also, NIST SP 800-53, Rev. 5.1, PE-3 *Physical Access Control* requires organizations to maintain and monitor visitor access records, including, for example, names and organizations of people visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names and organizations of persons visited.

The CIGIE OCIO has not allocated sufficient resources to ensure the implementation of physical and environmental protection controls at the agency's facility in Georgia. Management indicated that due to the agency's plans to relocate the staff from the Georgia facility, funding for these controls was not prioritized. The lack of sufficient resources allocated to physical and environmental protection controls increases the risk of unauthorized access, equipment damage, and potential data breaches. This can compromise the confidentiality, integrity, and availability of the agency's systems and information.

Recommendation 6:
We recommend the CIGIE OCIO ensures physical and environmental protection access controls are in place and regularly monitored.

Recommendation 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.

Recommendation 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.

4. CIGIE OCIO Needs to Improve Its Security Training Program.

NIST SP 800-53, Rev. 5.1, AT-2 *Literacy Training and Awareness* control requires organizations to provide security and privacy literacy training to system users (including managers, senior executives, and contractors). Also, NIST SP 800-53, Rev. 5.1, AT-3: *Role-based Training* control requires organizations to provide role-based security and privacy training based on the assigned roles and responsibilities of individuals as well as the security and privacy requirements of organizations and the systems to which personnel have authorized access, including technical training specifically tailored for assigned duties.

Our review of CIGIE OCIO's security training records revealed security training was not provided to all system users, and management did not obtain feedback on its training program and maintain performance measurements. We noted 1 out of 89 employees did not receive security awareness training in FY 24. The CIGIE OCIO did not prioritize resources to ensure security and privacy training was provided to all system users and performance metrics were maintained. The agency cannot protect confidentiality, integrity, and availability of information without providing adequate security training to all system users. The lack of security training increases the risk of security breaches and limits personnel's ability to handle their security and privacy responsibilities effectively. Also, it is difficult for management to measure the success of its security training programs if performance measurements are not maintained.

The Federal Cybersecurity Workforce Assessment Act requires federal agencies to take several actions related to cybersecurity workforce planning. That includes categorizing all IT, cybersecurity, and cyber-related positions using OPM personnel codes for specific work roles and identifying critical staffing needs. The NIST SP 800-181 Rev. 1, *Workforce Framework for Cybersecurity (*National Initiative for Cybersecurity Education *(NICE) Framework)* provides a set of building blocks for describing the Tasks, Knowledge, and Skills that are needed to perform cybersecurity work by individuals or teams.

Our review of CIGIE OCIO's information security policies and procedures revealed that CIGIE OCIO has not developed a cybersecurity workforce assessment plan nor conducted a cybersecurity workforce assessment to evaluate the knowledge, skills, and abilities of the agency's cybersecurity workforce.

The CIGIE OCIO did not prioritize resources to ensure the agency developed and conducted a cybersecurity workforce assessment. Without a cybersecurity workforce assessment, the CIGIE OCIO cannot effectively identify gaps in the knowledge, skills, and abilities of its cybersecurity personnel. This can lead to inadequate protection against cyber threats, reduced effectiveness in incident response, and potential non-compliance with regulatory requirements.

Recommendation 9:
We recommend that the CIGIE OCIO ensure security awareness and privacy training are provided to all system users as required by the agency's policy and that performance is tracked.

Recommendation 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 (NICE Framework).*

Recommendation 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.

5. CIGIE OCIO Needs to Improve its ISCM Program.

ISCM refers to the process of maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. FISMA emphasizes the importance of continuously monitoring information system security by requiring agencies to conduct assessments of security controls at a risk-based frequency. Best practices for implementing ISCM are outlined in NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* (SP 800-137).

The CIGIE OCIO has established an ISCM process for its information systems and defined the minimum frequency at which selected security controls or metrics are to be assessed or monitored. However, the CIGIE OCIO does not consistently monitor the established metrics, leading to unresolved issues. Additionally, the CIGIE OCIO does not adequately document lessons learned to improve its ISCM policies and strategy.

The CIGIE OCIO has not prioritized resources to monitor its ISCM metrics and document lessons learned. Failure to consistently document lessons learned and fully implement security controls can lead to significant risks, including increased vulnerability to cyber threats, non-compliance with regulatory standards, an ineffective security strategy, and potential service interruptions.

The NIST SP 800-53, Rev. 5.1, CA-7 *Continuous Monitoring* control requires organizations to develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes the establishment of system-level and organizational-level metrics to be monitored.

NIST SP 800-53, Revision 5.1, PL-2 *System Security and Privacy Plans* control requires organizations to review its system security and privacy plans according to the agency's defined frequency and update plans to address changes.

Our review of CIGIE OCIO's General Support System (GSS) system security plan (SSP), last updated on June 1, 2023, revealed that it does not align with the security control recommendations for moderate-level systems specified in NIST SP 800-53, Rev. 5.1. Specifically, the document lacks alignment with the new control families for Program Management and Supply Chain Risk Management, as well as the privacy family for Personally Identifiable Information Processing and Transparency. The CIGIE OCIO management stated they did not have sufficient resources needed to update the agency's SSP to align with new NIST requirements. The lack of an updated SSP increases the risk of not implementing safeguarding measures and privacy controls to protect the agency's operations, assets, and the privacy of individuals.

Recommendation 12:
We recommend the CIGIE OCIO update its SSP, 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.

Recommendation 13:
We recommend the CIGIE OCIO monitor its ISCM program and document lessons learned to make improvements to the ISCM policies and strategy.

6. CIGIE OCIO Needs to Improve Its Incident Response Program.

The OMB issued Memorandum 21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*,1 on August 27, 2021, in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*. The memorandum established federal agency requirements to increase the government's visibility before, during, and after a cybersecurity incident. The memorandum describes a maturity model for four event logging (EL) tires agencies must capture as well as any required retention times. The tier levels are EL0-Not Effective, EL1- Basic, EL2-Intermediate, and EL3-Advanced.

CIGIE stated the agency meets tier level EL1-Basic and is in the process of implementing logging requirements for EL2-Intermediate and EL3-Advanced. Also, we reviewed the CIGIE OCIO's project report and noted the agency reported meeting EL1-Basic logging requirements and completion for EL2-Intermediate was 40%, and EL3-Advanced was 33%.

The CIGIE OCIO has not prioritized resources to ensure network logging requirements for EL2-Intermediate and EL3-Advanced. The effect of not capturing logging data at required maturity levels hinders the agency's ability to analyze cybersecurity incidents before, during, and after their occurrence.

Recommendation 14:
We recommend the CIGIE OCIO implement logging requirements as required by OMB M-21-31.

7. CIGIE OCIO Needs to Improve its Contingency Planning.

The NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*, provides instructions, recommendations, and considerations to assist federal organizations in developing and maintaining effective contingency plans. The document provides guidance to help agencies evaluate information systems and operations to determine contingency planning requirements and priorities. The system-level business impact analyses' (BIA) should be integrated with the organizational-level BIA and include characterization of all system components, determination of missions and business processes and recovery criticality, identification of resource requirements, and identification of recovery priorities for system resources. Also, the results of the BIAs should determine contingency planning requirements and priorities, including mission essential functions and high value assets.

NIST SP 800-53, Rev. 5.1, CP-2: *Security and Privacy Controls for Information Systems and Organizations: Contingency Plan* control requires organizations to update, review, and approve its agency contingency plan.

Our review of CIGIE OCIO's system-level GSS BIA revealed the document does not align with NIST requirements. Specifically, the document does not identify all system components and how the agency's mission and business processes are dependent on these system components. System components are discrete, identifiable assets (i.e., hardware, software, and firmware elements) that compose a system. Also, the document does not include recovery criticality, identification of resource requirements, and identification of recovery priorities for system resources. Also, the CIGIE OCIO contingency plan was not finalized and approved by management.

CIGIE lacks internal controls for monitoring its security program to ensure that business impact analyses are conducted and contingency plans are maintained in alignment with established policies and procedures. Without regularly developed and updated business impact analyses, the agency cannot fully understand the criticality of its operations and the potential impact of disruptions. This can result in inadequate or misaligned contingency plans, leaving the organization vulnerable to unplanned downtime and data loss.

Recommendation 15:

We recommend the CIGIE OCIO develop an organizational-level and system-level BIA that aligns with the applicable NIST controls and updates its contingency plan.

Recommendation 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.

Brown & Company

Greenbelt, Maryland
October 28, 2024

Appendix I – Scope, Methodology and Criteria

Scope

We conducted this audit in accordance with generally accepted government auditing standards, 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 the CIGIE OCIO implemented selected security controls for certain information systems in support of the FISMA Act of 2014. The audit scope period was from January 18, 2024, through September 30, 2024.

Our overall objective was to evaluate CIGIE OCIO's security program and practices, as required by FISMA. Specifically, we reviewed 20 Core and 17 Supplemental IG FISMA Reporting Metrics in five security function areas — Identify, Protect, Detect, Respond, and Recover — to determine the effectiveness of the agencies' information security program and the maturity level of each function area. The maturity levels range from lowest to highest — Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized:

Function (Domains)

- Identify (Risk Management)
- Identify (Supply Chain 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)

We also performed audit procedures on CIGIE OCIO's internal and external systems. The audit also included a review of vulnerability assessments of CIGIE OCIO's managed internal systems and an evaluation of CIGIE OCIO's process for identifying and mitigating technical vulnerabilities.

Methodology

We reviewed the 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

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

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; 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 was no significant internal control weaknesses identified that affected the audit objective.

The audit was conducted at Brown & Company in Greenbelt, Maryland, CIGIE's headquarters in Washington, DC, and one facility in Brunswick, Georgia, from January 18, 2024, to September 30, 2024.

Criteria

The criteria used in conducting this audit included:

- NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments*;
- NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*;
- NIST SP 800-37, Rev. 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 800-50, *Building an Information Technology Security Awareness and Training Program;*
- NIST SP 800-53, Rev. 5.1, *Security and Privacy Controls for Information Systems and Organizations, September* 2020; updated as of December 10, 2020;
- NIST SP 800-61*, Rev. 1, Computer Security Incident Handling Guide;*
- NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information;*
- NIST SP 800-128*, Guide for Security-Focused Configuration Management of Information Systems;*
- NIST SP 800-137*, Information Security for Continuous Monitoring for Federal Information Systems and Organizations;*
- *NIST Framework for Improving Critical Infrastructure Cybersecurity, V 1.1;*
- *Chief Financial Officers Council and the Performance Improvement Council release the Playbook: Enterprise Risk Management;*
- *Federal Acquisition Regulation (FAR); Case 2007-004, Common Security Configurations;*
- *DHS Binding Operational Directive 23-01, Improving Asset Visibility and Vulnerability Detection on Federal Networks;*
- *OMB Memorandum M-24-04, Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements, December 4, 2023;*
- *OMB Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, September 14, 2022;*
- *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 2024 CyberScope Questionnaire

No.	FY24-Core IG FISMA Metrics Evaluation Questions	Core Metric or FY	Maturity Level	Rating	FY24-Auditor's Comments
	1. Identify - Risk Management				
1. Identify (RM)	1. To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third-party systems), and system interconnections?	Core Metric	Level 5: Optimized	5	Met
1. Identify (RM)	2. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including GFE and Bring Your Own Device (BYOD) mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting?	Core Metric	Level 4: Managed and Measurable	4	Auditor's Comment: The next level is not met because the CIGIE OCIO has not employed automation to track the life cycle of the agency's hardware assets with processes that limit the manual/procedural methods for asset management.
1. Identify (RM)	3. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting?	Core Metric	Level 5: Optimized	5	Met

No.	FY24-Core IG FISMA Metrics Evaluation Questions	Core Metric or FY	Maturity Level	Rating	FY24-Auditor's Comments
1. Identify (RM)	4. To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets?	FY24	Level 4: Managed and Measurable	4	The next level is not met because the CIGIE OCIO does not utilize impact-level prioritization for additional granularity to support risk-based decision-making.
1. Identify (RM)	5. To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels?	Core Metric	Level 2: Defined	2	*Auditor's Comment: The next level is not met because the CIGIE OCIO has not consistently implemented its policies, procedures, and processes to manage the cybersecurity risks associated with operating and maintaining its information systems.*
1. Identify (RM)	6. To what extent does the organization use an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain?	FY24	Level 4: Managed and Measurable	4	*Auditor's Comment: The next level is not met because the CIGIE OCIO does not utilize advanced technologies and techniques for managing supply chain risks to quickly adapt its information security and enterprise architectures to mitigate supply chain risks.*

No.	FY24-Core IG FISMA Metrics Evaluation Questions	Core Metric or FY	Maturity Level	Rating	FY24-Auditor's Comments
1. Identify (RM)	10. 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?	Core Metric	Level 1: Ad Hoc	1	*Auditor's Comment: the CIGIE OCIO has not identified and defined its requirements for an automated solution to provide a centralized, enterprise-wide (portfolio) view of cybersecurity risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards.*
1. Identify (RM)	11. Provide any additional information on the effectiveness (positive or negative) of the organization's risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?	Summary Q		3	The CIGIE OCIO has achieved the rating of Consistently Implemented (Level 3) for its Risk Management metrics evaluation.
	2. Supply Chain Risk Management				
2. Identity (SCRM)	14. To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements?	Core Metric	Level 1: Ad Hoc	1	*Auditor's Comment: the CIGIE OCIO has not defined and communicated policies, procedures, and processes for supply chain risk management requirements.*

No.	FY24-Core IG FISMA Metrics Evaluation Questions	Core Metric or FY	Maturity Level	Rating	FY24-Auditor's Comments
2. Identity (SCRM)	15. To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization's systems?	FY24	Level 1: Ad Hoc	1	*Auditor's Comment: the CIGIE OCIO has not defined and communicated its component authenticity policies and procedures.*
2. Identity (SCRM)	16. Provide any additional information on the effectiveness (positive or negative) of the organization's supply chain risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the supply chain risk management program effective? 16.1 Please provide an IG self-assessment rating (Effective/Not Effective) for the agency's identify function.	Summary Q		2	The CIGIE has achieved the rating of Defined (Level 2) for its Supply Chain Risk Management metrics evaluation.
	3. Protect - Configuration Management				
3. Protect (CM)	17. To what extent have the roles and responsibilities of configuration management stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?	FY24	Level 5: Optimized	5	Met

No.	FY24-Core IG FISMA Metrics Evaluation Questions	Core Metric or FY	Maturity Level	Rating	FY24-Auditor's Comments
3. Protect (CM)	18. To what extent does the organization use an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems?	FY24	Level 5: Optimized	5	Met
3. Protect (CM)	20. To what extent does the organization use configuration settings/common secure configurations for its information systems?	Core Metric	Level 2: Defined	2	Auditor's Comment: The next level is not met because the CIGIE OCIO does not consistently implement, assess, and maintain secure configuration settings for its information systems based on the principle of least functionality. Also, the CIGIE OCIO does not consistently use SCAP-validated software assessing (scanning) capabilities against all systems on the network (in accordance with BOD 23-01see) to assess and manage both code-based and configuration-based vulnerabilities.

No.	FY24-Core IG FISMA Metrics Evaluation Questions	Core Metric or FY	Maturity Level	Rating	FY24-Auditor's Comments
3. Protect (CM)	21. 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?	Core Metric	Level 2: Defined	2	*Auditor's Comment: The next level is not met because the CIGIE OCIO does not consistently implement its flaw remediation policies, procedures, and processes and ensures that patches, hotfixes, service packs, and anti-virus/malware software updates are identified, prioritized, tested, and installed in a timely manner.*
3. Protect (CM)	23. To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, as appropriate?	FY24	Level 5: Optimized	5	*Met.*

No.	FY24-Core IG FISMA Metrics Evaluation Questions	Core Metric or FY	Maturity Level	Rating	FY24-Auditor's Comments
3. Protect (CM)	25. Provide any additional information on the effectiveness (positive or negative) of the organization's configuration management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?	Summary Q		3	The CIGIE has achieved the rating of Consistently Implemented (Level 3) for its Configuration Management metrics evaluation.
	4. Protect - Identify and Access Management				
4. Protect (IAM)	28. To what extent has the organization developed and implemented processes for assigning position risk designations and performing appropriate personnel screening prior to granting access to its systems?	FY24	Level 2: Defined	2	The CIGIE has achieved the rating of Consistently Implemented (Level 3) for its Configuration Management metrics evaluation.
4. Protect (IAM)	30. 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 facilities [organization-defined entry/exit points], networks, and systems, including for remote access?	Core Metric	Level 2: Defined	2	*Auditor's Comment: The next level is not met because the CIGIE OCIO has not consistently implemented strong authentication mechanisms for non-privileged users of the organization's facilities [organization-defined entry/exit points] and networks, including for remote access, in accordance with Federal targets.*

No.	FY24-Core IG FISMA Metrics Evaluation Questions	Core Metric or FY	Maturity Level	Rating	FY24-Auditor's Comments
4. Protect (IAM)	31. 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 facilities [organization-defined entry/exit points], networks, and systems, including for remote access?	Core Metric	Level 2: Defined	2	*Auditor's Comment: The next level is not met because the CIGIE OCIO has not consistently implemented strong authentication mechanisms for privileged users of the organization's facilities [organization-defined entry/exit points], and networks, including for remote access, in accordance with Federal targets.*
4. Protect (IAM)	32. To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed?	Core Metric	Level 4: Managed and Measurable	4	*Auditor's Comment: The next level is not met because the CIGIE OCIO has not implemented EL3's advanced requirements for user behavior monitoring to detect and alert privileged user compromises.*
4. Protect (IAM)	34. Provide any additional information on the effectiveness (positive or negative) of the organization's identity and access management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?	Summary Q		2	The CIGIE has achieved the rating of Defined (Level 2) for its Identity and Access Management metrics evaluation.

No.	FY24-Core IG FISMA Metrics Evaluation Questions	Core Metric or FY	Maturity Level	Rating	FY24-Auditor's Comments
	5. Protect- Data Protection & Privacy				
5. Protect (DPP)	36. To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle? • 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	Core Metric	Level 4: Managed and Measurable	4	*Auditor's Comment: The next level is not met because the CIGIE OCIO has not employed advanced capabilities to enhance protective controls such as media marking to protect PII and sensitive data, dual authorization for sanitization of media devices; and configuring systems to record the date the PII was collected, created, or updated and when the data is to be deleted or destroyed according to an approved data retention schedule.*
5. Protect (DPP)	37. To what extent has the organization implemented security controls (e.g., EDR) to prevent data exfiltration and enhance network defenses?	Core Metric	Level 5: Optimized	5	Met
5. Protect (DPP)	38. To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events?	FY24	Level 5: Optimized	5	Met

No.	FY24-Core IG FISMA Metrics Evaluation Questions	Core Metric or FY	Maturity Level	Rating	FY24-Auditor's Comments
5. Protect (DPP)	39. To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E- Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements)	FY24	Level 2: Defined	2	Auditor's Comment: The next level is not met because the CIGIE OCIO has not provided cybersecurity awareness and privacy training to all system users.
5. Protect (DPP)	40. Provide any additional information on the effectiveness (positive or negative) of the organization's data protection and privacy program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the data protection and privacy program effective?	Summary Q		4	The CIGIE OCIO has achieved the rating of Managed and Measurable (Level 4) for its Data Protection & Privacy metrics evaluation.
	6. Protect - Security Training				
6. Protect (ST)	42. To what extent does the organization use an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover?	Core Metric	Level 1: Ad Hoc	1	Auditor's Comment: The next level is not met because the CIGIE OCIO did not establish a security and privacy workforce development and improvement program. As a result, the Agency has not assessed its workforce's knowledge, skills, and abilities.

No.	FY24-Core IG FISMA Metrics Evaluation Questions	Core Metric or FY	Maturity Level	Rating	FY24-Auditor's Comments
6. Protect (ST)	44. To what extent does the organization ensure that security awareness training is provided to **all system users** and is tailored based on its mission, risk environment, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting?	FY24	Level 2: Defined	2	Auditor's Comment: The next level is not met because the CIGIE OCIO did not ensure all appropriate users completed the security awareness training within the agency's defined timeframes and did not maintain completion records. Also, the CIGIE OCIO did not obtain feedback on its security awareness training program, thus was not able to uses that information to make improvements.
6. Protect (ST)	45. To what extent does the organization ensure that **specialized security** training is provided to individuals with significant security responsibilities (as defined in the organization's security policies and procedures and in accordance with 5 Code of Federal Regulation 930.301)?	FY24	Level 3: Consistently Implemented	3	Auditor's Comment: The next level is not met because the CIGIE OCIO did not obtain feedback on its specialized security training and maintain performance measurements.
6. Protect (ST)	46. Provide any additional information on the effectiveness (positive or negative) of the organization’s security training program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the security training program effective? 46.1 Please provide an IG self-assessment rating (Effective/Not Effective) for the agency's protect function.	Summary Q		2	The CIGIE OCIO has achieved the rating of Defined (Level 2) for its Security Training metrics evaluation.

No.	FY24-Core IG FISMA Metrics Evaluation Questions	Core Metric or FY	Maturity Level	Rating	FY24-Auditor's Comments
	7. Detect - Information Security Continuous Monitoring				
7. Detect (ISCM)	47. 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?	Core Metric	Level 4: Managed and Measurable	4	Auditor's Comments: The next level is not met because the CIGIE OCIO ISCM policies and strategy are not consistently implemented at the organization, business process, and information system levels.
7. Detect (ISCM)	49. How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls?	Core Metric	Level 2: Defined	2	*Auditor's Comment: The next level is not met because the CIGIE OCIO did not update its System Security Plan (SSP) to align with NIST SP-800 53, revision 5.1.*
7. Detect (ISCM)	50. How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings?	FY24	Level 2: Defined	2	Auditor's Comment: The next level is not met because the CIGIE OCIO does not capture qualitative and quantitative performance measures on the performance of its ISCM program.

No.	FY24-Core IG FISMA Metrics Evaluation Questions	Core Metric or FY	Maturity Level	Rating	FY24-Auditor's Comments
7. Detect (ISCM)	51. Provide any additional information on the effectiveness (positive or negative) of the organization's ISCM program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the ISCM program effective? 51.1 Please provide an IG self-assessment rating (Effective/Not Effective) for the agency's detect function.	Summary Q		2	The CIGIE OCIO has achieved the rating of Defined (Level 2) for its Information Security Continuous Monitoring metrics evaluation.
	8. Respond - Incident Response				
8. Respond (IR)	52. To what extent does the organization use an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents?	FY24	Level 4: Managed and Measurable	4	*Auditor's Comments: The next level is not met because the CIGIE OCIO does not make near real-time updates to its incident response plan based on changing risk environments and threat information. Also, the CIGIE OCIO did not participate in DHS's Cyber Storm national level exercise, as appropriate, or other exercises to assess cybersecurity preparedness and examine incident response processes.*

No.	FY24-Core IG FISMA Metrics Evaluation Questions	Core Metric or FY	Maturity Level	Rating	FY24-Auditor's Comments
8. Respond (IR)	53. To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization?	FY24	Level 5: Optimized	5	*Met*
8. Respond (IR)	54. How mature are the organization's processes for incident detection and analysis?	Core Metric	Level 2: Defined	2	Auditor's Comments: The next level is not met because the CIGIE OCIO does not meet the logging requirements at the maturity event logging tier (EL2) in accordance with M-21-31.
8. Respond (IR)	55. How mature are the organization's processes for incident handling?	Core Metric	Level 5: Optimized	5	*Met*
8. Respond (IR)	56. To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner?	FY24	Level 5: Optimized	5	*Met*

No.	FY24-Core IG FISMA Metrics Evaluation Questions	Core Metric or FY	Maturity Level	Rating	FY24-Auditor's Comments
8. Respond (IR)	59. Provide any additional information on the effectiveness (positive or negative) of the organization's incident response program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the incident response program effective? 59.1 Please provide an IG self-assessment rating (Effective/Not Effective) for the agency's respond function.	Summary Q		3	The CIGIE OCIO has achieved the rating of Consistently Implemented (Level 3) for its Incident Response metrics evaluation.
	9. Recover - Contingency Planning				
9. Recover (CP)	61. To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts?	Core Metric	Level 2: Defined	2	*Auditor's Comment: The next level is not met because the CIGIE OCIO did not conduct an organizational BIA to identify the operational and financial impacts resulting from the disruption of business functions and processes.*
9. Recover (CP)	62. To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans?	FY24	Level 3: Consistently Implemented	3	*Auditor's Comment: The next level is not met because the CIGIE OCIO does not coordinate the development of its contingency plan with external service providers.*

No.	FY24-Core IG FISMA Metrics Evaluation Questions	Core Metric or FY	Maturity Level	Rating	FY24-Auditor's Comments
9. Recover (CP)	63. To what extent does the organization perform tests/exercises of its information system contingency planning processes?	Core Metric	Level 3: Consistently Implemented	3	*Auditor's Comment: The next level is not met because the CIGIE OCIO did not employ automated mechanisms to its test system contingency plan and did not coordinate its plan testing with external stakeholders.*
9. Recover (CP)	64. To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate?	FY24	Level 4: Managed and Measurable	4	*Auditor's Comment: The next level is not met because the CIGIE OCIO did not perform a full recovery and reconstitution of systems to a known state.*
9. Recover (CP)	66. Provide any additional information on the effectiveness (positive or negative) of the organization's contingency planning program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the contingency planning program effective? 66.1 Please provide an IG self-assessment rating (Effective/Not Effective) for the agency's recover function.	Summary Q		3	The CIGIE OCIO has achieved the rating of Consistently implemented (Level 3) for its Contingency Planning metrics evaluation.

Appendix III - Acronyms

	Acronyms
BIA	Business Impact Analyses
CIGIE	Council of the Inspectors General on Integrity and Efficiency
DISA	Defense Information Systems Agency
EL	Event Logging
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GRC	Governance, Risk, and Compliance
GSS	General Support System
IG	Inspector General
ISCM	Information Security Continuous Monitoring
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OCIO	Office to the Chief Information Officer
OMB	U.S. Office of Management and Budget
REV	Revision
SCAP	Security Content Automation Protocol
SCRM	Supply Chain Risk Management
STIG	Security Technical Implementation Guides
SP	Special Publication
SSP	System Security Plan

Appendix IV – Management's Comments

NONCONFIDENTIAL // EXTERNAL

COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY

DATE: October 21, 2024

TO: Gail Jenifer, Member, Brown & Company

From: David A. Morris, Chief Operating Officer DAVID MORRIS Digitally signed by DAVID MORRIS Date: 2024.10.21 17:25:58 -04'00'

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 2024

This memorandum provides the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) comments and actions planned and undertaken to address the recommendations contained in the Audit of CIGIE's compliance with provisions of the Federal Information Security Modernization Act (FISMA) for Fiscal Year 2024. CIGIE appreciates the comprehensive assessment of CIGIE's information security program by the auditors, along with the insights and recommendations that will help CIGIE strengthen the security and resilience of the systems.

CIGIE remains firmly committed to managing its information security program with diligence and transparency. Over the past few years, in addition to the work done to meet cybersecurity mandates, CIGIE has actively participated in several Department of Homeland Security programs, such as the Cloud Log Aggregation Warehouse (CLAW), Protective DNS Services, Continuous Diagnostics and Mitigation (CDM), Web Application Scanning (WAS), the DHS Vulnerability Disclosure Program (VDP) via Bugcrowd, and the Joint Cyber Defense Collaborative (JCDC). These initiatives have significantly enhanced CIGIE's ability to monitor and defend against cybersecurity threats.

Additionally, by migrating all critical technology resources to FedRAMP-authorized systems, including hosting in the Azure High-Cloud environment and utilizing the Office 365 Government Community Cloud (GCC), CIGIE has eliminated single points of failure and achieved a 100-percent cloud-powered infrastructure. This cloud transition has greatly increased the resilience, scalability, and security of CIGIE's IT systems.

Given the size of CIGIE and the steps the agency has taken to protect its information systems, CIGIE is taking steps to focus on risk management-based security outcomes. As stated in the FY 2023 - 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, dated February 10, 2023:

> *IGs have the discretion to determine whether an agency is effective in each of the Cybersecurity Framework Function (e.g., protect, detect) and whether the agency's overall information security program is effective based on the results of the determinations of effectiveness in each function and the overall assessment.*

1750 H Street, NW ★ Suite 400 ★ Washington DC ★ 20006-4679

Therefore, an IG has the discretion to determine that an agency's information security program is effective even if the agency does not achieve a level 4 (managed and measurable).

Reflecting OMB's shift in emphasis away from compliance in favor of risk management-based security outcomes, IGs are encouraged to evaluate the IG metrics based on the risk tolerance and threat model of their agency and to focus on the practical security impact of weak control implementations, rather than strictly evaluating from a view of compliance order the mere presence or absence of controls.

Again, CIGIE greatly appreciates the work the auditors have done, and CIGIE will continue to prioritize the protection of its critical infrastructure and the mitigation of cybersecurity risks. Below is CIGIE management's response to the 16 recommendations contained in the report. CIGIE agrees with these recommendations and will develop plans of action and milestones to address them in FY 2025.

Recommendation 1 – It is recommended the CIGIE OCIO implement a Governance, Risk, Compliance (GRC) solution to manage and monitor cybersecurity risks required by NIST SP 800-39 and to provide a centralized enterprise-wide view of all risks across the agency.

CIGIE agrees with this recommendation. A GRC tool would be helpful for enterprise risk management and CIGIE will undertake a review of available GRC solutions and/or other options, along with the associated costs, to develop a plan to strengthen this area.

In addition to reviewing the feasibility of implementing a GRC solution, CIGIE will work to enhance its existing cyber risk-management practices, including strengthening manual processes and leveraging existing automated tools to prioritize and address risks to CIGIE's systems.

Recommendation 2 – It is recommended that 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 (SCRM) and as required by OMB.

CIGIE agrees with this recommendation. Although CIGIE currently makes purchases from Federally approved vendors to mitigate risks, a comprehensive SCRM needs to be developed. CIGIE will take actions to develop a comprehensive SCRM that will include policies, procedures, and guidelines for assessing and managing supply chain risks.

Recommendation 3 – It is recommended that CIGIE OCIO develop and implement comprehensive anti-counterfeit policies and procedures and provide appropriate training for personnel.

CIGIE agrees with this recommendation. As a part of the SCRM strategy, CIGIE will determine what anti-counterfeit policies and procedures are necessary.

Recommendation 4 – It is recommended CIGIE OICO remediate vulnerabilities in its information systems in a timely manner as required by the agency's policy.

CIGIE agrees with this recommendation. The audit report highlighted one high-level vulnerability relating to an SSL certificate that was not remediated within 30 days. In that case, the vulnerability was remediated less than 60 days after being identified, it was limited to a single server and located on the intranet, protected by perimeter firewalls, and inaccessibility to the public, so the risk of exploitation was minimal. However, CIGIE did not fix that vulnerability within the timeframe identified in the policy.

Recommendation 5 – It is recommended that CIGIE OCIO scan all information products to assess configuration setting, resolve unsecured configuration and provide appropriate training for personnel.

CIGIE agrees with this recommendation.

Recommendation 6 – It is recommended that CIGIE OCIO ensure physical and environmental access controls are in place and regularly monitored.

CIGIE agrees with this recommendation. The CIGIE office space in Brunswick, Georgia is on a campus not accessible to the public, and CIGIE's IT equipment is co-located with other agencies' IT equipment. CIGIE had been scheduled to move to a new location and had planned on addressing the issues in the new location. That move has now been postponed for at least five years, and CIGIE has already begun taking steps to address the issues identified.

Recommendation 7 – It is recommended that 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 effective operations.

CIGIE agrees with this recommendation. The CIGIE office space in Brunswick, Georgia is on a campus not accessible to the public, and CIGIE's IT equipment is co-located with other agencies' IT equipment. CIGIE had been scheduled to move to a new location and had planned on addressing the issues in the new location. That move has now been postponed for at least five years, and CIGIE has already begun taking steps to address the issues identified.

Recommendation 8 – It is recommended that CIGIE OCIO ensure that all visitor access to the facility and network area is recorded, including entry and exit times, purpose of visit, and areas accessed.

CIGIE agrees with this recommendation. The CIGIE office space in Brunswick, Georgia is on a campus not accessible to the public, and CIGIE's IT equipment is co-located with other agencies' IT equipment. CIGIE had been scheduled to move to a new location and had planned on addressing the issues in the new location. That move has now been postponed for at least five years, and CIGIE has already begun taking steps to address the issues identified.

Recommendation 9 – It is recommended that CIGIE OCIO ensure security awareness and privacy training is provided to all system users as required by the agency's policy, and track performance.

CIGIE agrees with this recommendation. One employee started in September 2023 and the completed training from September 2023 was incorrectly counted towards completing the FY 2024 training. CIGIE acknowledges the error.

Recommendation 10 – It is recommended the CIGIE develop a cybersecurity workforce assessment plan that aligns with the NIST Special Publication 800-181 Revision 1, Workforce Framework for Cybersecurity (NICE Framework).

CIGIE agrees with this recommendation. CIGIE will take steps to develop a cybersecurity workforce assessment plan that aligns with NIST 800-181.

Recommendation 11 – It is recommended that CIGIE conduct a cybersecurity workforce assessment of its workforce's knowledge, skills, and abilities to identify any skill gaps and specialize training needs.

CIGIE agrees with this recommendation.

Recommendation 12 – It is recommended that CIGIE OCIO update its system security plan (SSP), policies, and procedures to align with the NIST control families, specifically focusing on Program Management, Supply Chain Risk Management, and the privacy-related controls for Personally Identifiable Information Processing and Transparency.

CIGIE agrees with this recommendation.

Recommendation 13 – It is recommended that CIGIE monitor its ISCM program and document lessons learned to make improvements to the ISCM policies and strategy.

CIGIE agrees with this recommendation.

Recommendation 14 – It is recommended that CIGIE OCIO implement logging requirements as required by OMB M-21-31.

CIGIE agrees with this recommendation. CIGIE will accelerate the implementation of logging requirements as specified in OMB M-21-31.

Recommendation 15 – It is recommended that CIGIE develop an organizational-level and system-level business impact analyses (BIA) that aligns with the applicable NIST controls and update its contingency plan.

CIGIE agrees with this recommendation. CIGIE will conduct a comprehensive organizational level and system level business impact assessment that aligns with NIST requirements.

Recommendation 16 – It is recommended that CIGIE 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.

CIGIE agrees with this recommendation. CIGIE will review and approve its contingency plan to ensure that it reflects the results of the BIAs and addresses the identified criticality of systems and operations.

Appendix V – Auditor's Response to Management's Comments

Brown & Company CPAs and Management Consultants, PLLC

We acknowledge receipt of CIGIE's memorandum dated October 21, 2024, which outlines CIGIE's comments and planned actions in response to the findings and recommendations presented in our Independent Auditor's Performance Audit Report on CIGIE's compliance with the FISMA for Fiscal Year 2024. We appreciate the thoroughness of CIGIE's response and its commitment to addressing the identified issues.

After reviewing the response, we find that CIGIE's planned actions to address all 16 recommendations are appropriate and aligned with best practices for information security management. CIGIE's agreement with the recommendations and the steps provided for implementation demonstrates a proactive approach to strengthening the agency's information security program. Specific actions, such as the adoption of a Governance, Risk, and Compliance (GRC) tool, the development of a supply chain risk management strategy, and enhancements to the cybersecurity workforce assessment plan, are commendable steps toward achieving compliance and risk management goals. We will evaluate the progress of these corrective actions during the next audit.

We appreciate the collaboration and look forward to continued progress in enhancing CIGIE's information security posture.