

Information Security: Fiscal Year 2022 Independent Evaluation of the Smithsonian Institution's Information Security Program

In Brief

OIG-A-23-07, May 15, 2023

Background

Each year, the Department of Homeland Security and the Office of Management and Budget publish metrics to assist Inspectors General in their assessments of information security programs.

The metrics rank the maturity level of five functions (Identify, Protect, Detect, Respond, and Recover) on a scale of 1 to 5. As an entity's information security program progresses in maturity, it moves from an informal ad hoc state (Level 1) to formally documented policies and procedures (Level 2) that are consistently implemented (Level 3), managed through quantitative or qualitative measurement (Level 4), and finally optimized based on mission needs (Level 5). When an entity achieves Level 4 in at least three of the five cybersecurity functions, its information security program is considered effective overall.

What OIG Did

The Office of the Inspector General contracted with Castro & Company, LLC (Castro) to evaluate the effectiveness of the Smithsonian's information security program in fiscal year 2022. Two major applications were reviewed: [REDACTED]

What Was Found

Effective Information Security Program. For fiscal year 2022, Castro found that the Smithsonian Institution's (Smithsonian) information security program was effective overall, because it was operating at a managed and measurable level (Level 4) in four of five cybersecurity functions (Protect, Detect, Respond, and Recover) and at consistently implemented (Level 3) for the fifth function, Identify, which includes risk management and supply chain risk management.

Castro noted that Smithsonian continues to make improvements to their information security program. For example, the Assessment and Authorization policies and procedures were updated to include additional centralized review of this documentation and training for personnel responsible for key activities. Centralized monitoring was increased with the use of various dashboards and key performance indicators, and the tools used by the Security Operations Center were refined to identify and respond to potential threats.

Areas for Improvement. Castro also noted areas where the information security program can be further improved. For example, the Smithsonian's [REDACTED] is physically located within both the Smithsonian's [REDACTED] and the [REDACTED] [REDACTED] for contingency purposes, but the [REDACTED] security plan made no reference to the [REDACTED] or the [REDACTED] security controls for operating within the cloud. In addition, the Smithsonian has developed a formal IT Supply Chain Risk Management Strategy and implemented many, but not all, of the high priority milestones. For example, [REDACTED]

What Was Recommended

Castro made three recommendations to strengthen the Identify cybersecurity function. Castro recommended (1) [REDACTED]

[REDACTED] Management concurred with all three recommendations.

For a copy of the full report, visit <http://www.si.edu/oig>.

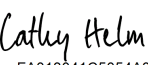


Date: May 15, 2023

To: Lonnie Bunch, Secretary

Cc: Meroë Park, Deputy Secretary and Chief Operating Officer
Ron Cortez, Under Secretary for Administration
Rick Flansburg, Deputy Under Secretary for Administration
Deron Burba, Chief Information Officer
Juliette Sheppard, Director, Information Technology Security, Office of the Chief Information Officer (OCIO)
Huyen Tran, Director, Office of System Modernization
Carmen Iannacone, Chief Technology Officer, OCIO
Danee Gaines Adams, Chief Privacy Officer, OCIO
Catherine Chatfield, Enterprise Risk Program Manager

From: Cathy L. Helm, Inspector General

DocuSigned by:

FA013041C5054A3...

Subject: *Fiscal Year 2022 Independent Evaluation of the Smithsonian Institution's Information Security Program (OIG-A-23-07)*

This memorandum transmits the final audit report of Castro & Company, LLC (Castro) on the fiscal year 2022 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 2022, Castro found that the Smithsonian's information security program was operating effectively as defined by the Department of Homeland Security. Castro made three recommendations for Smithsonian management to enhance information security at Smithsonian. Management concurred with all three 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 call me or Joan Mockeridge, Assistant Inspector General for Audits, at (202) 633-7050.

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

Fiscal Year 2022



Contents

Introduction.....	1
Purpose.....	1
Background.....	1
The Smithsonian Institution	1
The Office of the Chief Information Officer	1
Smithsonian Privacy Office	2
Objective, Scope, and Methodology	2
Objective.....	2
Scope.....	2
Methodology	3
Metric Maturity Levels	4
Audit Results.....	5
Identify Function	6
Risk Management Domain.....	6
Supply Chain Risk Management Domain.....	7
Protect Function	8
Configuration Management Domain	8
Identity and Access Management Domain	9
Data Protection and Privacy Domain.....	9
Security Training Domain.....	9
Detect Function	9
Information Security Continuous Monitoring Domain.....	10
Respond Function	10
Incident Response Domain	10
Recover Function	11
Contingency Planning Domain	11
Recommendations.....	11
Appendix A - Acronyms.....	12
Appendix B – Management’s Response and Castro & Company Response	13

Ms. Cathy Helm
Inspector General
Office of the Inspector General
Smithsonian Institution
600 Maryland Ave, Suite 695E
Washington, DC 20024

Dear Ms. Helm:

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, 2022.

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 made recommendations related to the challenges faced by the Smithsonian that, if effectively addressed by Smithsonian management, should strengthen the Smithsonian information security program. Smithsonian management has provided us with a response to this fiscal year 2022 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

April 26, 2023

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) 2022 Department of Homeland Security (DHS) Inspector General Reporting Metrics Version 1.1. 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. Further, due to FISMA reporting dates being moved up in FY 2022, the Smithsonian OIG was not able to report 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, 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 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 Office, located within the OCIO, is charged with safeguarding the personally identifiable information and sensitive personally identifiable information that the Smithsonian routinely collects, uses, processes, stores, maintains, disseminates, discloses, and disposes of, in order to carry out its mission. The Smithsonian Privacy Office develops and enforces privacy policies and procedures that are carried out by the Smithsonian units and reviews and approves all collections of personally identifiable information and sensitive personally identifiable information. The Smithsonian Privacy Officer reports directly to the Chief Information Officer.

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 during the period of October 1, 2021, through September 30, 2022 (FY 2022).¹ 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.

Scope

The Smithsonian has [REDACTED]. Each year, a representative sample of systems is selected for FISMA testing. For FY 2022, Castro, in coordination with the OIG, selected the following two systems for evaluation:

1. [REDACTED]
2. [REDACTED]

The Smithsonian follows federal best practices and categorizes their systems (low, moderate, or high) using guidance outlined in Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. This categorization is a key factor used in

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.

determining necessary security controls for each system. For the above systems in our FY 2022 scope, we noted their FIPS 199 security categorizations were both 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-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*, and OMB Office of the Federal Chief Information Officer *FY22 Core IG Metrics Implementation Analysis Guidelines document*.

In FY 2022, OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), transitioned the Inspector General (IG) metrics process to a multi-year cycle. Under this multi-year cycle, OMB will select a core group of metrics, representing a combination of Administration priorities and other highly valuable controls, that must be evaluated annually. The remainder of the standards and controls will be evaluated in metrics on a two-year cycle based on a calendar agreed to by CIGIE, the Chief Information Security Officer Council, OMB, and the Cybersecurity and Infrastructure Agency (CISA). The FY 2022 IG metrics evaluated represent the core group of metrics and were chosen based on alignment with Executive Order (EO) 14028, "Improving the Nation's Cybersecurity", as well as recent OMB guidance to agencies in furtherance of the modernization of federal cybersecurity, including:

- Moving the United States Government Toward Zero Trust Cybersecurity Principles (M-22-09) – OMB and CISA solicited public feedback on strategic and technical guidance documents meant to move the United States government towards a zero-trust architecture. The goal of OMB's Federal Zero Trust Strategy is to accelerate agencies towards a baseline of early zero trust maturity.
- Multifactor Authentication and Encryption (EO 14028) – Per the EO, agencies were required to fully adopt multifactor authentication and encryption for data at rest and in transit by November 8, 2021. For agencies that were unable to meet these requirements within 180 days of the date of the order, the agency head was directed to provide a written rationale to the Secretary of Homeland Security through the Director of CISA, the Director of OMB, and the Assistant to the President for National Security Affairs.
- Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents (M-21-31) – This memorandum provides specific requirements for log management. It includes a maturation model, prioritizing the most critical log types and requirements, to build a roadmap to success.
- Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response (M-22-01) – On October 8, 2021, this memorandum was issued for agencies to focus on improving early detection capabilities, creating "enterprise-level visibility" across components and sub-agencies, and requires agencies to deploy an Endpoint Detection and Response solution.
- Software Supply Chain Security & Critical Software – Section 4 of EO 14028 tasks OMB, the National Institute of Standards and Technology (NIST), and other federal entities with developing new guidelines and frameworks to improve the security and integrity of the technology supply chain. In collaboration with industry and other partners, this effort is providing frameworks and guidelines on how to assess and build secure technology, including open-source software.

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 include Identify, Protect, Detect, Response, and

Recover. Within these five functions are nine domains, which include Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response, Contingency Planning, and Supply Chain Risk Management.

Metric Maturity Levels

The Smithsonian’s implementation of controls and processes related to each reporting metric were evaluated and rated on a maturity model spectrum from Level 1: Ad-hoc to Level 5: Optimized, and ratings throughout the nine domains were determined using a simple majority where the most frequent level across the questions served as the domain rating. The table below provides a description of the different levels.

Table 1: FY 2022 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*.² 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.

² 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 2022. This determination was made following guidance outlined in the FY 2022 Core IG Metrics Implementation Analysis and Guidelines 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: FISMA Metric Results

Function Areas	Domains	Results
Identify	Overall	Consistently Implemented (Level 3)
	Risk Management	Managed and Measurable
	Supply Chain Risk Management	Defined
Protect	Overall	Managed and Measurable (Level 4)
	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 (Level 4)
Respond	Incident Response	Managed and Measurable (Level 4)
Recover	Contingency Planning	Managed and Measurable (Level 4)

Overall, we found that the Smithsonian continues to make improvements to their security program and further refine existing controls and processes. Improvements made to the Smithsonian’s security program in FY 2022 included:

- Updating Assessment and Authorization (A&A) policies and procedures to include additional centralized review of A&A documentation and training for personnel responsible for key A&A activities.
- Increased centralized monitoring through the use of various dashboards and key performance indicators.
- Further refinement of tools used by the Security Operations Center to identify and respond to potential security incidents.

While we determined the Smithsonian’s information security program was operating effectively, we also noted some areas where improvements should continue to be made. Specifically, the Smithsonian should continue working on making improvements to [REDACTED]. We have identified deficiencies in internal control that are deemed significant within the context of our audit objectives and based on the audit work performed.³ Based on the results of our audit, we identified two reportable issues and issued three associated recommendations to Smithsonian management. The following sections outline the results of our audit across the five FISMA function areas and nine domains.

³ Government Accountability Office, *Government Auditing Standards*, Reporting Standards for Performance Audits, paragraph 9.31, Reporting on Internal Control.

Identify Function

Castro determined that the Smithsonian’s Identify function was operating at Level 3, Consistently Implemented in FY 2022. 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 two domains: Risk Management, and Supply Chain Risk Management.

Risk Management Domain

Castro determined that the Smithsonian’s risk management domain was operating at Level 4, Managed and Measurable in FY 2022. 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 centrally maintain a governance, risk, and compliance tool which was used to carry out key risk management activities, including inventory management, and all assessment and authorization activities. While the Smithsonian had formal risk management policies, procedures, and controls in place in FY 2022, we did note areas where controls needed strengthening as detailed below.

1. [REDACTED] **Did Not Address** [REDACTED]

We noted that the Smithsonian’s [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] document, we noted the [REDACTED]
[REDACTED]
[REDACTED] As a result,
[REDACTED]
[REDACTED].

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

We noted the Smithsonian [REDACTED]
[REDACTED]
[REDACTED] While we noted the Smithsonian [REDACTED]

procedures were being carried out in FY 2022, we noted these procedures were not effective in ensuring [REDACTED]

Finally, we noted that the [REDACTED] We noted a similar issue with the effectiveness of the Smithsonian [REDACTED]

Supply Chain Risk Management Domain

Castro determined that the Smithsonian's supply chain risk management (SCRM) domain was operating at Level 2, Defined in FY 2022. In the past several years, several high-profile security incidents have occurred where vulnerabilities were introduced into federal agency IT environments through their supply chains. The federal government considers supply chain risks to be a significant area of potential weakness and as a result, has been taking several steps to try and address risks in this area. NIST issued Special Publication 800-161 *Supply Chain Risk Management Practices for Federal Information Systems and Organizations in 2015*, and more recently released Revision five of Special Publication 800-53 *Security and Privacy Controls for Information Systems and Organizations*, with a new control family that focuses on SCRM.

Castro noted that the Smithsonian has taken a number of steps to develop and implement supply chain risk management controls including for example:

- Developed an IT Supply Chain Risk Management Policy, Strategy, and Implementation Plan, which included the Smithsonian's strategy and implementation plan for implementing SCRM controls and processes,
- Defined roles and responsibilities for SCRM,
- Implemented a process to annually review the SCRM strategy,
- Defined criteria for determining how critical a supplier is to the Smithsonian's supply chain,
- Developed a Supplier Information Security Risk Assessment document that was used to give the Smithsonian an understanding of a supplier's security posture, and
- Implemented the use of standard privacy and security clauses to be used in contracts.

While the Smithsonian has developed a formal IT Supply Chain Risk Management Strategy and implemented many of the controls and processes within that strategy, we did note areas where controls needed strengthening as detailed below.

2. [REDACTED]

The Smithsonian has developed a [REDACTED]⁴ for implementing a [REDACTED]. The Smithsonian's [REDACTED] outlines five high-level objectives for implementing their [REDACTED]. Further, within each objective, the Smithsonian has identified more detailed implementation milestones that describe how the objectives will be achieved. For each implementation milestone, the Smithsonian has also identified a priority of high, moderate, or low, and identified a target completion date. While the Smithsonian has clearly identified the steps needed to implement their [REDACTED]

[REDACTED] was not fully implemented by September 30, 2022. Specifically, the Smithsonian had not implemented the following high priority milestones:

[REDACTED]

We noted the Smithsonian did not have [REDACTED] fully in place because [REDACTED]. For example, [REDACTED]. Without a fully developed and implemented [REDACTED], there is a higher risk of [REDACTED].

Protect Function

Castro determined that the Smithsonian’s Protect function operated at a Level 4, Managed and Measurable, in FY 2022. 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. NIST Special Publication (SP) 800-53, Rev 4, *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 2022, Castro noted the Smithsonian had formal configuration management policies, procedures, and plans in place⁵. Further, the Smithsonian had several Boards, including their Technical Review Board and Software Review Board, which oversee and approve significant changes to the Smithsonian information technology environment. While the Smithsonian had formal configuration management policies and procedures in place, we noted the Smithsonian [REDACTED]. Specifically, the Smithsonian had not implemented [REDACTED].

[REDACTED]



Identity and Access Management Domain

We determined that the Smithsonian’s Identity and Access Management domain was operating at Level 3, Consistently Implemented. For FY 2022, Identity and Access Management was focused on determining whether organizations had implemented strong authentication mechanisms for privileged and non-privileged users and to what extent the organization had implemented least privilege and separation of duty principles for privileged users.

We noted that the Smithsonian had implemented two-factor authentication and strong password requirements for accessing the Smithsonian network both remotely and onsite. Further, the Smithsonian had a formal process in place to approve, provision, and monitor the use of administrative or privileged accounts.

Data Protection and Privacy Domain

We determined that the Smithsonian’s Data Protection and Privacy domain was operating at Level 4, Managed and Measurable. For FY 2022, Data Protection and Privacy metrics were focused on encryption of data and controls to enhance network security and prevent data exfiltration.

We noted that the Smithsonian implemented Data Loss Prevention technology in FY 2022 that automatically blocked access to sensitive data. Further, we noted that the Smithsonian utilized a variety of technologies to encrypt sensitive data at rest and in transit.

Security Training Domain

Castro determined that the Smithsonian’s Security Training domain was operating at Level 4, Managed and Measurable in FY 2022. For FY 2022, Security Training metrics were focused on whether the organization utilized an assessment of skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training. In FY 2022, the Smithsonian had a comprehensive awareness and training program in place that included identifying and evaluating the security needs of personnel.

Detect Function

Castro determined that the Smithsonian’s Detect function was operating at Level 4, Managed and Measurable in FY 2022. The Detect function is comprised of one domain, Information Security Continuous Monitoring.

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 2022, 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 maintained a series of key performance indicators, 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 IT environment.

Respond Function

Castro determined that the Respond function was operating at Level 4, Managed and Measurable in FY 2022. The Respond function is comprised of one domain, Incident Response.

Incident Response Domain

In FY 2022, Incident Response metrics were focused on how mature the organization's processes were for incident detection, analysis, and handling. NIST SP 800-61 Rev 2. *Computer Security Incident Handling Guide*, states, "Computer security incident response has become an important component of information technology (IT) programs. Cybersecurity-related attacks have become not only more numerous and diverse but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services." We assessed the two Incident Response metric questions for FY 2022 at Level 4, Managed and Measurable.

In FY 2022, we noted [REDACTED]
[REDACTED] The Smithsonian had a [REDACTED]
[REDACTED]
[REDACTED] Finally, the
Smithsonian continued to [REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

Recover Function

Castro determined that the Smithsonian’s Recover function operated at Level 4, Managed and Measurable in FY 2022. The Recover function is comprised of one domain, Contingency Planning.

Contingency Planning Domain

For FY 2022, 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 whether the organization performs tests/exercises of its information system contingency planning processes. NIST SP 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 2022, we noted the Smithsonian had formal contingency plans in place that incorporated results of Business Impact Assessments. Further, contingency plans were tested, and lessons learned were documented and provided to management.

Recommendations

Castro has the following recommendation for [REDACTED]

1. [REDACTED]

Castro has the following recommendations to assist the Office of the Chief Information Officer with enhancing the information security program related to the issues noted above:

2. [REDACTED]
3. Fully implement high priority milestones identified within the Smithsonian [REDACTED]. Where [REDACTED] policy, procedures, or controls are developed to implement the high priority milestones, ensure those policy, procedures, and controls are fully documented.

Appendix A - Acronyms

████	████████████████████
████	████████████████████
CASTRO	Castro & Company, LLC
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CISA	Cybersecurity and Infrastructure Agency
DHS	Department of Homeland Security
EO	Executive Order
████	████████████████████
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IG	Inspector General
IT	Information Technology
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
████	████████████████████
████	████████████████████
SP	Special Publication

Appendix B – Management’s Response and Castro & Company 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 Institution

Office of the Chief Information Officer

Date: April 24, 2023

To: Cathy L. Helm, Inspector General

From: Deron Burba, Chief Information Officer

DocuSigned by:
Deron Burba
3B7C612876EA474...

CC: Ron Cortez, Under Secretary for Administration
Rick Flansburg, Deputy Under Secretary for Administration
Farleigh Earhart, Acting General Counsel
Porter Wilkinson, Chief of Staff to the Regents
Joan Mockeridge, Office of Inspector General
Celita McGinnis, Office of Inspector General
Juliette Sheppard, Director of IT Security
Carmen Iannacone, Chief Technology Officer
Huyen Tran, Director, Office of System Modernization
Catherine Chatfield, Enterprise Risk Program Manager

Subject: Management Response to “*Information Security: Fiscal Year 2022 Evaluation of the Smithsonian Institution's Information Security Program*”

Thank you for the opportunity to comment on the report. Management’s response to each of the recommendations is as follows.

Recommendation 1: [REDACTED]

Management Response: Management concurs with this recommendation and has [REDACTED]
[REDACTED] Management is also reviewing [REDACTED]
[REDACTED] We expect the remaining work to be completed by September 30, 2023.

Recommendation 2: [REDACTED]
[REDACTED]

Management Response: Management concurs with this recommendation and [REDACTED]
[REDACTED]
[REDACTED] We expect this work to be completed by September 30, 2023.

**Recommendation 3: Fully implement high priority milestones identified within the Smithsonian [REDACTED]
[REDACTED]. Where [REDACTED] policy, procedures, or controls are developed to implement the high priority milestones, ensure those policy, procedures, and controls are fully documented.**

Management Response: Management concurs with this recommendation. Some of the high priority milestones have been completed and the others are actively in progress. All policies and procedures related to these milestones will be documented. We expect the remaining work on high priority items to be completed no later than April 30, 2024.