OFFICE OF THE
INSPECTOR GENERAL

Smithsonian

Memo

Date: September 29, 2025

To: Lonnie Bunch, Secretary

Cc: Ron Cortez, Under Secretary for Finance and Administration
John Lynskey, Deputy CFO/Controller
Carmen Iannacone, Acting Chief Information Officer
Juliette Sheppard, Director, Information Technology Security, Officer of the Chief Information Officer (OCIO)
Danee Gaines Adams, Chief Privacy Officer, OCIO
Catherine Chatfield, Program Manager, Enterprise Risk Management and Audit Liaison

From: Nicole Angarella, Inspector General

Signed by:
Nicole L Angarella
6E3A9C42718646B...

Subject: *Fiscal Year 2025 Independent Evaluation of the Smithsonian Institution's Information Security Program* (OIG-A-25-07)

This memorandum transmits our final audit report of Castro & Company, LLC (Castro) on the *Fiscal Year 2025 Independent Evaluation of the Smithsonian Institution's (Smithsonian) Information Security Program.*

Under a contract monitored by this office, the Office of the Inspector General engaged Castro, an independent public accounting firm, to perform the audit. For fiscal year 2025, Castro found that the Smithsonian's information security program was operating effectively as defined by the Department of Homeland Security. Castro made no findings or recommendations.

Castro is responsible for the attached report and the conclusions expressed in the report. We reviewed Castro's report and related documentation and interviewed their representatives. Our review disclosed no instances in which Castro did not comply, in all material respects, with the U.S. Government Accountability Office's *Government Auditing Standards*.

We appreciate the courtesy and cooperation of all Smithsonian management and staff during this audit. If you have any questions, please contact me or Joan Mockeridge, Assistant Inspector General for Audits, Inspections, and Evaluations.

Smithsonian Institution Office of the Inspector General
Report on the Smithsonian Institution's
Information Security Program

Fiscal Year 2025

Contents

Castro & Company
Auditors ✓ Advisors

1635 King Street
Alexandria, VA 22314
Phone: 703.229.4440
Fax: 703.859.7603
www.castroco.com

Nicole Angarella
Inspector General
Office of the Inspector General Smithsonian Institution
600 Maryland Ave, Suite 695E Washington, DC 20024

Dear Ms. Angarella:

We are pleased to provide our report outlining the result of the performance audit conducted to evaluate the effectiveness of the Smithsonian Institution's (Smithsonian) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) for the fiscal year ending September 30, 2025.

FISMA requires each executive branch agency Inspector General, or an independent external auditor, to conduct an annual evaluation of their agency's information security program and practices, and to report to the Office of Management and Budget on the results of their evaluations. We understand that the Smithsonian is not required to comply with FISMA because it is not an executive branch agency; however, the Smithsonian applies FISMA standards to its information security program as a best practice to the extent practicable and consistent with its mission.

We conducted this performance audit 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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We have no findings or recommendations included in this report. Smithsonian management has provided us with a response to this fiscal year 2025 FISMA audit report. Their response is presented in its entirety in the Management's Response section of the report. We did not audit management's response and, accordingly, do not express any assurance on it. This report is issued for the restricted use of the Office of Inspector General, the management of the Smithsonian, the Office of Management and Budget, and the Department of Homeland Security.

Castro & Company, LLC

September 25, 2025

Introduction

On behalf of the Smithsonian Office of the Inspector General (OIG), Castro & Company, LLC (Castro) performed an independent performance audit of the Smithsonian Institution's (Smithsonian) information security program and practices. Our audit was based on guidance outlined in the Federal Information Security Modernization Act of 2014 (FISMA) and the fiscal year (FY) 2025 Department of Homeland Security (DHS) Inspector General Reporting Metrics Version 2.0, April 3, 2025. The Smithsonian is not required to comply with FISMA because it is not an executive branch agency, but the Smithsonian applies FISMA standards as a best practice to the extent practicable.

Purpose

FISMA was enacted to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. Specifically, FISMA requires agencies to develop, document, and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency. Further, FISMA requires the OIG to conduct an independent evaluation of the entity's information security program and report the results to the Office of Management and Budget (OMB).

To ensure the adequacy and effectiveness of the organization's information security program, FISMA requires entity program officials, chief information officers, chief information security officers, and senior agency officials for privacy, to conduct an annual evaluation of their information security programs and to report the results to DHS. However, since the Smithsonian is not required to comply with FISMA, it has chosen not to report metrics to DHS.

Background

The Smithsonian Institution

The Smithsonian is a trust instrumentality of the United States government founded in 1846 in response to the will of Englishman James Smithson who bequeathed the whole of his property to the United States with the mission "to found at Washington, under the name of the Smithsonian Institution, an establishment for the increase and diffusion of knowledge." As a trust instrumentality of the United States, the Smithsonian is not a part of the executive branch of the federal government and therefore, is not required to comply with FISMA; however, the Smithsonian applies FISMA standards as a best practice to the extent practicable.

Since its founding in 1846, the Smithsonian has become the world's largest museum and research complex consisting of 21 museums, the National Zoological Park, and 14 education and research facilities. A major portion of the Smithsonian's operations is funded from annual federal appropriations. In addition to federal appropriations, the Smithsonian receives private support, government grants and contracts, and income from investments and various business activities.

The Office of the Chief Information Officer

The Office of the Chief Information Officer (OCIO) has primary responsibility for the development, implementation, and enforcement of the Smithsonian's information technology (IT) security policies, procedures, and program. The OCIO centrally manages the security assessment and authorization activities over Smithsonian information systems, and centrally operates the majority of the Smithsonian's computer facilities, equipment, web infrastructure, web-hosting services, telecommunications, and networks. Where IT is decentralized, the OCIO provides direct management oversight. The Smithsonian's IT security group is managed by the Director of IT security who reports directly to the Chief Information Officer.

Smithsonian Privacy Office

The Smithsonian Privacy Program is administered by the Smithsonian Privacy Office, located within the OCIO, and led by the Smithsonian Privacy Officer who reports directly to the Chief Information Officer (CIO). The Smithsonian Privacy Officer is responsible for developing, implementing, and maintaining a Smithsonian-wide privacy program designed to ensure compliance with all applicable statutes, regulations, and policies regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of personally identifiable information (PII) by Smithsonian employees and affiliated persons. The Smithsonian Privacy Officer is also responsible for developing and evaluating privacy policy, managing privacy risks at the Institution, and ensuring the delivery of privacy training to all Smithsonian staff and affiliated persons who handle PII as a routine part of their job responsibilities.

Objective, Scope, and Methodology

Objective

Castro was contracted by the Smithsonian OIG to evaluate the effectiveness of the Smithsonian's information security program and practices in place during FY 2025. Castro conducted this performance audit 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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.[1]

Scope

Castro evaluated Smithsonian security and privacy controls in place during the period of October 1, 2024, through June 30, 2025. The Smithsonian has 32 major IT systems and general support systems. Each year, a representative sample of systems is selected for FISMA testing. For the period reviewed, Castro, in coordination with the OIG, selected the following three systems for evaluation:

1. [redacted]
2. [redacted]
3. [redacted]

[1] Internal Control deficiencies deemed significant to the objective of the audit (effectiveness of the Smithsonian's information security program and practices) are discussed within this report.

[redacted]

The Smithsonian follows federal best practices and categorizes their systems (low, moderate, or high) using guidance outlined in Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*. This categorization is a key factor used in determining necessary security controls for each system. For the above systems in our FY 2025 scope, we noted their Federal Information Processing Standard 199 security categorizations were all moderate.

Methodology

To evaluate the effectiveness of the Smithsonian's information security program and practices, Castro utilized a variety of audit procedures including interviews, review of available documentation, and judgmental sampling. Further, Castro utilized OMB Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements* (M-25-04), and the *FY 2025 Inspector General FISMA Reporting Metrics*.

In FY 2022, OMB and the Council of the Inspectors General on Integrity and Efficiency, transitioned the Inspector General metrics process to a multi-year cycle. Under this multi-year cycle, OMB selected a core group of metrics, representing a combination of Administration priorities and other highly valuable controls, that must be evaluated annually. Core metrics were chosen based on alignment with Executive Order 14028, *Improving the Nation's Cybersecurity*, as well as recent OMB guidance to agencies in furtherance of the modernization of federal cybersecurity. The remaining metrics were evaluated on a two-year cycle (beginning in FY 2023) based on a calendar agreed to by the Council of the Inspectors General on Integrity and Efficiency, the Chief Information Security Officer Council, OMB, and the Cybersecurity & Infrastructure Security Agency. For FY 2025, Castro evaluated the core metrics and FY 2025 Supplemental metrics[2] identified within the FY 2025 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics document.

The IG FISMA Reporting Metrics align with the six core functions in The National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 (Cybersecurity Framework): govern, identify, protect, detect, respond, and recover. The Cybersecurity Framework provides agencies with a common structure for managing and reducing their cybersecurity risks across the enterprise and provides OIGs with guidance for assessing the maturity of controls to address those risks. These metrics represent a continuation of work begun in FY 2016, when the DHS OIG metrics were aligned with the five functional areas in the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework). The five security functions included Identify, Protect, Detect, Response, and Recover. Within these now six functions are ten domains, which include Cybersecurity Governance, Cybersecurity Supply Chain Risk Management, Risk and Asset Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning.

[2] For FY 2025, OMB identified new Supplemental Metrics that were different from the annual metrics (two-year cycle) tested in FYs 2023 and 2024.

Metric Maturity Levels

The Smithsonian's implementation of controls and processes related to each reporting metric were evaluated on a maturity model spectrum from Level 1: Ad-hoc to Level 5: Optimized. In previous years, we utilized a mode-based scoring approach to assess the Smithsonian's maturity levels. Under this approach, ratings were determined by a simple majority, where the most frequent level across the questions served as the domain rating. For FY 2025, we utilized a weighted average scoring method per guidance outlined in the FY 2025 Inspector General FISMA Reporting Metrics. The table below provides a description of the different levels.

Table 1: FY 2025 OIG Evaluation Maturity Levels

Level	Description
1 – Ad-hoc	Policies, procedures, and strategies are not formalized, activities are performed in an ad-hoc, reactive manner.
2 – Defined	Policies, procedures, and strategies are formalized and documented, but not consistently implemented.
3 – Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
4 – Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies and procedures, and strategies are collected across the organization, and used to assess them and make necessary changes.
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.

Finally, based on generally accepted government auditing standards paragraph 8.41d, some factors that may be considered when determining the significance to the audit objectives include the five components of internal control and the integration of the components. Factors that we considered in determining the significance of internal controls to the audit objectives included the five components of internal control also contained in the *Standards for Internal Controls in the Federal Government*.[3] These standards provide criteria for designing, implementing, and operating an effective internal control system. *Standards for Internal Controls in the Federal Government* defines five components of internal controls:

- Control Environment,
- Risk Assessment,
- Control Activities,
- Information and Communication, and
- Monitoring.

[3] Government Accountability Office, *Standards for Internal Controls in the Federal Government*, GAO-14-704G, September 2014, paragraph OV2.04, Components, Principles and Attributes.

Audit Results

Using the maturity model noted above in Table 1, Castro determined that the Smithsonian's information security program was operating effectively during FY 2025. This determination was made following guidance outlined in the FY 2025 Inspector General FISMA Reporting Metrics document, which states, "*As with previous guidance on the use of the five-level maturity model, a Level 4, Managed and Measurable, information security program is still considered operating at an effective level of security*". Our overall assessment of an effective security program is based on our audit results at the domain level, which are summarized in Table 2 below.

Table 2: FY 2025 FISMA Metric Results

Functional Area	Domains	Results
Govern	Overall	Managed and Measurable
	Cybersecurity Governance	Managed and Measurable
	Supply Chain Risk Management	Managed and Measurable
Identify	Risk and Asset Management	Managed and Measurable
Protect	Overall	Managed and Measurable
	Configuration Management	Managed and Measurable
	Identity and Access Management	Consistently Implemented
	Data Protection and Privacy	Managed and Measurable
	Security Training	Managed and Measurable
Detect	Information Security Continuous Monitoring	Managed and Measurable
Respond	Incident Response	Managed and Measurable
Recover	Contingency Planning	Managed and Measurable

Overall, we found that the Smithsonian continued to make improvements to their security program and further refined existing controls and processes. Improvements made to the Smithsonian's security program in FY 2025 included:

- Further implementation of their Cybersecurity Supply Chain Risk Management (C-SCRM) program.
- Identification of security controls (minor system overlay) for minor systems handling sensitive PII
- Addition of an internal auditor to review OCIO assessment activities and the quality of security controls and documentation.
- Further enhancement and use of their Governance, Risk and Compliance tool and active monitoring of the security program through various dashboards and Key Performance Indicators (KPIs).

We noted that the Smithsonian continued to make improvements to their security program, and we have identified no deficiencies in internal control that are deemed significant within the context of our audit objectives and based on the audit work performed.[4] The following sections outline the results of our audit across the six FISMA function areas and ten domains.

[4] Government Accountability Office, *Government Auditing Standards*, Reporting Standards for Performance Audits, paragraph 9.31, Reporting on Internal Control.

Govern Function

Castro determined that the Smithsonian's Govern function was operating at Level 4, Managed and Measurable in FY 2025. The Govern function focuses on the development of cybersecurity profiles within the organization that help assess, prioritize, and communicate cybersecurity objectives, a cybersecurity risk management strategy to support operational decisions, cybersecurity roles and responsibilities, and risk management of the organization's cybersecurity and supply chain requirements. The Govern function is comprised of two domains: Cybersecurity Governance, and Cybersecurity Supply Chain Risk Management.

Cybersecurity Governance

Castro determined that the Smithsonian's Cybersecurity Governance domain was operating at Level 4, Managed and Measurable in FY 2025. We noted the Smithsonian identified cybersecurity and IT security goals and objectives and tied them to specific security processes and controls. Further, the Smithsonian implemented a formal risk management strategy, which identifies risks, and results in changes to how the Smithsonian implements cybersecurity and IT related controls and processes. Finally, the Smithsonian has identified key changes that were needed within the organization to manage risk at defined acceptable levels.

Cybersecurity Supply Chain Risk Management Domain

Castro determined that the Smithsonian's C-SCRM domain was operating at Level 4, Managed and Measurable in FY 2025. We noted the Smithsonian made significant progress implementing their C-SCRM strategy during the last two fiscal years. The Smithsonian's C-SCRM program has been substantially implemented and includes categorizing (low, moderate, high risk) and monitoring of third-party vendors and completing steps around verifying whether high priority vendors had appropriate security/privacy language within their contracts. Further, we noted that the Smithsonian had formal procurement processes for purchasing IT hardware and software and processes for installing hardware and software within the IT environment.

Identify Function

Castro determined that the Smithsonian's Identify function was operating at Level 4, Managed and Measurable in FY 2025. The Identify function helps organizations focus and prioritize their efforts, consistent with their risk management strategy and business needs based on the organization's understanding of business context, resources that support critical functions, and the related cybersecurity risks to systems, people, assets, data, and capabilities. The Identify function is comprised of one domain: Risk and Asset Management.

Risk and Asset Management Domain

Castro determined that the Smithsonian's risk and asset management domain was operating at Level 4, Managed and Measurable in FY 2025. Risk management is defined as the process of identifying, assessing, and responding to risk. An ineffective risk management program increases the likelihood that management will not have a clear understanding of risks present within the organization and therefore will not implement appropriate safeguards to maintain risk at an acceptable level.

Castro noted the Smithsonian continued to [redacted] Further, the Smithsonian continued to [redacted]

Protect Function

Castro determined that the Smithsonian's Protect function operated at a Level 4, Managed and Measurable, in FY 2025. The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event and is comprised of four domains: configuration management, identify and access management, data protection and privacy, and security training.

Configuration Management Domain

We determined that the Smithsonian's configuration management domain was operating at Level 4, Managed and Measurable in FY 2025. NIST Special Publication 800-53, Rev 5, *Security and Privacy Controls for Federal Information Systems and Organization*, defines configuration management as "A collection of activities focused on establishing and maintaining integrity of IT products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle."

In FY 2025, Castro noted the Smithsonian had formal configuration management policies, procedures, and plans in place[5]. We noted the Smithsonian had several Boards, including their Technical Review Board and Software Review Board, which oversaw and approved significant changes to the Smithsonian IT environment and had required configuration baselines implemented for platforms in use. Further, the Smithsonian, fully incorporated databases into their baseline scanning process.

[5] Configuration management policies include: [redacted]

Identity and Access Management Domain

We determined that the Smithsonian's Identity and Access Management domain was operating at Level 3, Consistently Implemented in FY 2025. For FY 2025, Identity and Access Management was [redacted]

While the Smithsonian has [redacted] and therefore determined that the Smithsonian had [redacted] Because this [redacted] by the Smithsonian, we are not issuing any new recommendations related to this issue.

Data Protection and Privacy Domain

We determined that the Smithsonian's Data Protection and Privacy domain was operating at Level 4, Managed and Measurable in FY 2025. For FY 2025, Data Protection and Privacy metrics were focused on the Smithsonian's encryption of data at rest and in transit, and security controls to enhance network security and prevent data exfiltration.

We noted that the Smithsonian had [redacted] The Smithsonian's data loss prevention tool was [redacted] When [redacted] Smithsonian personnel were [redacted] if they believed there was no issue present. Where [redacted] the Smithsonian Privacy Office had a formal process to review a sample of those [redacted] for appropriateness. We noted in FY 2024 and then again in FY 2025, [redacted]

Security Training Domain

Castro determined that the Smithsonian's Security Training domain was operating at Level 4, Managed and Measurable in FY 2025. For FY 2025, there was one Security Training metric, which was focused on determining if the Smithsonian used an assessment of skills, knowledge, and abilities of the Smithsonian's workforce to provide specialized security training within the different functional areas. We noted that the Smithsonian regularly performed evaluations and surveys to identify required skills and knowledge of personnel with security responsibilities. This information was used to update or enhance both general and specialized security training.

Detect Function

Castro determined that the Smithsonian's Detect function was operating at Level 4, Managed and Measurable in FY 2025. The Detect function is comprised of one domain, Information Security Continuous Monitoring (ISCM). In FY 2025, the ISCM domain was focused on the Smithsonian's use of ISCM policy and strategy, monitoring the integrity and security posture of all owned and associated assets, and determining to what extent the Smithsonian performed ongoing information assessments and granted system authorizations.

Information Security Continuous Monitoring Domain

Information Security Continuous Monitoring is focused on facilitating ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. Effective Information Security Continuous Monitoring allows organizations to timely respond to identified weaknesses or vulnerabilities to maintain risk within an acceptable level.

For FY 2025, we determined the Smithsonian had formal Information Security Continuous Monitoring processes in place that were centrally managed and carried out through the Smithsonian's Governance, Risk, and Compliance tool. Additionally, we noted that the Smithsonian continued to maintain and enhance a series of KPI's, dashboards, and scorecards within their Governance, Risk, and Compliance tool that allowed them to track completion of key Information Security Continuous Monitoring activities to provide senior management with information on the current risk posture of the Smithsonian's IT environment.

Respond Function

Castro determined that the Respond function was operating at Level 4, Managed and Measurable in FY 2025. The Respond function is comprised of one domain, Incident Response.

Incident Response Domain

In FY 2025, Incident Response metrics were focused on incident detection, analysis, and incident handling. NIST Special Publication 800-61 Rev 3. *Incident Response Recommendations and Considerations for Cybersecurity Risk Management,* states, "*Incident response is a critical part of cybersecurity risk management and should be integrated across organizational operations. All six NIST Cybersecurity Framework (CSF) 2.0 Functions play vital roles in incident response:*

- *Govern, Identify, and Protect help organizations prevent some incidents, prepare to handle incidents that do occur, reduce the impact of those incidents, and improve incident response and cybersecurity risk management practices based on lessons learned from those incidents.*
- *Detect, Respond, and Recover help organizations discover, manage, prioritize, contain, eradicate, and recover from cybersecurity incidents, as well as perform incident reporting, notification, and other incident-related communications*."

In FY 2025, we noted [redacted]
Further, the Smithsonian had a centralized Security Operations Center that monitored potential incidents and several [redacted]
Finally, the Smithsonian continued to [redacted]

Recover Function

Castro determined that the Smithsonian's Recover function operated at Level 4, Managed and Measurable in FY 2025. The Recover function is comprised of one domain, Contingency Planning.

Contingency Planning Domain

For FY 2025, the Contingency Planning metric questions were focused on whether the organization ensures the results of Business Impact Assessments are used to guide contingency planning, and the testing of contingency plans. NIST Special Publication 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, states, "Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods." In FY 2025, we noted the Smithsonian incorporated the results of Business Impact Assessments into their contingency planning process and tested contingency plans in accordance with their defined test schedules.

6 [redacted]

Appendix A – Acronyms

CASTRO	Castro & Company, LLC
C-SCRM	Cybersecurity Supply Chain Risk Management
CIO	Chief Information Officer
DHS	Department of Homeland Security
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
ISCM	Information Security Continuous Monitoring
IT	Information Technology
KPI	Key Performance Indicator
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
[redacted]	[redacted]
[redacted]	[redacted]

Appendix B – Management's Response and Castro & Company's Response

OIG provided the Smithsonian Institution management with a draft of Castro & Company's report for review and comment. Management's response is presented in its entirety in Appendix B. Castro & Company did not audit management's response and, accordingly, do not express any assurance on it.

Smithsonian
Office of the Under Secretary for Finance and Administration

OFFICIAL MEMO

DATE September 23, 2025

TO: Joan Mockeridge, Assistant Inspector General for Audits

FROM: Ronald S. Cortez, Under Secretary for Finance and Administration

CC: Meroe Park, Deputy Secretary and Chief Operating Officer
Greg Bettwy, Chief of Staff
Jennifer B. McIntyre, Chief Legal Officer
Porter Wilkinson, Chief of Staff to the Regents
Celita McGinnis, Office of Inspector General
Carmen Iannacone, Chief Technology Officer / Acting Chief Information Officer
Juliette Sheppard, Director, IT Security
Danee Gaines Adams, Privacy Officer
Isabel Meyer, Director, Digital Platforms
Catherine Chatfield, Program Manager, Enterprise Risk Management and OIG Liaison

SUBJECT: Management Response to "Smithsonian Institution Office of the Inspector General Report on the Smithsonian Institution's Information Security Program Fiscal Year 2025"

Thank you for the opportunity to review the report and noting that there were no findings identified in this period. As such, management concurs and does not have any comments.