In Brief

Information Security: Report on the Effectiveness of the Smithsonian Privacy Program and Practices, Fiscal Year 2022

OIG-A-23-02, November 30, 2022

Background

Each year, organizations face increasing threats to information systems and the sensitive data they handle. A common trend is for organizations to get attacked not only with ransomware, but also to get threatened with release of their sensitive data if they do not pay the ransom.

The Smithsonian Institution (the Smithsonian) collects, processes, stores, and transmits personally identifiable information (PII) of its employees, donors, and other members of the public. Its privacy inventory lists over [redacted] information systems handling PII, which include over [redacted] minor systems that handle sensitive PII, such as [redacted] Minor systems do not handle information critical to Smithsonian's mission.

What OIG Did

The Office of the Inspector General (OIG) contracted with an independent public accounting firm, Castro & Company, LLC (Castro), to assess the effectiveness of the Smithsonian Institution's (Smithsonian) privacy program and practices.

Castro reviewed the privacy assessments and other security documentation for five IT systems that handle sensitive PII (one major system and four minor systems).

What Was Found

Improvements in Smithsonian's Privacy Program.
Since the last audit of the privacy program in fiscal year 2015, the Smithsonian has taken a number of corrective actions, such as:

- Developed a privacy strategic plan that identifies key privacy goals and more detailed tasks to complete the identified goals.
- Completed a comprehensive review of its privacy holdings and developed a formal inventory of its electronic and hard-copy PII.
- Completed privacy impact assessments for all [redacted] systems.
- Implemented a process for Smithsonian units to evaluate their controls over hard-copy PII.

Minor Information Systems with Sensitive PII May Not be Secure.
Each information system that handles sensitive PII is required to have a privacy assessment that addresses the security controls for the system to ensure safeguards are in place to stop inappropriate uses and disclosure of the sensitive PII. However, Castro found that the Smithsonian has not taken sufficient steps to ensure that all minor information systems handling sensitive PII (over [redacted] at the time of testing) have appropriate security controls identified and in place. The Privacy Officer said that some of these minor systems that process credit card data are evaluated through the Payment Card Industry (PCI) Data Security Standards (DSS); but the PCI DSS evaluations are not integrated into the privacy assessments. Castro noted that the Office of the Chief Information Officer does not have a policy or process that requires security controls be identified and put in place for minor information systems that handle sensitive PII.

Policies and Procedures for Periodic Inventories of PII are Needed.
Smithsonian privacy policies and procedures do not describe how to perform periodic inventory reviews of the Smithsonian's PII holdings, such as how the Smithsonian verifies the accuracy of their current inventory or identifies new holdings of PII that should be added to the inventory. Comprehensive inventories of PII holdings are to be conducted every 3 to 5 years; the last one was in fiscal year 2018, and the next one is due to be completed in fiscal year 2023.

What Was Recommended

Castro made 3 recommendations to enhance security controls over sensitive PII: (1) clearly define how information systems are classified; (2) develop and implement a formal process to identify, document, and periodically test security controls for systems that handle sensitive PII; and (3) establish procedures for performing periodic inventories of PII. Smithsonian management concurred with the 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: November 30, 2022

To: Meroë Park, Deputy Secretary and Chief Operating Officer

Cc: Ron Cortez, Under Secretary for Administration
Rick Flansburg, Deputy Under Secretary for Administration
Deron Burba, Chief Information Officer
Danèe Gaines Adams, Smithsonian Privacy Officer
Juliette Sheppard, Director of IT Security
Carmen Iannacone, Chief Technology Officer
Catherine Chatfield, Enterprise Risk Program Manager

From: Cathy L. Helm, Inspector General

DocuSigned by:
Cathy Helm
FA013041C5054A3...

Subject: Information Security: Report on the Effectiveness of the Smithsonian Privacy Program and Practices, Fiscal Year 2022 (OIG-A-23-02)

This memorandum transmits the final audit report of Castro & Company, LLC (Castro) on the effectiveness of the Smithsonian's privacy program and practices. Under a contract monitored by this office, the Office of the Inspector General engaged Castro, an independent public accounting firm, to perform the audit.

Castro found that the Smithsonian has made significant progress in implementing a comprehensive privacy program since the last audit of the privacy program in fiscal year 2015. Also, additional improvement is needed to ensure information security controls over sensitive personally identifiable information (PII) are appropriately identified, documented, and implemented to stop inappropriate uses and disclosure of the sensitive PII. Castro made three recommendations to enhance controls over sensitive PII, and management concurred with all 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 Effectiveness of the Smithsonian Privacy Program and Practices

Fiscal Year 2022

Contents

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 privacy program and practices of the Smithsonian Institution (Smithsonian) for the fiscal year ending September 30, 2022.

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 privacy program and practices. Smithsonian management has provided us with a response to this 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

November 29, 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) privacy program and practices. Threats to information systems and the sensitive data organizations collect, process, store, and transmit continue to increase each year. According to Identity Theft Resource Center's 2021 Data Breach Report, there were 1,862 breaches last year, up 68 percent from the year prior, and exceeded 2017's previous record of 1,506. Cyber-criminal activities such as denial-of-service and ransomware attacks continue to be a significant risk to organizations. A common trend over the past several years saw organization's not only get attacked with ransomware, but also get threatened with release of their sensitive data including in many cases sensitive privacy data if they did not pay the ransom. As organizations move more of their activities online, and the amount of data processed increases, the challenges around identifying, tracking, and protecting the sensitive systems and data within an organization can become both a significant challenge and risk.

The Smithsonian is no different, with a large number of museums, research facilities, and archives spread throughout the United States and Panama, the risks and challenges around identifying and protecting sensitive Personally Identifiable Information can be significant. The Smithsonian collects and handles personally identifiable information (PII) of both its employees and members of the public, including children. If the Smithsonian fails to adequately safeguard this information, it could suffer significant financial and reputational damages. To manage these risks, the Smithsonian must have a comprehensive and effective privacy and cybersecurity risk management program in place.

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, not required to comply with many federal privacy and information security laws such as the Privacy Act of 1974 and Federal Information Security Modernization Act of 2014. However, the Smithsonian has adopted many of these standards and incorporated them into their policies.

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, 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.

Smithsonian Privacy Office

The Smithsonian Privacy Office, located within the Office of the Chief Information Officer (OCIO), is charged with safeguarding the PII 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 Smithsonian Privacy Office develops and enforces privacy policies and procedures that are carried out by the Smithsonian units, and reviews and is responsible for approving all collections of PII and sensitive PII. The Smithsonian Privacy Officer, who heads the Smithsonian Privacy Office, reports directly to the Chief Information Officer.

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, 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.

Objectives, Scope and Methodology

Castro was contracted by the Smithsonian OIG to evaluate the effectiveness of the Smithsonian's privacy program and practices. 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.

Castro's privacy audit scope was based on security and privacy requirements within the Smithsonian's policies and procedures and federal privacy best practices. Our methodology was developed using privacy controls located in National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organization* (Appendix J), NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*; and Office of Management and Budget memorandums related to privacy. In September 2020, NIST released Special Publication 800-53 Revision 5, *Security and Privacy Controls for Federal Information Systems and Organization.* Revision 5 eliminated Appendix J and incorporated the privacy controls into the other control families within the document. Castro reviewed the changes made in Revision 5 and incorporated those changes into the scope of this audit, where they were determined to be appropriate.

During the planning phase of our audit, we determined that the NIST 800-53 Revision 4 security controls were significant and relevant to our audit objectives. For each of the controls that we considered significant and relevant to our audit objectives, we gained an understanding of their design and how they were placed in operation by the Smithsonian. We then developed audit plans for each in-scope internal control and tailored audit steps based on our understanding of the Smithsonian's operations.

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*.[1] 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.

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

To assist in determining the significance of the controls determined to be significant and included in scope for our testing, we mapped each of the controls as listed in the NIST Special Publication 800-53 Revision 5, to the five components of internal control. This allowed us to group our testing and conclusions on control effectiveness to the recommended components of internal control outlined in the Standards for Internal Controls in the Federal Government and to meet government auditing standards' reporting requirements.

Further, when developing our audit scope, we reviewed key Smithsonian privacy and security policies and procedures to identify requirements for testing. Smithsonian policies and procedures reviewed in the development of our audit scope included:

- Smithsonian Directive 118, *Privacy Policy*, September 15, 2020
- Smithsonian Directive 118, *Privacy Program Handbook*, September 15, 2020
- Smithsonian Directive 119, *Privacy Breach Policy*, April 20, 2021
- Smithsonian Directive 119, Appendix, *Privacy Breach Reporting and Notification Process*, April 20, 2021
- Technical Standard & Guidelines IT-930-03, *Security Assessment & Authorization*, June 3, 2021
- Technical Standard & Guidelines IT-930-02, *Security Controls Manual*, June 2020

To evaluate the effectiveness of the Smithsonian's privacy program and practices, Castro's audit methodology included conducting interviews and reviewing available supporting documentation. We conducted interviews with multiple offices and personnel within the Smithsonian, including:

- Privacy Office,
- Office of the Chief Information Officer,
- Office of the General Counsel,
- Office of Contracting and Personal Property Management,
- Individuals responsible for Smithsonian's compliance with Payment Card Industry Data Security Standards.

At the time of our testing, the Smithsonian's privacy inventory included over [redacted] IT systems that handled Personally Identifiable Information. We noted over [redacted] of these systems were identified as handling sensitive Personally Identifiable Information such as [redacted]. We reviewed privacy assessments and any other available security documentation for five of the information systems that were identified in the Privacy Office's Personally Identifiable Information inventory. These information systems included:

1. [redacted] **(Privacy Assessment** [redacted] – [redacted]
2. [redacted] **(Privacy Assessment** [redacted] - [redacted]
3. [redacted] **(Privacy Assessment** [redacted] – [redacted]

4. [redacted] **(Privacy Assessment [redacted] –** [redacted]

5. [redacted] **(Privacy Assessment [redacted] –** [redacted]

Documentation reviewed during our audit included organization charts, the Smithsonian's inventory of PII, completed privacy assessments,[2] privacy notices, privacy training materials, and documentation supporting the Smithsonian's payment card industry compliance effort. Our audit evaluated compliance with Smithsonian privacy and security requirements and their general alignment with federal and industry privacy best practices.

Audit Results

Since that last audit of the privacy program in fiscal year 2015, the Smithsonian has taken corrective action on a number of issues, including:

- Developed a privacy strategic plan that identifies key privacy goals and more detailed tasks to complete the identified goals.
- Completed a comprehensive review of its privacy holdings and developed a formal inventory of its PII in both electronic and hard-copy form.
- Completed privacy impact assessments for all [redacted] systems and is currently transitioning completed Privacy Impact Assessments to a new Privacy Assessment process and template that covers both hardcopy and electronic collections of PII. As of November 3, 2021, the Smithsonian Privacy Office had:
    - Started and/or completed privacy assessments for [redacted] IT systems,
    - Started and/or completed privacy assessments for [redacted] hardcopy systems,
    - Not yet started privacy assessments for [redacted] IT systems,
    - Not yet started privacy assessments for [redacted] hardcopy systems
- Developed and implemented annual privacy-specific role-based training and a process to identify individuals who should complete privacy training.
- Implemented a process for Smithsonian Units to evaluate their controls over hard-copy PII.
- Developed and maintained privacy policies and procedures in accordance with Smithsonian requirements.

While the Smithsonian has made significant progress in implementing a comprehensive privacy program, we noted additional improvement is needed to ensure security controls over sensitive PII are appropriately identified, documented, and implemented. We have identified deficiencies in internal control that are

[2] The Smithsonian's PII inventory was comprised of over [redacted] information systems that collected, processed, stored, or transmitted PII. We judgmentally selected a sample of five (5) information system privacy assessments for testing.

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, as detailed in the sections below.

A. Minor Information Systems with Sensitive Personally Identifiable Information May Not be Secure

We found that the Smithsonian has not taken sufficient steps to ensure all minor information systems (over [redacted] at the time of testing) that collect, process, store, and transmit sensitive PII have appropriate security controls identified and in place. According to the Privacy Officer, some of the minor information systems process credit card data and therefore are assessed through the Payment Card Industry (PCI) Data Security Standards (DSS) process; however, privacy assessments do not require that the security controls reviewed under the PCI DSS process be included in the assessments to ensure safeguards are in place to stop inappropriate uses and disclosure of the sensitive PII.

We noted that the Smithsonian Privacy Office completes a privacy assessment for each information system that is identified as collecting, processing, storing, or transmitting sensitive PII. Further, while the Smithsonian, Privacy Officer noted security controls for systems handling sensitive PII are supposed to be addressed in Section 9 (Physical, Administrative, and Technical Controls) of the privacy assessment, our review of four privacy assessments showed that two did not address security controls at all and the other two addressed controls only at a very high level.

For two minor information systems, we noted that the privacy assessments did not address physical, administrative, and technical IT security controls. The two systems were: (1) [redacted] that [redacted] and (2) [redacted] that [redacted] According to the Smithsonian Privacy Officer, this section of the privacy assessments were not completed because these minor systems are [redacted]

For the other two systems, we noted that the privacy assessments addressed physical, administrative, and technical IT security controls at a very high level but did not describe how these controls were to be implemented. For the [redacted], the privacy assessment listed certain types of controls such as [redacted], but it did not describe how these controls were to be implemented. [redacted] For the [redacted] system, the privacy assessment did not adequately describe how security controls were implemented. It only listed the types of controls in place such as [redacted]

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

[redacted] rather than describing how these controls were implemented.

For the four minor information systems noted above, we requested any additional documentation from OCIO that may describe security controls in place and were informed that minor applications are not required to follow the Smithsonian's assessment and authorization process outlined in Smithsonian Technical Standards & Guidelines, IT-930-03, and therefore, not required to have system security plans or security documentation in place. Further, while OCIO management stated there may be additional information available from the Technical Review Board process,[4] we noted that the Smithsonian did not have formal policies or procedures requiring the Technical Review Board to identify and document security controls for minor systems.

Finally, while OCIO did provide a minor application security plan for one of the four minor systems ([redacted]), we noted the system security plan, which is typically required to be updated annually, was last updated in fiscal year 2017. OCIO informed us that the minor system security plan was originally used as part of the Technical Review Board process but had since been discontinued.

Lastly, IT-930-03 states that major applications are "Systems that require special management oversight because of the information they contain, process, store, or transmit, or because of their criticality to the Institution's mission", we noted that the Smithsonian does not consider this definition to include systems processing sensitive privacy data. As a result, the Smithsonian does not have a policy or process in place that requires security controls be identified and put in place for minor information systems that collect, process, store, or transmit sensitive PII.

B. Detailed Policies and Procedures for Performing Periodic Inventories of Personal Identifiable Information are Needed

Smithsonian privacy policies and procedures do not describe how to carry out or perform periodic inventory reviews of the Smithsonian's PII holdings, such as how the Smithsonian verifies the accuracy of their current inventory or identifies new holdings of PII that should be added to the inventory. Smithsonian Directive (SD) 118, *Privacy Policy*, and SD 118, *Privacy Program Handbook*, state the Privacy Office is responsible for conducting inventories of the Smithsonian's PII holdings every three to five years and reference a comprehensive inventory of PII that was conducted in fiscal year 2018, but they do not describe how a comprehensive PII inventory review should be carried out. Therefore, the next inventory is due to be completed in fiscal year 2023.

NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*, states, "Organizations should develop comprehensive policies and procedures for protecting the confidentiality of PII." Comprehensive policy and procedures should include clear procedures on how an inventory of PII is developed and maintained.

Without formally documented procedures that describe how to carry out key activities including periodic inventory reviews of the Smithsonian's PII holdings, the risk of those activities being carried out incorrectly or incompletely increases. In addition, a full and comprehensive inventory of PII, helps management to ensure that appropriate controls are in place to protect sensitive PII throughout the Smithsonian. Further,

[4] The Technical Review Board acts as an IT governance board responsible for improving the overall level of project success, system quality and productivity by ensuring that IT project risks are reduced to an acceptable level. The Technical Review Board ensures Smithsonian IT life cycle management processes are followed including privacy analysis and security issue identification and remediation.

while OCIO management stated the process used to carry out the fiscal year 2018 PII Inventory is described within the *Smithsonian Privacy Office's Smithsonian-wide Inventory of Personally Identifiable Information, Final Report*, we noted this report is not part of the Smithsonian's formal privacy policy and procedures[5]. For example. procedures should discuss how the Smithsonian Privacy Office identifies new instances of PII throughout the Smithsonian, whether through interviews, surveys, reviews of existing documentation, or other means. Additionally, procedures should clearly describe how selected methods (interview, survey, documentation review) will be designed and carried out. For example, if doing a survey, who will be included in the survey and what will the survey questions focus on.

Recommendations:

Castro recommends that the Chief Information Officer take the following actions:

1. Update IT-930-03 to clearly define how information systems are classified as either major or minor and whether the sensitivity of data is to be considered.

2. Develop and implement a formal process to identify, document, and periodically test, security controls for all systems (major or minor) that collect, process, store, or transmit sensitive personally identifiable information. Where systems processing sensitive PII are considered minor, documentation should clearly identify what controls are being inherited from other systems and what controls are specific to the system.

Castro recommends that the Smithsonian Privacy Officer:

3. Update the existing privacy directive to establish procedures for how periodic reviews of personally identifiable information will be conducted and by whom.

[5] Booz Allen Hamilton Inc., *Smithsonian-Wide Inventory of Personally Identifiable Information (PII),* Final Report, In Support of Closing Inventory-Related Finding from the FY15 Audit Report of the Smithsonian Institution's Privacy Program, November 20, 2017 – August 31, 2018.

Appendix A - Acronyms

Castro	Castro & Company, LLC
DSS	Data Security Standards
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
PCI	Payment Card Industry
PII	Personally Identifiable Information
SD	Smithsonian Directive
Smithsonian	Smithsonian Institution
SSP	System Security Plan

Appendix B – Prior Audit Reports

- *Audit of the Smithsonian Institution's Privacy Program*, (OIG-A-16-4, March 14, 2016).
- *Report on the Fiscal Year 2008, Audit of the Smithsonian Institution's Privacy Program*, (A-08-8, May 29, 2009).

Appendix C – 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 C. Castro & Company did not audit management's response and, accordingly, do not express any assurance on it.

Smithsonian Institution Memo

Office of the Chief Information Officer
Privacy Office

Date: November 4, 2022

To: Cathy L. Helm, Inspector General

From: Danee Gaines Adams, Smithsonian Privacy Officer

DocuSigned by:
Danee Gaines Adams
755EDCDF62F4493...

CC: Ron Cortez, Under Secretary for Administration
Rick Flansburg, Deputy Under Secretary for Administration
Greg Bettwy, Chief of Staff, Office of the Secretary
Deron Burba, Chief Information Officer
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
Carmen Iannacone, Chief Technology Officer
Catherine Chatfield, Enterprise Risk Program Manager

Subject: Management Response to the "*Draft Report of the Audit of the Effectiveness of the Smithsonian Privacy Program and Practices*"

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

Recommendations:

Castro recommends that the Chief Information Officer take the following actions:

1. **Update IT-930-03 to clearly define how information systems are classified as either major or minor and whether the sensitivity of data is to be considered.**

   Management concurs with this recommendation. IT-930-03 has been updated to clarify the requirements for classifying a system as a major application or minor application. Management considers this to be completed.

2. **Develop and implement a formal process to identify, document, and periodically test, security controls for all systems (major or minor) that collect, process, store, or transmit sensitive personally identifiable information. Where systems processing sensitive PII are considered minor, documentation should clearly identify what controls are being inherited from other systems and what controls are specific to the system.**

   Management concurs with this recommendation. We will review and update our procedures to ensure that any gaps in performing these activities are addressed and to clarify how these processes are being performed for minor systems.

   Expected completion: October 31, 2023

Castro recommends that the Smithsonian Privacy Officer:

3. **Update the existing privacy directive to establish procedures for how periodic reviews of personally identifiable information will be conducted and by whom.**

   Management concurs with this recommendation. We will review and update the existing privacy directive to ensure it reflects how periodic reviews of personally identifiable information will be conducted and by whom.

   Expected completion: October 31, 2023

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