Smithsonian Institution
Office of the Inspector General

In Brief

Audit of the Smithsonian Institution’s Privacy Program

Report Number OIG-A-16-4, March 14, 2016

What OIG Did

The Office of the Inspector General (OIG) contracted with an independent public accounting firm, Cotton & Company, to conduct this performance audit. The objective of the audit was to assess the effectiveness of the Smithsonian Institution’s (Smithsonian) privacy program and practices.

Background

New privacy threats emerge daily, and the evolving nature of these threats makes it challenging to continually evaluate the measures needed to address risks to personally identifiable information. The increasing mobility of data significantly escalates the already difficult task of identifying where sensitive personally identifiable information is located and effectively securing it. Digital issues are not the only threat; about a quarter of the data-leakage incidents reported by large agencies involved the loss of sensitive information from hard copies or printed materials.

Due to these challenges and because it operates in a decentralized environment, it is critical for the Smithsonian to have a well thought out and comprehensive privacy program in place.

What OIG Found

Cotton & Company found that the Smithsonian has made progress in privacy management since the last OIG privacy audit in May 2009. For example, in 2014 the Smithsonian hired a new Privacy Officer, implemented a new privacy policy, and formed working groups to identify and address privacy issues.

However, Cotton & Company determined that significant work is still needed to institute key privacy processes and controls. For example, key activities that have not been completed include developing an organization-wide privacy strategic plan and documenting a comprehensive list of personally identifiable information being collected, processed, and stored throughout the Smithsonian. Without a clear understanding of the types of personally identifiable information being handled, management officials do not have reasonable assurance that they are collecting only the information needed to carry out the Smithsonian’s mission and are adequately protecting that information from unauthorized use or disclosure. Additionally, Cotton & Company noted that the Smithsonian Privacy Office consists of one employee, the Privacy Officer, who supports 6,373 employees, 721 research fellows, and 9,817 volunteers.

To improve the privacy program, Cotton & Company found that:

- The Smithsonian needs a strategic privacy plan,
- The Smithsonian needs to develop a comprehensive inventory of personally identifiable information,
- The Smithsonian’s privacy impact assessment process needs improvement,
- The Smithsonian’s security awareness and privacy training need improvement,
- The Smithsonian needs to improve physical controls over personally identifiable information, and
- The Smithsonian needs to review and update privacy policies.

What OIG Recommended

Cotton & Company made 11 recommendations to address the findings listed above. Smithsonian management concurred with the recommendations and has proposed corrective actions to address them.

For additional information or a copy of the full report, contact OIG at (202) 633-7050 or visit http://www.si.edu/oig.

REPORT ON THE
FY 2015 INDEPENDENT AUDIT OF THE
SMITHSONIAN INSTITUTION PRIVACY PROGRAM
SMITHSONIAN INSTITUTION
PREPARED FOR THE OFFICE OF THE INSPECTOR GENERAL

MARCH 14, 2016

Cotton & Company LLP
635 Slaters Lane
Alexandria, Virginia 22314
703.836.6701 | 703.836.0941, fax
gbills@cottoncpa.com | www.cottoncpa.com

Cotton&
Company

Cotton & Company LLP
635 Slaters Lane
4th Floor
Alexandria, VA 22314

P: 703.836.6701
F: 703.836.0941
www.cottoncpa.com

March 14, 2016

To: Cathy L. Helm, Inspector General
Office of the Inspector General
Smithsonian Institution

Subject: Independent Performance Audit Report on the Smithsonian Institution's Privacy Program

Cotton & Company LLP is pleased to submit this independent performance audit report on its audit of the Smithsonian Institution's privacy program. Cotton & Company performed the work from June through August 2015.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards, as amended, promulgated by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Overall, management concurred with our recommendations. Management's written comments on our findings and recommendations can be found in Appendix I.

Sincerely,
Cotton & Company LLP

George E Bills

George E. Bills, CPA, CISSP, CISA, CIPP
Partner, Information Assurance

TABLE OF CONTENTS

ABBREVIATIONS

GAPP	Generally Accepted Privacy Principles
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PTA	Privacy Threshold Analysis
SD	Smithsonian Directive
SInet	Smithsonian's general support system
SP	Special Publication
SPO	Smithsonian Privacy Officer

INTRODUCTION

New privacy threats emerge on a daily basis, and the evolving nature of these threats is challenging government institutions to continually evaluate the measures they are taking to address risks to the personally identifiable information (PII) that they maintain, in both hard-copy and digital format. The increasing mobility of data (e.g., the cloud, mobile devices, flash drives) and the implementation of bring-your-own-device practices (e.g., the use of personal smartphones or tablet devices) within federal institutions significantly escalate the already difficult task of identifying where sensitive PII information (e.g., social security numbers, bank account numbers, passport information, healthcare-related information, credit card numbers, state ID) is located and effectively securing it. In addition, digital issues are not the only threat; the annual Federal Information Security Management Act report showed that about a quarter of the data-leakage incidents reported by large agencies in 2014 involved the loss of sensitive information from hard copies or printed materials, not digital records.[1]

With all of these challenges, as well as a decentralized environment, it is critical for the Smithsonian Institution (the Smithsonian) to have a well-thought-out and comprehensive privacy program in place.

OBJECTIVE

Cotton & Company LLP conducted an independent performance audit of the effectiveness of the Smithsonian's privacy program and practices. This report presents the results of the audit, based on work performed by Cotton & Company.

Scope

Cotton & Company conducted this 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 objective. We believe that, based on the objectives of this audit, the evidence obtained through our review of the Smithsonian's Privacy Program provides a reasonable basis for our findings and conclusions.

The scope of our audit was inclusive of the Smithsonian and all its divisions, including Smithsonian Enterprises. We conducted testing at Smithsonian offices in Washington, D.C. and Arlington, Virginia, from June to August 2015, and reporting concluded in December 2015.

Methodology

Our audit methodology was based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Appendix J: Privacy Controls; NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*; and Office of Management and Budget (OMB) memorandums related to privacy. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets.[2] Additionally, Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36) requires that OMB issue guidance to agencies on implementing the privacy provisions of the E-Government Act.[3] These documents outline federal privacy best practices for developing and

[1] OMB, *Annual Report to Congress: Federal Information Security Management Act*, February 27, 2015.
[2] NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010.
[3] OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003.

implementing a privacy program, and identifying and reducing, where appropriate, the collection and handling of sensitive PII. We recognize that the Smithsonian is not a federal agency, and that it based its privacy policy on the American Institute of Certified Public Accountants ten Generally Accepted Privacy Principles (GAPP).[4] However, the criteria we used for this audit are representative of best practices for managing a privacy program and securing PII, regardless of the type of entity or the privacy data they handle.

To accomplish our audit objective, Cotton & Company interviewed Smithsonian personnel associated with the Smithsonian's Privacy Office, Office of the Chief Information Officer (OCIO), and administrative units that handle PII. Further, we reviewed five information systems in our testing that, per the OCIO and SPO, contained PII.[5] Additionally, the audit team reviewed documentation related to the Smithsonian's privacy and information security program, such as privacy policies and procedures, security awareness training material, internal and external web pages including referenced privacy notices, and privacy incident reports. These activities were performed to evaluate compliance with Smithsonian requirements, as well as federal requirements that represent best practices.

SUMMARY OF RESULTS

The Smithsonian has made progress in privacy management since the last privacy audit.[6] In 2014 the Smithsonian hired a new Privacy Officer, implemented a new privacy policy, and formed working groups to identify and address privacy issues.

However, we determined that significant work is still needed to institute key privacy processes and controls. For example, two key activities that have not been completed include developing an organization-wide privacy strategic plan and documenting a comprehensive list of PII being collected, processed, and stored throughout the Smithsonian. Without a clear understanding of the types of PII being handled, management lacks reasonable assurance that they are only collecting PII needed to carry out the Smithsonian's mission and are adequately protecting that PII from unauthorized use or disclosure. Additionally, we noted that the Smithsonian Privacy Office consists of one employee, the Smithsonian Privacy Officer, who supports 6,373 Smithsonian Employees, 721 Research Fellows, and 9,817 Volunteers.[7]

To improve its privacy program, we found that:

- The Smithsonian needs a strategic privacy plan,
- The Smithsonian needs to develop a comprehensive inventory of PII,
- The Smithsonian's privacy impact assessment process needs improvement,
- The Smithsonian's security awareness and privacy training need improvement,
- The Smithsonian needs to improve physical controls over PII, and
- The Smithsonian needs to review and update privacy policies.

[4] Smithsonian Directive (SD) 118, *Privacy Policy*, March 11, 2014. The 10 GAPP principles are: management; notice; choice and consent; collection; use, retention, and disposal; access; disclosure to third parties; security for privacy; quality; and monitoring and enforcement.

[5] The five systems were the Smithsonian's general support system, Pan-Institutional Database for Advancement, Medgate, Raiser's Edge, and Enterprise Resource Planning.

[6] Smithsonian OIG, A-08-08, *FY2008 Audit of Smithsonian Institution's Privacy Program*, May 29, 2009.

[7] The Smithsonian internet site (http://www.si.edu/About), October 13, 2015.

AUDIT FINDINGS AND RECOMMENDATIONS

A. The Smithsonian Needs a Strategic Privacy Plan

The Smithsonian Privacy Office has not developed a formal strategic privacy plan to guide the organization through the process of identifying privacy risks and defining how it will develop and implement privacy policies, procedures, and practices to minimize those identified risks. This is in contrast to a key NIST publication,[8] which recommends that agencies have a strategic privacy plan for implementing applicable privacy controls, policies, and procedures as well as update it at least biennially. The strategic privacy plan should lay out the vision for how the Smithsonian will protect the privacy of its employees, visitors, and volunteers. A plan also should establish a roadmap for achieving that vision, including goals, objectives, and milestones.

The Smithsonian Privacy Officer (SPO) has identified certain areas where personally identifiable information is being maintained and utilized by the Smithsonian. Additionally, the SPO has implemented some initiatives to address privacy risks based on a Smithsonian-wide risk assessment, which identified privacy protection as one of the Institution's top 15 risk areas. In September 2015, after the completion of our testing, the SPO provided a draft copy of a privacy strategic plan for fiscal year 2016.

Without a formally documented organization-wide strategic privacy plan in place, which clearly identifies privacy risks throughout the organization and controls that can mitigate those risks to an acceptable level, management cannot be reasonably sure they are using their limited privacy resources in the most efficient and effective manner. In addition, management may be unaware of existing privacy risks.

Recommendation:

1. We recommend that the Smithsonian Privacy Officer finalize a strategic privacy plan.

B. The Smithsonian Needs to Develop a Comprehensive Inventory of PII

The Smithsonian Privacy Office has not developed a comprehensive inventory of the PII it has collected, processed, and stored in both electronic and hard-copy formats. This is in contrast to a key NIST publication,[9] which recommends that management establish, maintain, and update an inventory of all programs and information systems identified as collecting, using, maintaining, or sharing PII.

The Smithsonian also lacks controls to ensure that it identifies and minimizes its collection, processing, and storage of PII. Reducing holdings of PII is a best practice recommended by both NIST[10] and OMB.[11] NIST advises that PII be collected and retained only as necessary to accomplish the legally authorized purpose. OMB advises agencies to review their current holdings of all PII and ensure such holdings are accurate, relevant, timely, and complete, and reduce them to the minimum necessary for the proper performance of a documented agency function.

[8] NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organization*, Control AR-1: Governance and Privacy Program, April 2013.

[9] NIST SP 800-53 R4, Control SE-1: Inventory of Personally Identifiable Information, April 2013.

[10] NIST SP 800-53 R4, Control DM-1: Minimization of Personally Identifiable Information, April 2013.

[11] OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* Section B – 1 Privacy Requirements, May 22, 2007.

The Smithsonian has not conducted a comprehensive review to ascertain all locations within the Smithsonian where PII, in both electronic and hard-copy format, is being handled. Additionally, without a complete understanding of PII in use at the Smithsonian, including what the PII is used for, where it comes from, what format it is in, and how it is secured, the Smithsonian cannot effectively determine where it can reduce the collection of PII, as NIST and the OMB recommend. The Smithsonian has not made it a high priority to create an inventory of PII or develop a plan to reduce PII holdings. Accordingly, the likelihood increases that PII has not been identified and adequate controls over the PII are not in place.

Recommendations: We recommend that the Smithsonian Privacy Officer:

2. Strengthen management of the Smithsonian's PII holdings by:
   - A. Developing a formal process to periodically conduct a comprehensive inventory of PII used by the Smithsonian.
   - B. Documenting a comprehensive inventory of PII used by the Smithsonian.
3. Develop and implement a plan to reduce PII holdings where possible.

C. The Smithsonian Privacy Impact Assessment Process Needs Improvement

The Smithsonian does not have adequate controls in place to ensure privacy impact assessments (PIA) are completed for Smithsonian information systems containing PII. The objective of the PIA is to systematically identify the risks and potential effects of collecting, maintaining, and disseminating PII and to examine and evaluate alternative processes for handling information to mitigate potential privacy risks. Additionally, a privacy threshold analysis (PTA) may be used first to determine whether a PIA should be completed. The PTA is a precursor, self-assessment tool that can be used by agencies to determine whether they properly maintain PII. The PTA includes a description of the system and what PII, if any, is collected or used, and from whom.

NIST recommends that agencies conduct PIAs for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.[12]

Specifically, we requested PIAs for the Smithsonian's general support system (SInet) and four other systems[13] that we were informed contained PII, such as information on employee health, donors, and vendors. We noted the following issues:

- SInet, the Smithsonian's general support system structure, which includes both network shared drives and email, does not have a completed PIA. We noted that the Smithsonian Office of the Chief Information Officer (OCIO) stated that SInet does not contain PII. However, through our interviews with the Smithsonian Office of Human Resources and the Office of Finance and Accounting officials, we noted that PII is maintained on shared drives and within email, which is part of the SInet system boundary.

[12] NIST SP 800-53 R4, Control AR-2: Privacy Impact and Risk Assessment, April 2013

[13] The four systems were Pan-Institutional Database for Advancement, Medgate, Raiser's Edge, and Enterprise Resource Planning.

- While we received PTAs for two of the five systems, the Smithsonian was unable to provide PIAs for any of the five systems in our scope.

Prior to May 2014, the PIA assessment process was managed by OCIO as part of the system Certification and Authorization process for evaluating, describing, testing, and authorizing systems. However, the SPO now handles this process. An oversight in this transition of ownership could have led to the inability to provide requested PIA documentation. Further, the Smithsonian does not have a comprehensive list of all systems, which identifies whether a PIA is required. Finally, even though PII is stored in shared drives and email on SInet, the SPO has not required SInet to undergo a PIA. Since the SPO did not accurately perform the SInet PTA, a PIA for this system was not required.

Weak controls over the privacy impact assessment process increase the risk that information systems containing sensitive PII will not be appropriately identified and evaluated, to ensure collection of PII is appropriate and adequate controls are in place to protect the confidentiality of the PII.

Recommendations: We recommend that the Smithsonian Privacy Officer:

4. Strengthen existing policies and procedures used to identify all systems requiring a PIA.
5. Create a central repository for all PIAs.
6. Ensure a PIA is completed for all Smithsonian information systems containing PII.

D. The Smithsonian Security Awareness and Privacy Training Needs Improvement

The Smithsonian does not have adequate controls to ensure all personnel receive appropriate privacy training. Specifically, we noted that targeted, role-based privacy training is not provided to employees and contractors who handle PII as part of their daily job responsibilities. This is in contrast to a key NIST publication,[14] which recommends agencies administer and certify both basic and targeted role-based privacy training, at least annually, for personnel having responsibility for PII or for activities that involve PII.

We noted that the Smithsonian has annual security awareness training that includes slides related to privacy; however, this training is only required for individuals with a Smithsonian network (SInet) account. As such, users with access to PII but without an SInet account (e.g., volunteers, maintenance, and janitorial services with access to hard-copy PII) may not receive privacy awareness training. This is in contrast to a key OMB publication,[15] which requires that all employees and contractors, regardless of whether they have network accounts, receive annual security and privacy awareness training.

The SPO is currently developing targeted, role-based privacy training for individuals who handle sensitive PII; however, this training has not been finalized and implemented.

The Smithsonian OCIO relies on its network account management process to identify individuals for security awareness training, which includes privacy training. When an individual is granted a network account, they are added to the training system, which identifies and tracks them until training is completed. As such, employees who are not network users do not receive annual privacy training. This

[14] NIST SP 800-53 R4, Control AR-5: Privacy Awareness and Training, April 2013.

[15] Stated in OMB Memorandum 04-14, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Training Question 53, November 18, 2013.

training issue was identified, specifically for volunteers, in a prior OIG report.[16] In October 2015, after the conclusion of our fieldwork, the OIG closed this recommendation upon its conclusion that corrective actions by OCIO addressed the deficiency. As a result, we are not making a recommendation related to this issue.

The Smithsonian increases its risk of PII being inappropriately collected, processed, or stored because it lacks a formal privacy training program. All Smithsonian employees who have access to PII (including those employees and volunteers that do not have a network account) need training. Targeted role-based privacy training is necessary for those employees that handle PII on a daily basis.

Recommendations:

7. We recommend that the Smithsonian Privacy Officer finalize and implement targeted, role-based privacy training for individuals who handle PII.
8. We recommend that the Smithsonian Privacy Officer formally identify and track individuals who are required to take targeted, role-based training to ensure they complete that training.

E. The Smithsonian Needs to Improve Physical Controls Over Sensitive Personally Identifiable Information

We identified instances where Smithsonian employees had not taken adequate steps to safeguard PII and passwords. Specifically, we performed three after-hour walkthroughs of select Smithsonian offices and noted the following instances where hard-copy PII and passwords were left in the open:

- Eight instances where passwords were found written on sticky notes and left in open view on a desks,
- File folders containing PII and applications for credentials were found on a desk,
- A time-and-attendance binder containing six-month-old timesheets that had names and social security numbers was found in an open and unlocked room,
- A Paper Declaration for Federal Employment document containing PII was found on a desk,
- A Retirement System Adjustment Worksheet containing PII was found in an unlocked desk cabinet, and
- Multiple badges of employees were found on their desks in open view.

These employees were not complying with existing Smithsonian policy, which states that PII on paper should be reasonably protected from unauthorized access,[17] and that passwords should not be left in writing in the user's office.[18]

Additionally, the Smithsonian does not have a formal process in place to periodically test compliance with physical controls over PII and passwords. This is in contrast to a key NIST publication,[19] which

[16] Smithsonian OIG, A-13-10, *FY 2013 Evaluation of the Smithsonian Institution's Information Security Program*, July 9, 2014.

[17] Smithsonian Technical Note, *IT-930-TN26 – Media Protection Policy and Procedures*, October 17, 2006. SD 118, Privacy Program Handbook, June 16, 2014.

[18] SD 931, *Use of Computers, Telecommunications Devices and Networks*, September 18, 2009.

[19] NIST SP 800-53 R4, Control AR-4: Privacy Monitoring And Auditing, April 2013.

recommends that an organization monitor and audit privacy controls and internal privacy policy to ensure effective implementation.

Weak physical controls over PII increase the risk of unauthorized individuals obtaining and using that data for inappropriate purposes. Additionally, writing passwords down greatly increases the risk of accounts being used by unauthorized individuals. Finally, because many people reuse or slightly modify existing passwords, the likelihood that unauthorized individuals could guess additional passwords in use is higher.

Recommendations:

9. We recommend that the Chief Information Officer develop, document, and implement a formal process to periodically test compliance with Smithsonian requirements regarding the physical handling of passwords, such as inspections.
10. We recommend that the Smithsonian Privacy Officer develop and implement a formal process to periodically test compliance with Smithsonian privacy requirements to safeguard PII in physical form.

F. The Smithsonian Needs to Review and Update Privacy Policies

The Smithsonian lacks controls to ensure that it periodically reviews and updates its privacy policy. Specifically, the Smithsonian Directive 119, *Breach Notification Policy*, has not been reviewed and updated since 2010. This is in contrast to key NIST guidance,[20] which recommends that an organization update its privacy plan, policies, and procedures at least biennially. It also violates Smithsonian policy, which requires a review and update of directives for currency every three years.[21]

Additionally, even though privacy incidents have occurred at the Smithsonian within the last fiscal year, management has not reviewed the effectiveness of the breach notification policy. NIST guidance states that incident response policies should be continually updated and improved based on the lessons learned during each incident. [22]

The current privacy officer has been in place for a little over a year, and in that time has been reviewing and updating the existing privacy policy. However, without a formal process in place to periodically evaluate existing privacy and breach-handling policies, the risks of the Smithsonian’s breach response policy not being effective in the event of a breach are higher.

Recommendation:

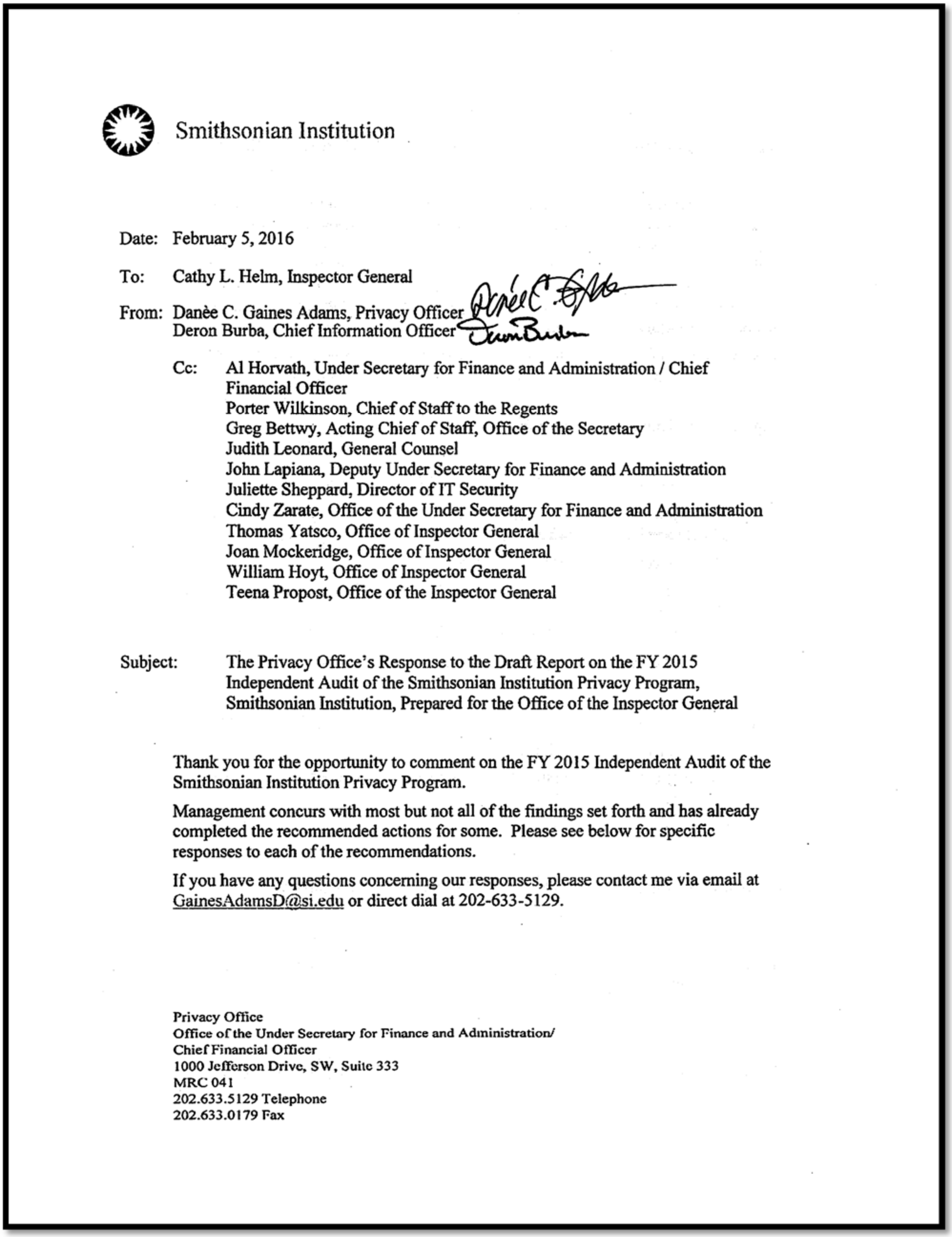
11. We recommend that the Smithsonian Privacy Officer implement controls to ensure a review of the Smithsonian Breach Notification Policy is conducted after significant breaches and the policy is updated as necessary.

[20] NIST SP 800-53 R4, Control AR-1: Governance and Privacy Program, April 2013.

[21] SD 100, SMITHSONIAN DIRECTIVES, Section 5.3: Determining the Status of Existing Directives, February 12, 2015.

[22] NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, Section 5.4: Post-Incident Activity, April 2010.

APPENDIX I – MANAGEMENT'S RESPONSE



Smithsonian Institution

Date: February 5, 2016

To: Cathy L. Helm, Inspector General

From: Danèe C. Gaines Adams, Privacy Officer
Deron Burba, Chief Information Officer

Cc: Al Horvath, Under Secretary for Finance and Administration / Chief Financial Officer
Porter Wilkinson, Chief of Staff to the Regents
Greg Bettwy, Acting Chief of Staff, Office of the Secretary
Judith Leonard, General Counsel
John Lapiana, Deputy Under Secretary for Finance and Administration
Juliette Sheppard, Director of IT Security
Cindy Zarate, Office of the Under Secretary for Finance and Administration
Thomas Yatsco, Office of Inspector General
Joan Mockeridge, Office of Inspector General
William Hoyt, Office of Inspector General
Teena Propost, Office of the Inspector General

Subject: The Privacy Office's Response to the Draft Report on the FY 2015 Independent Audit of the Smithsonian Institution Privacy Program, Smithsonian Institution, Prepared for the Office of the Inspector General

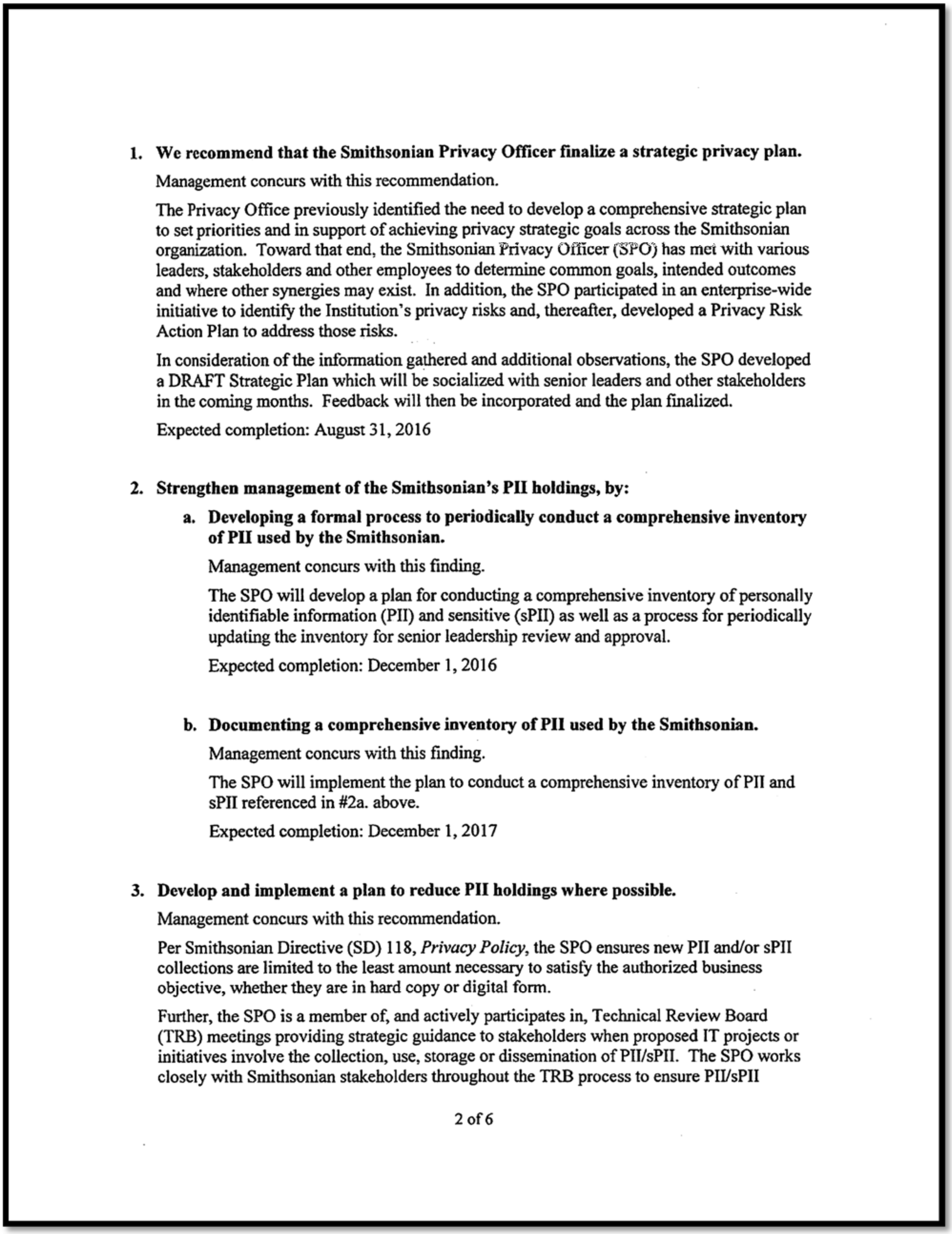
Thank you for the opportunity to comment on the FY 2015 Independent Audit of the Smithsonian Institution Privacy Program.

Management concurs with most but not all of the findings set forth and has already completed the recommended actions for some. Please see below for specific responses to each of the recommendations.

If you have any questions concerning our responses, please contact me via email at GainesAdamsD@si.edu or direct dial at 202-633-5129.

Privacy Office
Office of the Under Secretary for Finance and Administration/
Chief Financial Officer
1000 Jefferson Drive, SW, Suite 333
MRC 041
202.633.5129 Telephone
202.633.0179 Fax

APPENDIX I – MANAGEMENT'S RESPONSE



1. **We recommend that the Smithsonian Privacy Officer finalize a strategic privacy plan.**

   Management concurs with this recommendation.

   The Privacy Office previously identified the need to develop a comprehensive strategic plan to set priorities and in support of achieving privacy strategic goals across the Smithsonian organization. Toward that end, the Smithsonian Privacy Officer (SPO) has met with various leaders, stakeholders and other employees to determine common goals, intended outcomes and where other synergies may exist. In addition, the SPO participated in an enterprise-wide initiative to identify the Institution's privacy risks and, thereafter, developed a Privacy Risk Action Plan to address those risks.

   In consideration of the information gathered and additional observations, the SPO developed a DRAFT Strategic Plan which will be socialized with senior leaders and other stakeholders in the coming months. Feedback will then be incorporated and the plan finalized.

   Expected completion: August 31, 2016

2. **Strengthen management of the Smithsonian's PII holdings, by:**

   a. **Developing a formal process to periodically conduct a comprehensive inventory of PII used by the Smithsonian.**

      Management concurs with this finding.

      The SPO will develop a plan for conducting a comprehensive inventory of personally identifiable information (PII) and sensitive (sPII) as well as a process for periodically updating the inventory for senior leadership review and approval.

      Expected completion: December 1, 2016

   b. **Documenting a comprehensive inventory of PII used by the Smithsonian.**

      Management concurs with this finding.

      The SPO will implement the plan to conduct a comprehensive inventory of PII and sPII referenced in #2a. above.

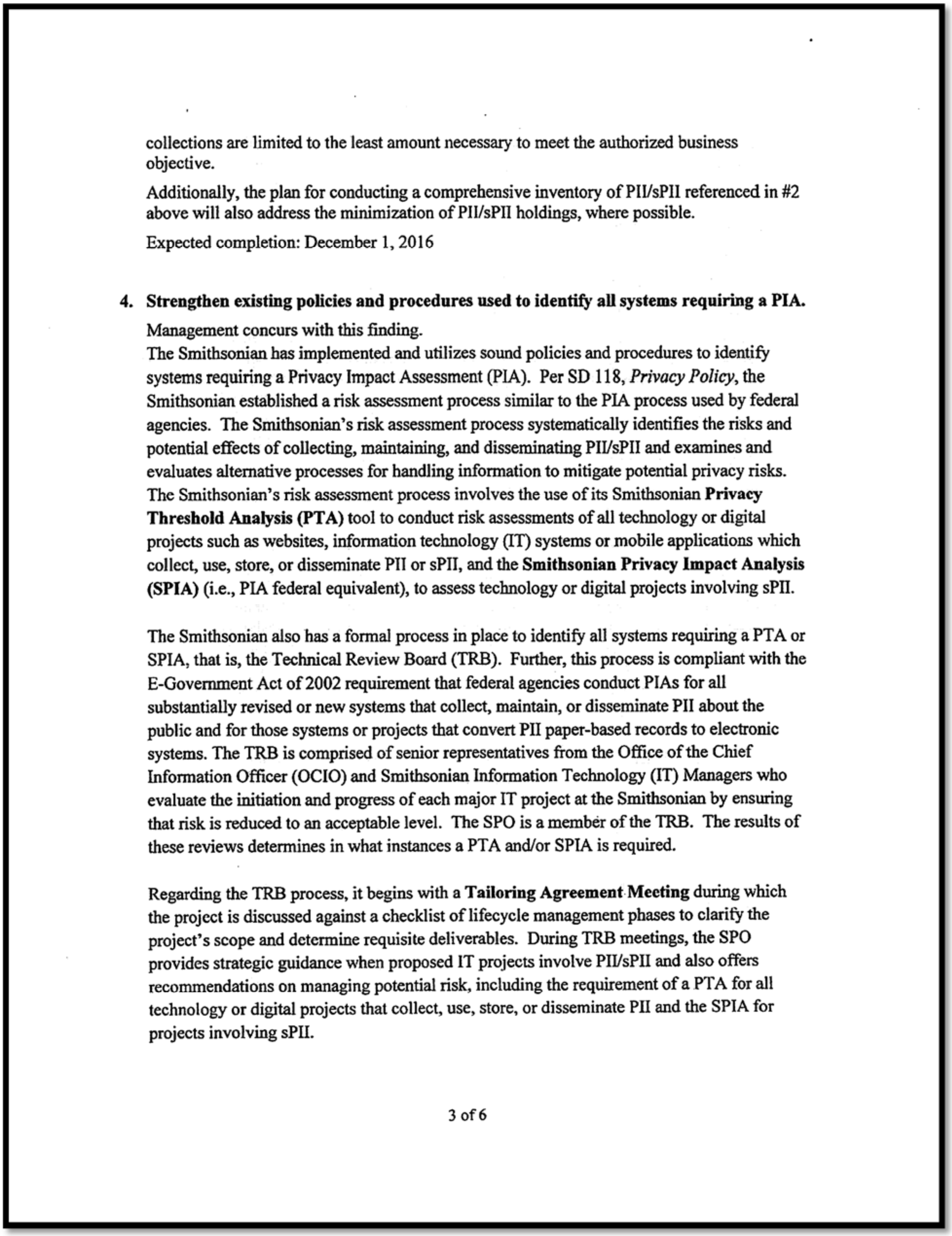
      Expected completion: December 1, 2017

3. **Develop and implement a plan to reduce PII holdings where possible.**

   Management concurs with this recommendation.

   Per Smithsonian Directive (SD) 118, *Privacy Policy*, the SPO ensures new PII and/or sPII collections are limited to the least amount necessary to satisfy the authorized business objective, whether they are in hard copy or digital form.

   Further, the SPO is a member of, and actively participates in, Technical Review Board (TRB) meetings providing strategic guidance to stakeholders when proposed IT projects or initiatives involve the collection, use, storage or dissemination of PII/sPII. The SPO works closely with Smithsonian stakeholders throughout the TRB process to ensure PII/sPII



collections are limited to the least amount necessary to meet the authorized business objective.

Additionally, the plan for conducting a comprehensive inventory of PII/sPII referenced in #2 above will also address the minimization of PII/sPII holdings, where possible.

Expected completion: December 1, 2016

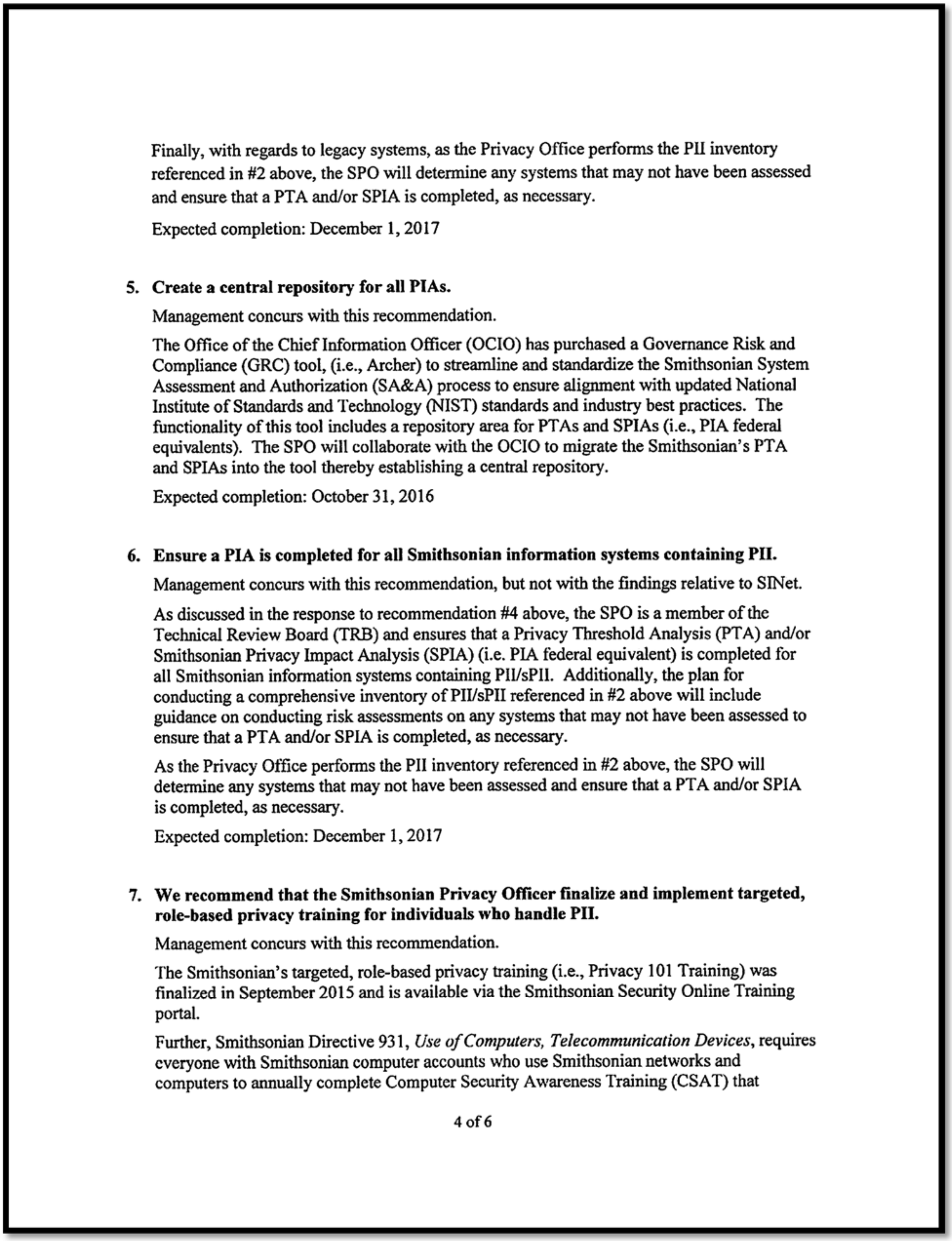
4. **Strengthen existing policies and procedures used to identify all systems requiring a PIA.**

Management concurs with this finding.

The Smithsonian has implemented and utilizes sound policies and procedures to identify systems requiring a Privacy Impact Assessment (PIA). Per SD 118, *Privacy Policy*, the Smithsonian established a risk assessment process similar to the PIA process used by federal agencies. The Smithsonian's risk assessment process systematically identifies the risks and potential effects of collecting, maintaining, and disseminating PII/sPII and examines and evaluates alternative processes for handling information to mitigate potential privacy risks. The Smithsonian's risk assessment process involves the use of its Smithsonian **Privacy Threshold Analysis (PTA)** tool to conduct risk assessments of all technology or digital projects such as websites, information technology (IT) systems or mobile applications which collect, use, store, or disseminate PII or sPII, and the **Smithsonian Privacy Impact Analysis (SPIA)** (i.e., PIA federal equivalent), to assess technology or digital projects involving sPII.

The Smithsonian also has a formal process in place to identify all systems requiring a PTA or SPIA, that is, the Technical Review Board (TRB). Further, this process is compliant with the E-Government Act of 2002 requirement that federal agencies conduct PIAs for all substantially revised or new systems that collect, maintain, or disseminate PII about the public and for those systems or projects that convert PII paper-based records to electronic systems. The TRB is comprised of senior representatives from the Office of the Chief Information Officer (OCIO) and Smithsonian Information Technology (IT) Managers who evaluate the initiation and progress of each major IT project at the Smithsonian by ensuring that risk is reduced to an acceptable level. The SPO is a member of the TRB. The results of these reviews determines in what instances a PTA and/or SPIA is required.

Regarding the TRB process, it begins with a **Tailoring Agreement Meeting** during which the project is discussed against a checklist of lifecycle management phases to clarify the project's scope and determine requisite deliverables. During TRB meetings, the SPO provides strategic guidance when proposed IT projects involve PII/sPII and also offers recommendations on managing potential risk, including the requirement of a PTA for all technology or digital projects that collect, use, store, or disseminate PII and the SPIA for projects involving sPII.



Finally, with regards to legacy systems, as the Privacy Office performs the PII inventory referenced in #2 above, the SPO will determine any systems that may not have been assessed and ensure that a PTA and/or SPIA is completed, as necessary.

Expected completion: December 1, 2017

5. **Create a central repository for all PIAs.**

   Management concurs with this recommendation.

   The Office of the Chief Information Officer (OCIO) has purchased a Governance Risk and Compliance (GRC) tool, (i.e., Archer) to streamline and standardize the Smithsonian System Assessment and Authorization (SA&A) process to ensure alignment with updated National Institute of Standards and Technology (NIST) standards and industry best practices. The functionality of this tool includes a repository area for PTAs and SPIAs (i.e., PIA federal equivalents). The SPO will collaborate with the OCIO to migrate the Smithsonian's PTA and SPIAs into the tool thereby establishing a central repository.

   Expected completion: October 31, 2016

6. **Ensure a PIA is completed for all Smithsonian information systems containing PII.**

   Management concurs with this recommendation, but not with the findings relative to SINet.

   As discussed in the response to recommendation #4 above, the SPO is a member of the Technical Review Board (TRB) and ensures that a Privacy Threshold Analysis (PTA) and/or Smithsonian Privacy Impact Analysis (SPIA) (i.e. PIA federal equivalent) is completed for all Smithsonian information systems containing PII/sPII. Additionally, the plan for conducting a comprehensive inventory of PII/sPII referenced in #2 above will include guidance on conducting risk assessments on any systems that may not have been assessed to ensure that a PTA and/or SPIA is completed, as necessary.

   As the Privacy Office performs the PII inventory referenced in #2 above, the SPO will determine any systems that may not have been assessed and ensure that a PTA and/or SPIA is completed, as necessary.

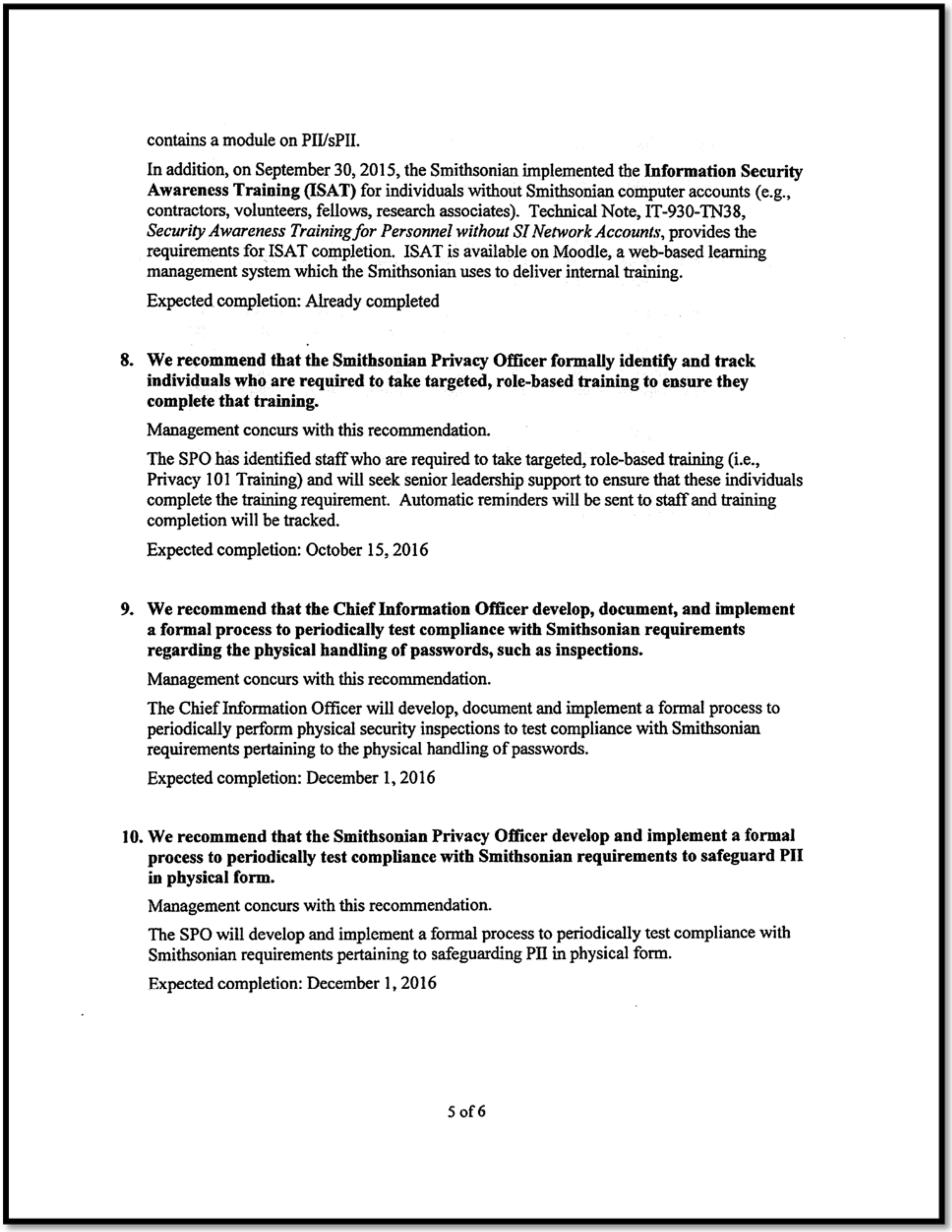
   Expected completion: December 1, 2017

7. **We recommend that the Smithsonian Privacy Officer finalize and implement targeted, role-based privacy training for individuals who handle PII.**

   Management concurs with this recommendation.

   The Smithsonian's targeted, role-based privacy training (i.e., Privacy 101 Training) was finalized in September 2015 and is available via the Smithsonian Security Online Training portal.

   Further, Smithsonian Directive 931, *Use of Computers, Telecommunication Devices*, requires everyone with Smithsonian computer accounts who use Smithsonian networks and computers to annually complete Computer Security Awareness Training (CSAT) that



contains a module on PII/sPII.

In addition, on September 30, 2015, the Smithsonian implemented the **Information Security Awareness Training (ISAT)** for individuals without Smithsonian computer accounts (e.g., contractors, volunteers, fellows, research associates). Technical Note, IT-930-TN38, *Security Awareness Training for Personnel without SI Network Accounts*, provides the requirements for ISAT completion. ISAT is available on Moodle, a web-based learning management system which the Smithsonian uses to deliver internal training.

Expected completion: Already completed

8. **We recommend that the Smithsonian Privacy Officer formally identify and track individuals who are required to take targeted, role-based training to ensure they complete that training.**

   Management concurs with this recommendation.

   The SPO has identified staff who are required to take targeted, role-based training (i.e., Privacy 101 Training) and will seek senior leadership support to ensure that these individuals complete the training requirement. Automatic reminders will be sent to staff and training completion will be tracked.

   Expected completion: October 15, 2016

9. **We recommend that the Chief Information Officer develop, document, and implement a formal process to periodically test compliance with Smithsonian requirements regarding the physical handling of passwords, such as inspections.**

   Management concurs with this recommendation.

   The Chief Information Officer will develop, document and implement a formal process to periodically perform physical security inspections to test compliance with Smithsonian requirements pertaining to the physical handling of passwords.

   Expected completion: December 1, 2016

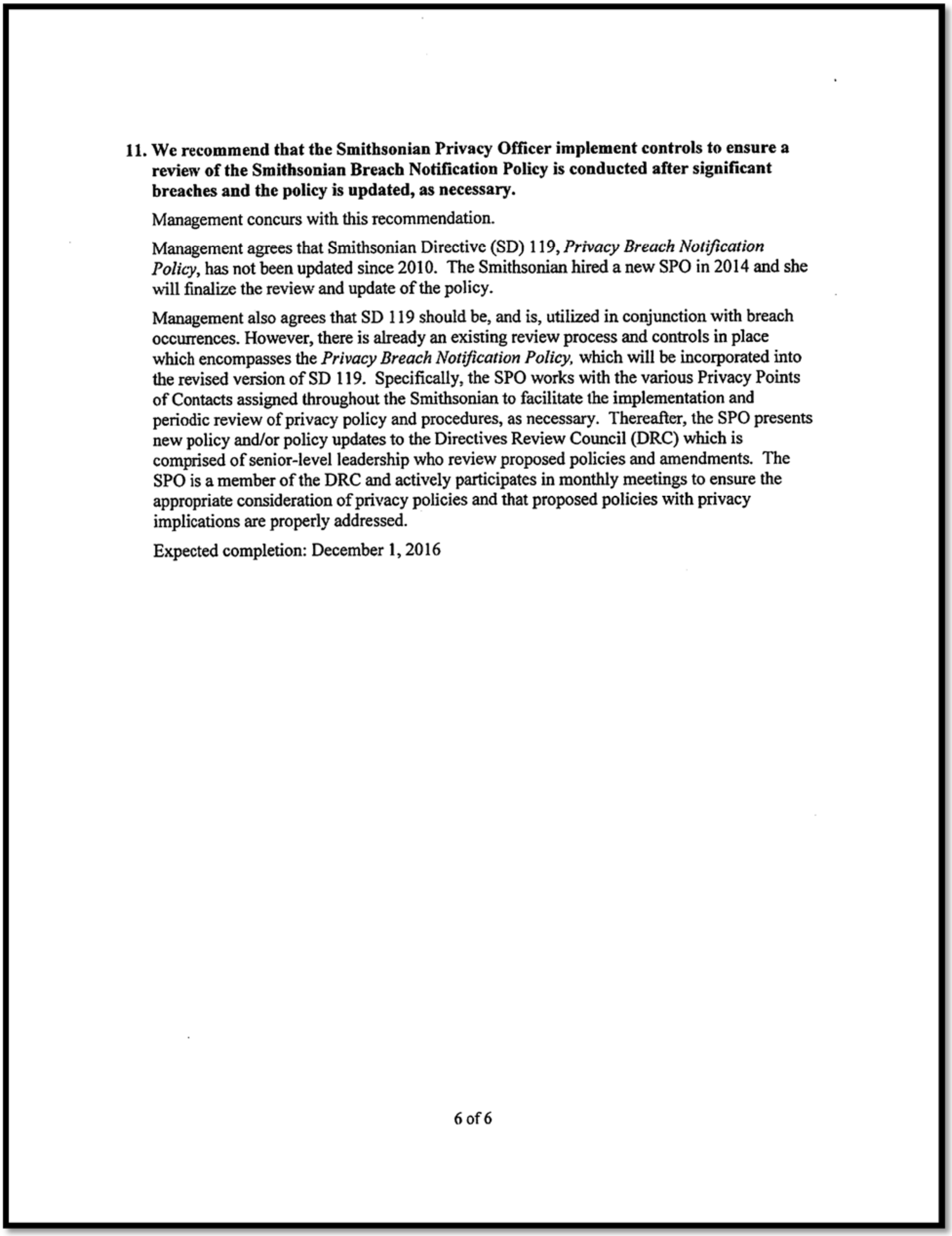
10. **We recommend that the Smithsonian Privacy Officer develop and implement a formal process to periodically test compliance with Smithsonian requirements to safeguard PII in physical form.**

    Management concurs with this recommendation.

    The SPO will develop and implement a formal process to periodically test compliance with Smithsonian requirements pertaining to safeguarding PII in physical form.

    Expected completion: December 1, 2016

APPENDIX I – MANAGEMENT'S RESPONSE



11. **We recommend that the Smithsonian Privacy Officer implement controls to ensure a review of the Smithsonian Breach Notification Policy is conducted after significant breaches and the policy is updated, as necessary.**

Management concurs with this recommendation.

Management agrees that Smithsonian Directive (SD) 119, *Privacy Breach Notification Policy*, has not been updated since 2010. The Smithsonian hired a new SPO in 2014 and she will finalize the review and update of the policy.

Management also agrees that SD 119 should be, and is, utilized in conjunction with breach occurrences. However, there is already an existing review process and controls in place which encompasses the *Privacy Breach Notification Policy,* which will be incorporated into the revised version of SD 119. Specifically, the SPO works with the various Privacy Points of Contacts assigned throughout the Smithsonian to facilitate the implementation and periodic review of privacy policy and procedures, as necessary. Thereafter, the SPO presents new policy and/or policy updates to the Directives Review Council (DRC) which is comprised of senior-level leadership who review proposed policies and amendments. The SPO is a member of the DRC and actively participates in monthly meetings to ensure the appropriate consideration of privacy policies and that proposed policies with privacy implications are properly addressed.

Expected completion: December 1, 2016