In Brief

Information Security: Fiscal Year 2021 Independent Evaluation of the Smithsonian Institution's Information Security Program

OIG-A-22-05, June 24, 2022

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 to evaluate the effectiveness of the Smithsonian's information security program in fiscal year 2021. Three major applications were reviewed: Smithsonian network, Digital Asset Management System, and Smithsonian Tropical Research Institute's payroll and compensation system (Evolution).

What Was Found

Effective Information Security Program. For fiscal year 2021, Castro & Company, LLC (Castro) found that the Smithsonian Institution's (Smithsonian) information security program was operating at a managed and measurable level (Level 4) in three of five cybersecurity functions (Protect, Respond, and Recover) and therefore effective. Castro noted that Smithsonian's information security program was improved by addressing previously identified issues and recommendations, such as the use of its governance, risk, and compliance tool to centralize both the administration of security activities and the increased use of dashboards and key performance indicators for monitoring.

Areas for Improvement. Castro also noted areas where improvements in the information security program can continue to be made. For example, OCIO's security control manual does not require three specific controls—separation of duties, least privilege, and audit events—to be applied to all information systems. In addition, improvement is needed to ensure all phases of the Assessment and Authorization process are being carried out effectively. Castro identified that OCIO's assessment and authorization process for the three major systems reviewed did not identify and remediate several issues (such as the lack of segregation of duty controls in the Evolution payroll system).

For two of the three systems, there was no evidence that system changes were properly tested, analyzed for security impact, and approved before implemented. Castro also found that for the three systems, OCIO did not address failures identified in security scans. Castro determined that security configuration baselines were in use for all three systems reviewed, but OCIO did not document required risk-based decisions or obtain waivers when failures were identified in the compliance scans assessing baseline security controls.

What Was Recommended

Castro and Company, LLC made nine recommendations to strengthen three (identify, protect, and detect) cybersecurity functions, such as updating the Security Control Manual, ensuring documentation is retained when system changes are tested and approved before implemented, and documenting resolution of failures identified in compliance scans. Management concurred with all nine recommendations.

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

OFFICE OF THE
INSPECTOR GENERAL

Memo

Smithsonian

Information requiring protection from public dissemination has been redacted from this report in accordance with Smithsonian Directive 807, Requests for Smithsonian Institution Information, Exemption 2 and 5 U.S.C. § 552(b)(7)(E).

Date: June 24, 2022

To: Lonnie Bunch, Secretary

Cc: Meroë Park, Deputy Secretary and Chief Operating Officer
Ron Cortez, Under Secretary for Administration
Deron Burba, Chief Information Officer
Juliette Sheppard, Director, Information Technology Security, Office of the Chief Information Officer (OCIO)
Carmen Iannacone, Chief Technology Officer, OCIO
Joshua Tewksbury, Director, Smithsonian Tropical Research Institute (STRI)
Fernando Bouche, Information Technology Manager, STRI
Isabel Meyer, Digital Asset management System Branch Manager, OCIO

From: Cathy L. Helm, Inspector General Cathy L Helm

Subject: *Fiscal Year 2021 Independent Evaluation of the Smithsonian Institution's Information Security Program* (OIG-A-22-05)

This memorandum transmits the final audit report of Castro & Company, LLC (Castro) on the fiscal year 2021 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 2021, Castro found that the Smithsonian's information security program was operating effectively as defined by the Department of Homeland Security. Castro made nine recommendations for Smithsonian management to enhance information security at Smithsonian. Management concurred with all nine 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 2021

Castro & Company
Auditors ✓ Advisors

Contents

Introduction 1
Purpose 1
Background 1
The Smithsonian Institution 1
The Office of the Chief Information Officer 1
Smithsonian Privacy Office 2
Objectives, Scope, and Methodology 2
Audit Results 3
Identify Function 4
Risk Management Domain 4
Supply Chain Risk Management Domain 8
Protect Function 8
Configuration Management Domain 8
Identity and Access Management Domain 11
Data Protection and Privacy Domain 11
Security Training Domain 11
Detect Function 12
Information Security Continuous Monitoring Domain 12
Respond Function 13
Incident Response Domain 13
Recover Function 13
Contingency Planning Domain 13
Recommendations 14
Appendix A - Acronyms 15
Appendix B – Management's Response and Castro & Company Response 16

Castro & Company
Auditors ✓ Advisors

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

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, 2021.

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 2021 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

June 22, 2022

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) 2021 Department of Homeland Security (DHS) Inspector General Reporting Metrics Version 1.1, and guidance outlined in the FISMA. 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.

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. Nevertheless, based on the results of our audit, the Smithsonian OIG reported FISMA results 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 19 museums, the National Zoological Park, and nine research facilities, libraries, and archives. 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 OCIO centrally manages the Smithsonian's information technology (IT) environment and has primary responsibility for the development, implementation, and enforcement of the Smithsonian's IT security policies, procedures, and program. The OCIO centrally operates the majority of the Smithsonian's computer facilities, equipment, web infrastructure, web-hosting services, telecommunications, and networks. Where IT is decentralized, 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 (SPO), located within the OCIO, is charged with safeguarding the personally identifiable information and sensitive PII that the Smithsonian routinely collects, uses, processes, stores, maintains, disseminates, discloses, and disposes of, in order to carry out its mission. The SPO 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.

Objectives, Scope, and Methodology

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, 2020, through September 30, 2021 (FY 2021).[1] We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The Smithsonian has 32 major information technology systems and general support systems. Each year, a representative sample of systems is selected for FISMA testing. For FY 2021, Castro, in coordination with the OIG, selected the following three systems for evaluation:

1. **Smithsonian Institution Network (SINet)** – SINet is the Smithsonian's general support system and is located throughout the Smithsonian in almost every building and museum. SINet principally supports SINet Information Technology Infrastructure, SINet Enterprise Services, and SINet Web Services. SINet includes network transport, network security and shared infrastructure that provides the core capability to the rest of the Smithsonian's major applications and miscellaneous information technology systems that support the mission and objectives of the Smithsonian. SINet's shared infrastructure consists of the hosting environment (servers), numerous productivity applications (Email, SharePoint, Communication Services), Smithsonian Websites, Remote Access (Virtual Private Network and Citrix), and the end user's desktop environment.
2. **Digital Asset Management System (DAMS)** – DAMS is the central digital asset repository for over 40 Smithsonian units. DAMS is a collection management system that serves as the Smithsonian's enterprise digital media repository and provides storage, management, access, delivery, and preservation. DAMS works as an underlying mechanism to ensure the stewardship of the Smithsonian's digital media assets to support the Smithsonian's essential mission – the increase and diffusion of knowledge.
3. **Evolution, Payroll, HR and Time & Attendance System (Evolution)** – Evolution is an in-house Smithsonian Tropical Research Institute (STRI) payroll system with a complete suite of human resources (HR) tools and modules for payroll processing. Evolution provides payroll services to STRI personnel located at the STRI in the Republic of Panama. Smithsonian employees hired under Panamanian labor laws that work at STRI are not part of the Smithsonian's core payroll system and are therefore managed within Evolution.

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 determining necessary security controls for each system. For the above systems in our FY 2021 scope, we

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

noted FIPS 199 security categorizations of SINet, DAMS, and Evolution as moderate, low, and moderate respectively.

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 the DHS FY 2021 OIG FISMA Reporting Metrics Version 1.1. These metrics represent a continuation of work begun in FY 2016, when the DHS OIG metrics were aligned with the five function areas in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework). The five security functions include Identify, Protect, Detect, Response, and Recover. Within the security 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.

The Supply Chain Risk Management domain, which is part of the Identify function area, was new for FY 2021. While we assessed the Smithsonian's implementation of supply chain risk management controls, we did not consider those results when rating the Identify function in accordance with the OIG FISMA Reporting guidance.

Finally, the effectiveness of each reporting metric was 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 2021 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.

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 2021. This determination was made following guidance outlined in the FY 2021 DHS OIG FISMA Reporting Metrics Version 1.1, which states, "*Within the context of a maturity model, a Level 4, Managed and Measurable, information security program is 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	Consistently Implemented
	Supply Chain Risk Management	Defined (*Not Considered for overall Identify assessment*)
Protect	**Overall**	**Managed and Measurable (Level 4)**
	Configuration Management	Consistently Implemented
	Identity and Access Management	Consistently Implemented
	Data Protection and Privacy	Managed and Measurable
	Security Training	Managed and Measurable
Detect	Information Security Continuous Monitoring	**Consistently Implemented (Level 3)**
Respond	Incident Response	**Managed and Measurable (Level 4)**
Recover	Contingency Planning	**Managed and Measurable (Level 4)**

Our audit found that the Smithsonian has continued to make improvements to their security program including:

- Increased centralized administration of security activities through the Smithsonian's Governance, Risk, and Compliance tool.
- Increased centralized monitoring with the use of various dashboards and Key Performance Indicators.
- Refinement of log and monitoring data used by the Security Operations Center.

While we determined the Smithsonian's information security program was operating effectively, we also noted some areas where improvements could continue to be made. Specifically, the Smithsonian should continue refining and expanding their use of dashboards and key performance indicators, and also ensure all phases of the assessment and authorization process are being carried out effectively.

Based on the results of our audit, we identified six reportable issues and issued nine associated recommendations to Smithsonian management. The following sections outline the results of our audit across the five FISMA function areas and nine domains.

Identify Function

Castro determined that the Smithsonian's Identify function was operating at Level 3, Consistently Implemented in FY 2021. 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. While both domains are discussed below, only the Risk Management domain was considered when rating the Identify function.

Risk Management Domain

Castro determined that the Smithsonian's risk management domain was operating at Level 3, Consistently Implemented in FY 2021. Risk management is defined as the process of identifying, assessing, and responding to risk. An ineffective risk management program increases the risk that management will not have a clear understanding of risks present within the organization and therefore not implement appropriate safeguards to maintain risk at an acceptable level.

Castro noted the Smithsonian risk management roles and responsibilities were clearly identified within the Smithsonian policies, and risk management activities were being carried out with central oversight by the Smithsonian's Director of IT Security. The Smithsonian centrally maintained 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 2021, we did note several areas where controls needed strengthening.

1. **The Smithsonian's Selection of Security Controls Within their Control Catalog Needs Strengthening**

   The Smithsonian has developed a formal control catalog within Smithsonian Information Technology Technical Standards and Guidelines IT-930-02, *Security Controls Manual*, Version 4.3. While the Smithsonian's control catalog is based on security controls outlined in NIST SP 800-53 Rev. 4, it has been tailored by OCIO, to only include those controls that the Smithsonian believes are necessary for their environment. Controls identified in the Smithsonian's control catalog are required to follow the assessment and authorization process outlined in Technical Standards and Guidelines IT-930-03, *Security Assessment and Authorization,* which includes formally documenting them within a system security plan and periodically assessing them for effectiveness as part of the Smithsonian's continuous monitoring program.

   Our review of the Smithsonian's control catalog identified three NIST 800-53 controls that we believe management should include within their control catalog. While some of the controls below (e.g., separation of duties) may already be addressed to a degree within system documentation (policies or procedures), they are not required to be documented within the system security plan and to be periodically assessed for effectiveness as part of the Smithsonian's continuous monitoring program because they are not included in the control catalog.

   - Separation of Duties - 5 (AC-5) – Separation of duties address the potential for abuse of authorized privileges and helps to reduce the risk of malicious activity without collusion. The Smithsonian did not require separation of duties for all moderate systems. Rather, separation of duties controls were in the Smithsonian's control catalog as an overlay. Overlays add additional controls to the Smithsonian's security control baseline to help address specific risks to types of systems and data. The separation of duties control is only required for administrative accounts applicable to Enterprise HR or financial systems. Other roles within systems which may perform sensitive activities (such as process or approve financial transactions) or have access to sensitive data (such as sensitive personally identifiable information) were not required to be addressed.
   - Least Privilege - 6 (AC - 6) - Organizations employ least privilege for specific roles or duties within information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. While the Smithsonian's control catalog (within Security Controls Manual IT-930-02) did include the

least privilege control, it only included control enhancements (2, 7, and 9[2]) that were focused on privileged user activities and logging. [redacted] Further, while users were allowed to have multiple roles in the system, management had not documented which roles should not be combined or what controls the Evolution application provided to limit what each role could do.

- Audit Events - 2 (AU-2) - Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. For example, a system that processes sensitive PII may require logging and monitoring of access to that sensitive data. The Smithsonian did not include audit events within their control catalog (IT-930-02). Management should be identifying what events need to be audited at the system level based on the specific purpose, types of data, and overall risks to each system.

2. SI Assessment and Authorization Procedures Need Strengthening

The Smithsonian has developed and documented formal assessment and authorization policies and procedures within Technical Standards & Guideline IT-930-03, *Security Assessment & Authorization*, Version 1.4. We noted the Smithsonian relies on both their governance, risk, and compliance tool and centralized oversight of assessment and authorization activities to ensure procedures are carried out effectively and in accordance with established policy. While we noted the Smithsonian's assessment and authorization procedures were being carried out in FY 2021, we noted several issues that should have been identified and remediated during OCIO's centralized review process. Specifically, our review of system security plans for three systems in scope identified the following issues:

- (Evolution) The privacy overlay was not selected for the Evolution system, which processes sensitive privacy data.
- (Evolution) The Enterprise HR/Financial system overlay was not fully selected for the Evolution system. As a result, segregation of duties was not addressed within the Evolution system security plan.
- (Evolution) Evolution is physically located in the [redacted]. The Evolution Security System Plan did not address physical and environmental security controls over that location.
- Several control descriptions for controls in our testing scope did not accurately describe how controls had been implemented within the Smithsonian's IT environment. For example, we noted the system owner:
    - (SINet) Least Privilege - 6 (AC-6) – Did not accurately describe how administrative level accounts are currently designed and implemented within the Smithsonian's IT environment. For example, the SINet system security plan did not accurately discuss the different tiered accounts [redacted] currently being used for admin activities.

[2] AC-6 (2) The organization requires that users of information system accounts, or roles, with access to [*Assignment: organization-defined security functions or security-relevant information*], use non-privileged accounts or roles, when accessing nonsecurity functions. AC-6 (7) The organization: (a) Reviews [*Assignment: organization-defined frequency*] the privileges assigned to [*Assignment: organization-defined roles or classes of users*] to validate the need for such privileges; and (b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs. AC-6 (9) The information system audits the execution of privileged functions.

- (SINet) Remote Access - 17 (AC-17) – Inaccurately identified in the SSP as two methods of remote access, while documentation provided identified four different methods that could be used for personnel to remotely access the Smithsonian network environment.
- (SINet) Identification and Authentication (Organizational Users) - 2 (IA-2) – OCIO did not accurately describe all forms of remote access in the SINet SSP, and further stated that [redacted]
- (SINet) Authenticator Management - 5 (IA-5) – [redacted]
- (SINet) Contingency Training – 3 (CP-3) – Inaccurately stated contingency training should be conducted within 30 days of being assigned contingency roles and responsibilities, while Smithsonian Information Technology Technical Standard and Guidelines IT-930-02 stated training should be conducted within 180 days. OCIO management confirmed that the system security plan was not accurate and have since updated it to state 180 days.
- (SINet) Malicious Code Protection – (SI-3) - Referenced the use of [redacted] which had been replaced with newer tools. Further, the control description did not reference or discuss the use of [redacted] which was identified in IT-930-TN42.
- (DAMS) Session Termination -12 (AC-12) – Inaccurately stated in the DAMS system security plan that, "DAMS will automatically terminate a session after a 15-minute period of inactivity." However, we determined DAMS was configured to terminate sessions after 30 minutes of inactivity.
- (Evolution) Access Control Policy and Procedures – 1 (AC-1) - Policies and procedures did not identify, or reference existing Evolution account management procedures and stated procedures were being developed.

Technical Standard & Guideline, IT-930-03 *Security Assessment & Authorization*, section 7.1 requires system security plans to accurately describe how controls have been designed and implemented. Specifically, IT-930-03 states, "For each control that is not inherited from a common control, the specific implementation details must be defined for that particular system. Because the control catalog only describes controls at a high level, each system may implement the same control differently based on its technical and operational environment. Implementation details must document how the control is implemented for the entire system, including everything in the boundary. Implementation details must accurately describe what is currently in place. There should not be any language about what is planned but not yet implemented."

Supply Chain Risk Management Domain

In the past several years, a number of high-profile security incidents have occurred where vulnerabilities were introduced into federal agencies information technology environment 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 a number of steps to try and reduce risks in this area. For example, NIST issued Special Publication 800-161 *Supply Chain Risk Management Practices for Federal Information Systems and Organizations in 2015*, and more recently updated and released NIST Special Publication 800-53 Rev 5, which identifies specific controls around supply chain risk management.

For FY 2021, supply chain risk management was added as a new domain within the OIG FISMA metrics under the Identify function. IGs were asked to evaluate where agencies were in respect to implementing supply chain risk management controls in the FY 2021 OIG metrics.

While Castro determined that the Smithsonian's supply chain risk management function was operating at a maturity model Level 1, Defined, in FY 2021 this domain was not included in the overall assessment for the Identify function.

Castro noted that the Smithsonian has developed and documented a formal supply chain risk management strategy document and included privacy and security requirements within their third-party contracts. However, the Smithsonian had not implemented the recently developed supply chain risk management strategy as of September 30, 2021. Further, while federal executive branch agencies were required to implement NIST 800-53 Rev. 5 as of September 2021, the Smithsonian, who does not have to comply with FISMA, had not yet determined whether they will adopt the new requirements including those specific to supply chain risk management.

Protect Function

Castro determined that the Smithsonian's Protect function operated at a Level 4, Managed and Measurable, in FY 2021. 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 3, Consistently Implemented. NIST 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 2021, Castro noted the Smithsonian had formal configuration management policies, procedures, and plans. We noted 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. Further, the Smithsonian maintained formal documentation identifying items that were configuration controlled. We noted that for systems in scope, required Center for Internet Security

benchmarks were applied. While the Smithsonian had formal configuration management policies and procedures in place, we noted the following areas where configuration management controls could be strengthened.

3. Evidence That DAMS System Changes Were Properly Tested and Approved Could Not be Provided

We selected nine changes made to the DAMS system in FY 2021 for testing. While management did provide documentation from their change management system related to the nine changes, we noted this documentation, which includes general notes and the status of the change, did not show whether changes had been tested, analyzed for security impact, and approved before implementation. While the *DAMS Configuration Management Plan* did describe activities in the change control process, including required approvals and security impact, it did not require evidence of testing, security impact analysis, and approvals to be formally documented and retained.

Smithsonian Technical Note IT-920-TN04, *Configuration Management Step Three – Comply with CM,* states "System Owners and System Administrators shall ensure that each change to configuration components defined in the system's CM Plan is documented." Further, section 3.3.1 of the *DAMS Configuration Management Plan* states, "The change control process is based on approval of both the DAMS Project Manager and the representative(s) of the impacted business unit. Priorities are considered and estimates for the level of effort for the change are established. Security Impact and Risk are assessed prior to proposed changes being approved through the Change Control Board process. DAMS works with the vendor to test changes and OCIO for server configuration and builds. Change Control Board Reports are sent by the Manager to the Change Control Board Members and Chair in preparation for the Change Control Board meeting."

Without formal documentation showing changes were properly tested, considered for security impact, and approved, management's assurance that changes were appropriate is diminished.

4. Evidence That Evolution System Changes Were Properly Tested and Approved Could Not be Provided

We selected two changes made to the Evolution system in FY 2021 for testing. Through our testing, we determined that Smithsonian Evolution management did not use the ServiceNow system to manage changes as required by the Evolution Configuration Management Plan. Smithsonian Technical Note IT-920-TN04, *Configuration Management Step Three – Comply with CM,* states "System Owners and System Administrators shall ensure that each change to configuration components defined in the system's CM Plan is documented". As a result, documentation showing that changes were approved and potential security impact of changes were considered were not available for our review. We determined the current Evolution change management system served more as a project management tool rather than a repository to document key aspects of the change process. Smithsonian Evolution management stated they would use [redacted] to document change management activities going forward.

Without formal documentation showing changes were properly requested, tested, considered for security impact, and approved, management cannot be sure all changes made to the system were appropriate.

5. Controls Around the Implementation and Management of Required Security Control Baselines Need Strengthening

The Smithsonian has developed and approved formal security configuration baselines for use on Smithsonian configurable systems and infrastructure. Smithsonian-approved baselines are based on recommended security configurations from the Center for Internet Security. While we noted security configuration baselines were in use for all systems in scope, we determined that required risk-based decisions and/or waivers were not obtained for failures identified in the Center for Internet Security compliance scans. Specifically, we noted the following for each system in scope:

- **SINet** – We reviewed five baseline compliance scan reports for SINet, and noted 39 failures were identified in the reports. Per Smithsonian management, no risk-based decisions or waivers were in place for the issues noted.
- **DAMS** – We reviewed four Red Hat Linux baseline compliance scans for DAMS, and noted a total of 26 failures were identified in the reports. Per the Smithsonian DAMS management, no waivers or Risk Acceptances (also called Risk Based Decisions - RBD) had been developed for these failures. We did note that DAMS had a Plan of Actions and Milestones (POA&M), which stated compliance scan deviations needed to be remediated or submitted for risk-based decisions.
- **Evolution** – We reviewed one Microsoft Windows compliance scan for Evolution and noted two failures were identified in the report. Per Smithsonian Evolution management, no waivers or Risk Based Decisions had been developed for these failures. Further, we did not identify this issue within the Evolution POA&M document.

Finally, we noted control CM-6, Configuration Settings, was identified as a common control within the Smithsonian's Security Controls Manual, control catalog (IT-930-02) and within the DAMS and Evolution system security plans. As a common control, personnel at the system level where the control is being inherited would generally not be involved in carrying out any aspect of the control. However, we noted Smithsonian personnel at the system level are required to be involved in the waivers, Risk Based Decision, or POA&M processes. Incorrect categorization of security controls can increase the likelihood of individuals not having a clear understanding of their roles and responsibilities with regard to a specific control or process and increase the likelihood of key activities related to the control not being effectively carried out.

IT-960-TN31, *Configuration Management of System Security Baselines*, section 4, Procedures D, states, "If the system sponsor determines that their application will require deviations from the approved baseline, the system sponsor will identify where it is necessary to deviate from the Smithsonian baseline and provide a business case justification for accepting documented deviations as part of the system's compliance report. Follow the guidelines in IT-930-TN01, *IT Security Waivers and Exceptions*, to request a waiver or exception."

IT-930-TN01, IT Security Waivers and Exceptions defines a waiver as a temporary reprieve from a specific requirement pending corrective action, not to exceed one year. IT-930-TN01 further states that waivers must include compensatory measures that reduce risk during the waiver period. IT-930-TN01 defines an exception as an approved deviation from required policies/standards which cannot be met. When standards cannot be met, compensatory measures are required to provide security equivalent to the excepted policy standards. Exceptions are generally limited to systems that are unable to comply due to detrimental impact to mission, excessive costs, and/or commercial-off-the-shelf products that cannot be configured to support the control requirement. Exceptions will only be granted when compliance with a requirement would unduly impede mission performance, and when

alternative compensatory security measures will provide equivalent protection of the excepted security requirement(s).

Identity and Access Management Domain

We determined that the Smithsonian's Identity and Access Management domain was operating at Level 3, Consistently Implemented. Identity and Access Management was focused on ensuring access to physical and logical assets and associated facilities was limited to authorized users, processes, and devices, and its management was consistent with the assessed risk of unauthorized access to authorized activities and transactions.

We noted background checks were being completed for Smithsonian employees, contractors, and interns, or waivers were obtained when background checks could not be completed due to Coronavirus Disease 2019 (COVID-19) restrictions. Further, we noted two-factor authentication was being enforced and privileged/administrative accounts were being appropriately administered.

Data Protection and Privacy Domain

We determined that the Smithsonian's Data Protection and Privacy domain was operating at Level 4, Managed and Measurable. Data Protection and Privacy was focused on ensuring data, including privacy data were appropriately collected, processed, stored, and disposed of consistent with the organization's risk strategy and policy and procedures.

We noted that the Smithsonian's Privacy Office had a formal process in place to monitor the Smithsonian's compliance with documented privacy policy and procedures. Key monitoring activities by the Smithsonian Privacy Office were carried out using the Smithsonian's Governance, Risk, and Compliance tool and through regular participation in Technical Review Board meetings. Further, we noted the Smithsonian had formal breach response policies and procedures in place, as well as formal procedures in place to monitor breach response activities being carried out. Finally, we noted the Smithsonian had a formal process in place to deliver privacy training to individuals who regularly handled sensitive privacy data.

Castro did identify one issue within the Data Protection and Privacy domain related to privacy controls not being appropriately selected for the Evolution system. This issue is discussed within the Identify function, Risk Management domain, Smithsonian Assessment and Authorization Procedures Need Strengthening finding above.

Security Training Domain

Castro determined that the Smithsonian's Security Training domain was operating at Level 4, Managed and Measurable in FY 2021. Security Training was focused on ensuring the organization's personnel and partners were provided cybersecurity awareness education and were trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements.

In FY 2021, the Smithsonian had a comprehensive awareness and training program in place that included general security and privacy awareness training for all Smithsonian personnel, and specialized security and privacy training for individuals charged with security and privacy roles and responsibilities. Further, the Smithsonian had formal procedures and mechanisms in place to track completion of training and timely

follow up with individuals when training was not completed by identified due dates. At the time of our testing, over 99 percent of Smithsonian personnel had completed annual security awareness training.

Detect Function

Castro determined that the Smithsonian's Detect function was operating at Level 3, Consistently Implemented in FY 2021. 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 2021, we determined the Smithsonian had clearly identified which individuals were assigned with security roles and responsibilities. Further, we noted 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 dashboards 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 Information Technology environment.

While the Smithsonian did have formal Information Security Continuous Monitoring controls in place during FY 2021, we noted two issues with the implementation of those controls, which are discussed within the Risk Management function and below.

6. **SINet's Reauthorization to Operate Was Not Completed within Required Smithsonian Timeframes**

   Smithsonian Technical Standard & Guideline IT-930-03, *Security Assessment & Authorization*, section 12, Ongoing Assessment & Authorization, notes the authorization frequency of moderate systems should be every two years. Our testing noted SINet, which was categorized as a moderate system, was authorized to operate in August 2018 and then reauthorized in August 2021, which was three years after the previous authorization date. Per OCIO management, the individual within OCIO that was responsible for reauthorizing systems was likely unaware of the two-year requirement. We were informed that the OCIO's automated control within their Governance, Risk, and Compliance tool did not alert individuals that the ATO needed updating due to an incorrect ATO expiration date being entered.

Respond Function

Castro determined that the Respond function was operating at Level 4, Managed and Measurable in FY 2021. The Respond function is comprised of one domain, Incident Response.

Incident Response Domain

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 all seven Incident Response metric questions at Level 4, Managed and Measurable.

In FY 2021, we noted incident response activities were centrally managed by OCIO. Further, incident response plans were in place and tested for all systems in scope. The Smithsonian had a centralized Security Operations Center that monitored potential incidents and several key performance indicators in place to help evaluate whether incident response activities were being effectively carried out. Finally, the Smithsonian continued to refine Security Operations Center monitoring tools to further reduce the number of false positives being identified.

Recover Function

Castro determined that the Smithsonian's Recover function operated at Level 4, Managed and Measurable in FY 2021. The Recover function is comprised of one domain, Contingency Planning.

Contingency Planning Domain

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 2021, we noted the Smithsonian had formal contingency plans in place for systems in scope. Further, contingency plans were tested, and lessons learned were documented and provided to management.

Recommendations

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

1. Review and consider updating IT-930-02, *Security Control Manual*, to:
    a. Require control, AC-5 Segregation of Duties, for all moderate systems. Further, Smithsonian management should expand their current implementation of AC-5 to address both administrative and non-administrative accounts.
    b. Require control, AC-6 Least Privilege, for all moderate and high systems. Further, Smithsonian management should expand their current implementation of AC-6 to address both administrative and non-administrative accounts.
    c. Include control, AU-2 Auditable Events, for all low, moderate, and high systems.
2. Strengthen existing assessment and authorization procedures to ensure security controls are appropriately selected and control descriptions within system security plans are accurately documented and maintained.
3. Review and update the SINet system security plan where it is determined implementation statements do not accurately describe current controls in place. At a minimum, the SINet system owner should update implementation descriptions for the following controls, AC-6 Least Privilege, AC-17 Remote Access, IA-2 Identification and Authentication Organizational Users, IA-5 Authenticator Management, CP-3 Contingency Training, and SI-3 Malicious Code Protection.
4. Develop, document, and fully implement controls to ensure failures identified in baseline compliance scans are addressed in accordance with established Smithsonian policy.
5. Consider changing control CM-6 Configuration Settings, in the Smithsonian Security Control Manual from common to hybrid to better reflect and communicate responsibilities related to the management of security configuration baselines.

Castro has the following recommendations for the DAMS system owner related to the issued noted above:

6. Review and update the DAMS SSP where it is determined implementation statements do not accurately describe current controls in place. At a minimum, the DAMS system owner should update implementation descriptions for the following controls, AC-12 Session Termination.
7. Develop, document in the DAMS Configuration Management Plan, and implement formal procedures to ensure all changes to the DAMS application are appropriately tested, reviewed for potential security impact, and approved before implementation. Further, documentation of testing, security impact analysis, and approval should be documented and retained for future reference.

Castro has the following recommendations for the Evolution system owner related to the issued noted above:

8. Review and update the Evolution system security plan where it is determined implementation statements do not accurately describe current controls in place. At a minimum, the Evolution system owner should update the Evolution SSP to include physical and environmental security controls, the privacy and Enterprise HR or financial system overlays, and update AC-1 Account Management to accurately describe policy and procedures in place.
9. Develop, document, and implement formal procedures to ensure all changes to the Evolution application are appropriately tested, reviewed for potential security impact, and approved before implementation. Further, documentation of testing, security impact analysis, and approval should be documented and retained for future reference.

Appendix A - Acronyms

AC	Access Control
Castro	Castro & Company, LLC
CM	Configuration Management
COVID-19	Coronavirus Disease 2019
CP	Contingency Planning
DAMS	Digital Asset Management System
DHS	Department of Homeland Security
Evolution	Evolution, Payroll, HR and Time & Attendance System
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
HR	Human Resources
ICT	Information and Communications Technology
IR	Incident Response
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
POA&M	Plan of Actions and Milestones
R&D	Research and Development
SINet	Smithsonian Institution Network
SPO	Smithsonian Privacy Office
SSP	System Security Plan
STRI	Smithsonian Tropical Research Institute

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: May 19, 2022

To: Cathy L. Helm, Inspector General

From: Deron Burba, Chief Information Officer

DocuSigned by:
Deron Burba
3B7C612876EA474...

CC: Ron Cortez, Under Secretary for Administration
Douglas Hall, Senior Advisor
Judith Leonard, 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
Danee Gaines Adams, Privacy Officer
Carmen Iannacone, Chief Technology Officer
Fernando Bouche, STRI OIT Manager
Isabel Meyer, DAMS Branch Manager
Catherine Chatfield, Enterprise Risk Program Manager

Subject: Management Response to "R*eport on the Smithsonian Institution's Information Security Program Fiscal Year 2021*"

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

Recommendation 1: 1. Review and consider updating IT-930-02, Security Control Manual, to:

a. **Require control, AC-5 Segregation of Duties, for all moderate systems. Further, Smithsonian management should expand their current implementation of AC-5 to address both administrative and non-administrative accounts.**

b. **Require control, AC-6 Least Privilege, for all moderate and high systems. Further, Smithsonian management should expand their current implementation of AC-6 to address both administrative and non-administrative accounts.**

c. **Include control, AU-2 Auditable Events, for all low, moderate, and high systems.**

Management concurs with this recommendation. Management reviewed and evaluated the controls in this recommendation along with conducting a complete review of all control baselines, overlays, inheritances, assessment frequencies, and SI organization-defined control parameters for the control catalog. We have added AC-6 to the Moderate and High baselines and allocated that control to all the systems. We have assessed the separation of duties risks to our systems to determine which should require AC-5, extended the overlays to include this control wherever appropriate, and allocated AC-5 to the systems within these overlays, resulting in allocating this control to approximately 70% of the Moderate systems. For AU-2, rather than adding this as a separate control, we have added additional guidance to AU-01 to ensure that

the requirements of AU-02 are addressed in the system monitoring procedures and that this is assessed as part of AU-01. We believe this meets the intention of the AU-02 control without duplicating effort. Management considers this recommendation completed.

Recommendation 2: Strengthen existing assessment and authorization procedures to ensure security controls are appropriately selected and control descriptions within system security plans are accurately documented and maintained.

Management concurs with this recommendation. The System Risk Management Team Lead has implemented an increased level of scrutiny and now performs more stringent quality assurance checks for the security controls, implementation detail descriptions, and assessments. Additional guidance and training have been provided to the Information System Security Officers (ISSOs) on the creation of the implementation details and security control assessments based on Smithsonian policy. Weekly office hours have been implemented for the ISSOs to ask questions pertaining to implementation details, control assessments and authorization package support. Additional reports and key performance indicators have also been created to monitor these processes. These quality assurance activities have been added to the assessment and authorization procedure documentation. We have also reviewed all controls allocated to SI systems to verify their allocation status and inheritances. Additionally, as part of planning related to NIST 800-53 revision 5, we have performed a complete review of the control catalog, including all baselines, overlays, inheritance rules, assessment frequencies, organization-defined parameters, and additional SI instructions for the controls. Management considers this recommendation completed.

Recommendation 3: Review and update the SINet system security plan where it is determined implementation statements do not accurately describe current controls in place. At a minimum, the SINet system owner should update implementation descriptions for the following controls, AC-6 Least Privilege, AC-17 Remote Access, IA-2 Identification and Authentication Organizational Users, IA-5 Authenticator Management, CP-3 Contingency Training, and SI-3 Malicious Code Protection.

Management concurs with this finding. A thorough review and updating of the entire SINET authorization package has been conducted and all controls have been reviewed and updated. Additional quality assurance processes, as described in Recommendation 2, have been implemented to improve the accuracy of all implementation details. Management considers this recommendation completed.

Recommendation 4: Develop, document, and fully implement controls to ensure failures identified in baseline compliance scans are addressed in accordance with established Smithsonian policy.

Management concurs with this finding. The System Risk Management (SRM) Team Lead has worked with the Information System Security Officers (ISSOs) to review the baseline deviations for their systems and either correct them or obtain documented risk acceptance as appropriate. The SRM Team Lead has also started reviewing a monthly report generated by the compliance scans and is providing additional training and guidance to the ISSOs as needed. Additionally, baseline compliance has been added to the monthly Software Review Board and is being measured in the IT Security Key Performance Indicators. Significant work has been performed to review and resolve deviations, including documenting risk acceptance where appropriate, but there are still deviations that need to be remediated. We have also identified additional improvements that can be made to enhance the process. Management expects the remaining work to improve processes and ensure that all deviations have been addressed to be completed by January 31, 2023.

Recommendation 5: Consider changing control CM-6 Configuration Settings, in the Smithsonian Security Control Manual from common to hybrid to better reflect and communicate responsibilities related to the management of security configuration baselines.

Management concurs with this finding. Control CM-6 has been changed to Hybrid on all systems. Management considers this recommendation completed.

Recommendation 6: Review and update the DAMS SSP where it is determined implementation statements do not accurately describe current controls in place. At a minimum, the DAMS system owner should update implementation descriptions for the following controls, AC-12 Session Termination.

Management concurs with this finding. The implementation details for AC-12 have been updated for DAMS and the System Security Plan has been regenerated. Additional quality assurance processes, as described in Recommendation 2, have been implemented to improve the accuracy of all implementation details. Management considers this recommendation completed.

Recommendation 7: Develop, document in the DAMS Configuration Management Plan, and implement formal procedures to ensure all changes to the DAMS application are appropriately tested, reviewed for potential security impact, and approved before implementation. Further, documentation of testing, security impact analysis, and approval should be documented and retained for future reference.

Management concurs with this finding. While all changes to DAMS were being thoroughly evaluated, reviewed, tested and validated prior to production implementation, there was not complete documentation of the approvals as part of the process. An approval status has been added to [redacted] to ensure that all changes are approved by the Project Manager prior to implementation. The DAMS change management procedures and workflow have also been reviewed and updated. Management considers this recommendation completed.

Recommendation 8: Review and update the Evolution system security plan where it is determined implementation statements do not accurately describe current controls in place. At a minimum, the Evolution system owner should update the Evolution SSP to include physical and environmental security controls, the privacy and Enterprise HR or financial system overlays, and update AC-1 Account Management to accurately describe policy and procedures in place.

Management concurs with this finding. When these issues were pointed out during the audit, the PII overlay controls were added to the Evolution authorization package along with AC-05 Separation of Duties. The implementation details for AC-01 were also updated. Additionally, a [redacted] authorization package was created to document the physical and environmental security controls for the hosting facility in Panama, and the Evolution authorization package has been configured to inherit those controls instead of the ones provided by the [redacted] Additional quality assurance processes, as described in Recommendation 2, have been implemented to improve the accuracy of all implementation details. Management considers this recommendation completed.

Recommendation 9: Develop, document, and implement formal procedures to ensure all changes to the Evolution application are appropriately tested, reviewed for potential security impact, and

approved before implementation. Further, documentation of testing, security impact analysis, and approval should be documented and retained for future reference.

Management concurs with this finding. A new [redacted] Form, "Evolution Support Request", has been created to document the approvals and other related activities for change/support requests. The Change Management documentation has also been updated to reflect the new form and procedure. Management considers this recommendation completed.

For the recommendations that Management considers completed, evidence has been placed in the IG Evidence share.