SMITHSONIAN INSTITUTION

FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA)

FISCAL YEAR 2014 INDEPENDENT EVALUATION REPORT

CliftonLarsonAllen

CliftonLarsonAllen LLP
www.cliftonlarsonallen.com

Cathy L. Helm
Inspector General
Office of the Inspector General
Smithsonian Institution
600 Maryland Avenue
Washington, DC 20024

Dear Ms. Helm:

We are pleased to provide this FY 2014 Independent FISMA Evaluation Final Report that presents the results of our audit of the Smithsonian Institution's (Smithsonian) information security program.

FISMA requires Inspectors General to conduct annual evaluations of their organization's security programs and practices, and to report to the Office of Management and Budget (OMB), the results of these evaluations. OMB Memorandum M-15-01 of October 3, 2014, provides instructions for meeting the FISMA reporting requirements. The Smithsonian has decided to participate in the FISMA evaluation as part of their information security program. The Smithsonian is not required by law to comply with FISMA.

We completed our response to OMB Memorandum M-15-01 based on our independent evaluation as of December 31, 2014, subsequent review through the date of this report of documentation supporting the security program performance statistics reported by Smithsonian management, and review of Plans of Action and Milestones. In preparing our responses, we collaborated with Smithsonian management and appreciate their cooperation in this effort.

We appreciate the opportunity to assist your office with these reports. Should you have any questions please call George Fallon, Principal, at (301) 931-2050.

CliftonLarsonAllen LLP

Calverton, Maryland
December 14, 2015

REPORT ON FISCAL YEAR 2014
Independent Evaluation of the Smithsonian Institution's
Information Security Program

TABLE OF CONTENTS

INTRODUCTION 1

PURPOSE 1

BACKGROUND 1

OBJECTIVES, SCOPE, AND METHODOLOGY 2

RESULTS IN BRIEF 3

RESULTS OF THE AUDIT 4

I. OCIO Needs to Improve Its Security Assessment and Authorization Process 4
II. OCIO Needs An Information Security Continuous Monitoring (ISCM) Strategy 8
III. OCIO Needs To Improve Its Plan of Action and Milestones Process 8
IV. OCIO Needs To Conduct or Document Its Continuous Monitoring Activities 9
V. OCIO Needs To Conduct Configuration Baseline Compliance Assessments 10
VI. The Smithsonian Needs To Strengthen Access Controls Management 11
VII. OCIO Needs To Implement Multi-Factor Authentication for Remote Access 14
VIII. OCIO Needs To Improve Its Patch Management of Identified Vulnerabilities 14

Appendix A - Status of Prior Years' Findings and Recommendations 16
Appendix B - Management's Response 18

REPORT ON FISCAL YEAR 2014
Independent Evaluation of the Smithsonian Institution's
Information Security Program

ACRONYMS

AC	Access Control
AD	Active Directory
ArtCIS	Art Collection Information System
AIS	Automated Information Systems
CIO	Chief Information Officer
CLA	CliftonLarsonAllen
CM	Configuration Management
CP	Contingency Planning
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
FIPS	Federal Information Processing Standards Publication
FY	Fiscal Year
HRMS	Human Resources Management System
IA	Identification and Authentication
IR	Incident Response
ISCM	Information Security Continuous Monitoring
MGS STARS	Monster Government Solutions Smithsonian Tracking and Applicant Referral System
NFC	National Finance Center
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OHR	Office of Human Resources

OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPS	Office of Protection Services
PANDA	PAN-Institutional Database for Advancement
POA&M	Plans of Action and Milestones
SA&A	Security Assessment and Authorization
SAR	Security Assessment Reports
SP	Special Publication
SSP	System Security Plan
ST&E	Security Test and Evaluation
TN	Technical Note
TSG	Technical Standards and Guidelines
VPN	Virtual Private Network
webTA	Web Time & Attendance

REPORT ON FISCAL YEAR 2014
Independent Audit of the Smithsonian Institution's
Information Security Program

INTRODUCTION

On behalf of the Office of the Inspector General (OIG), the auditing firm of CliftonLarsonAllen (CLA) conducted an independent audit of the Smithsonian Institution's (Smithsonian) information security program and practices consistent with Title III of the 2002 E-Government Act, also known as the Federal Information Security Management Act (FISMA).

PURPOSE

FISMA was enacted to strengthen the security of federal government information systems. Although the Smithsonian is not subject to FISMA because it is not an executive branch agency, the Smithsonian has adopted FISMA through its Technical Standards and Guidelines (TSG). FISMA outlines federal information security compliance criteria, including the requirement for an annual independent audit by the OIG.

BACKGROUND

The goal of information security is to build a defensible enterprise that enables organizations to harness technological innovation, while protecting an organization's information and information systems. FISMA requires organizations to adopt a risk-based, life-cycle approach to improving information security that includes annual security program reviews, independent evaluations by the OIG, and reporting to the Department of Homeland Security (DHS) and the Congress.

FISMA, DHS, and the National Institute of Standards and Technology (NIST) identify security requirements for federal information security programs. These include:

- **Security Assessment and Authorization.** NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, requires that security authorization packages be prepared for each major information system and have official authorization. The security authorization package contains: (i) the security plan; (ii) the security assessment report; and (iii) the plan of action and milestones. The information in these key documents is used by authorizing officials to make risk-based authorization decisions. The security authorization process is an inherently Federal responsibility and therefore, authorizing officials must be federal employees. OMB policy requires that organizations conduct ongoing authorizations of information systems by implementing continuous monitoring programs. If the agency has established continuous monitoring programs, this can satisfy three-year reauthorization requirements.

- **Minimum Security Requirements.** NIST Federal Information Processing Standards Publication 200 (FIPS 200), *Minimum Security Requirements for Federal Information and Information Systems*, is a mandatory federal standard developed by NIST in response to FISMA. FISMA requires that each agency develop, maintain and annually update an inventory of major information systems (i.e., major applications and general support systems) operated by the agency or under its control. Federal entities must meet the minimum security requirements as defined in the standard through the use of the security controls in accordance with NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

The use of security controls from SP 800-53, Revision 4 provides organizations the guidelines for selecting and specifying security controls for information systems to meet the requirements of FIPS Publication 200. SP 800-53 was revised to ensure that systems are more resilient in the face of cyber-attacks and other threats.

- **Continuous Monitoring.** NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions and includes testing and evaluating the information systems as part of the ongoing system development life cycle process.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this audit were to assess the effectiveness of the Smithsonian information security program and practices and to determine compliance with FISMA requirements and Smithsonian information security policies, procedures, standards, and guidelines.

On behalf of the OIG, CLA performed an independent performance audit of the Smithsonian information security program. We conducted this audit in accordance with *Government Auditing Standards*, December 2011 Revision, 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.

Our methodology included performing security reviews of the Smithsonian's information technology (IT) infrastructure and reviewing its Plans of Action and Milestones (POA&Ms). We also conducted detailed interviews with the Office of the Chief Information Officer (OCIO) personnel and major system owners or sponsors. CLA developed a three year audit rotation plan, in consultation with the OIG, to review the Smithsonian's 19 major systems. We evaluated the following five major systems in FY 2014:

- General Support System (SInet)—SInet is the computing infrastructure and core services used by Smithsonian employees and volunteers to perform their daily work. The services include internet, phone, email, remote access, content filtering, file storage, and many others that are integral to running an organization the size of the Smithsonian.

- Web Time & Attendance (webTA)—the Smithsonian's web-based online system for entering time and attendance data.

- The Museum System (TMS), also known as the Art Collection Information System (ArtCIS), is a commercial software product from Gallery Systems, Inc. that is currently used by all seven of the Smithsonian's art museums plus the Anacostia Community Museum, the National Air and Space Museum (NASM), and the National Museum of African American History and Culture (NMAAHC) to meet their collections information management needs.

- Monster Government Solutions Smithsonian Tracking and Applicant Referral System (MGS STARS)—Monster Hiring Management Enterprise, created by Monster Government Solutions, is

a service delivery mechanism that streamlines hiring management efforts. Monster Hiring Management Enterprise is a software tool that utilizes the public Internet to provide desired functionality. Customers access it by using a web browser. The Smithsonian calls this system MGS STARS.

- PAN-Institutional Database for Advancement (PANDA) — PANDA is comprehensive fund raising software and reporting system that serves as the central systems for documenting philanthropic activity at the Smithsonian PANDA consists of two web-based applications, Ellucian's Advance Web and IBM Cognos. PANDA centralizes the identification, tracking, management, soliciting and stewardship of individuals and organizations that have a philanthropic relationship with the Smithsonian Institution.

We performed procedures to test: (1) the implementation of a Smithsonian-wide security program and (2) operational and technical controls specific to each application such as service continuity, logical access, and change management controls. Additionally, we evaluated management's actions to address recommendations from previous FISMA evaluation reports.

We performed our audit from October 2014 through March 2015, at Smithsonian facilities in Washington, D.C. and Virginia. Smithsonian management and staff were helpful and accommodating throughout this review. This evaluation was prepared based on information available as of March 6, 2015.

RESULTS IN BRIEF

We found that OCIO continued to make progress in improving controls over information technology resources. However, the OCIO needs to do additional work to ensure controls are in place and operating effectively. We noted some control weaknesses resulting from the OCIO not implementing security patches or software updates in a timely manner. We also found that some system managers were not consistently submitting quarterly monitoring reports or remediating security vulnerabilities within established timeframes. Specifically, we found that OCIO needs to:

- improve its security assessment and authorization process and implement additional controls and plans in key areas,
- implement an information security continuous monitoring strategy,
- improve its plan of action and milestones process,
- conduct or document its continuous monitoring activities for 3 of 5 systems tested,
- conduct configuration baseline compliance,
- strengthen access controls management,
- implement multi-factor authentication for remote access, and
- take more action to improve its patch management of identified vulnerabilities.

Smithsonian management concurred with our recommendations and has proposed corrective actions to address them. Please refer to Appendix B for management's complete response.

Furthermore, OCIO needs to continue its focus on implementing recommendations from prior reports. Appendix A details each of the open IT security recommendations.

RESULTS OF THE AUDIT

The following is a detailed discussion of our findings, as well as recommendations for strengthening the Smithsonian's information security program. We present our findings in the order of greatest risk.

I. OCIO Needs to Improve Its Security Assessment and Authorization Process

We noted weaknesses in the OCIO's security assessment and authorization process in the following areas: baseline security control, common controls, management of exceptions and waivers, system security plans, and security control assessment. Not addressing these issues could increase the vulnerability of Smithsonian systems to IT security risks.

Baseline Security Controls Need to be Updated

The OCIO has not implemented all required controls from NIST SP 800-53, Revision 4, published in April 2013. The Smithsonian's existing controls described in system security plans, security test and evaluations (ST&Es), Technical Notes (TN), and TSGs were based on the outdated NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*. The OCIO had not developed or implemented a plan for the full adoption of NIST SP 800-53, Revision 4. Consequently, the OCIO did not implement Revision 4 by OMB's established deadline of April 2014.

Outdated system security plans, ST&Es, TNs, and TSGs may increase the likelihood of inadequately addressing the new IT security risks identified in NIST 800-53 Revision 4.

OCIO Needs a Complete Catalog of Common Controls

Common security controls provide the foundation for ensuring the effectiveness of enterprise-wide system security operations. Common controls are security controls that are inherited by one or more information systems within the Smithsonian. These controls are intended to do the following:

- Promote more cost-effective and consistent information security across the organization and can also simplify risk management activities.
- Provide a security capability for multiple information systems.

The OCIO did not have an accurate and comprehensive catalog of all common controls in its *Security Controls Manual*, version 3.9 (TSG IT-930-02). While the individual system security plans for SInet and webTA identified ten security controls as common controls (see below), they were not listed in the OCIO's *Security Controls Manual* as common controls:

1. AC-19 Access Control for Mobile Devices (webTA SSP)
2. AT-3 Role-Based Security Training (SInet SSP)
3. IR-5 Incident Monitoring (SInet and webTA SSP)
4. MA-2 Controlled Maintenance (SInet SSP)
5. MP-3 Media Marking (webTA SSP)
6. MP-4 Media Storage (SInet SSP)
7. MP-5 Media Transport (SInet SSP)

8. MP-6 Media Sanitization (SInet SSP)
9. SC-4 Information in Shared Resources (SInet SSP)
10. SC-23 Session Authenticity (SInet SSP)

In addition, the SInet and webTA SSPs did not identify who is responsible for the common controls.

If the common control catalog is inaccurate or incomplete, IT staff may not implement critical controls due to a misunderstanding that a risk is mitigated by a common control. This may result in insufficient protection of sensitive or critical resources. Alternatively, they may implement controls that are already provided and waste scarce resources.

OCIO Needs to Consistently Manage Its Exceptions and Waivers

Information systems that do not fully comply with policy requirements due to a system weakness or need for a permanent exception to Smithsonian policy must have an approved waiver or exception from any portion of information security policy requirements. A waiver is the written permission required to temporarily eliminate the requirements of a specific policy or control. An exception is an authorization to proceed outside of policy when certain conditions apply. Policy requirements may not be followed as intended.

OCIO did not have a formal, documented process to manage exceptions and waivers, which resulted in miscommunication regarding their validity. The list of 12 SInet exceptions and waivers reported to the IT System Sponsors and Mission Sponsors during the annual management briefing presentation, in October 2014, was not accurate. According to the Director of IT Security, one fiscal year 2013 waiver was never issued. The Director of IT Security also stated that the two waivers, as shown below, may have been invalid.

Waiver Never Issued

- FY13 SInet Designated Information System Security Officer (AC-5)

Invalid Waivers

- FY11 Managed IT Infrastructure: SInet Separation of Duties (AC-5) Waivers
- FY12 SInet Waiver IIS/Apache CM Reports / Lack of Tool Web Resource Constraints

Having an inaccurate list of exceptions and waivers is a significant issue because it may provide management and IT staff with an incomplete perspective on the risks associated with a system and inhibit their ability to make effective decisions about risk mitigation strategies

OCIO Needs to Adequately Review Three of the Five System Security Plans We Tested

The protection of a system must be documented in a SSP. The purpose of this plan is to provide an overview of the security requirements of each system and describe the controls in place or planned for meeting those requirements. The plan also delineates responsibilities and expected behavior of all individuals who access the system.

The OCIO did not adequately review the accuracy and completeness of system security plans. We evaluated the SSPs for the five systems: SInet, webTA, ArtCIS, MGS STARS and PANDA. As part of this

review, we assessed the implementation details of five control families[1] [Access Control (AC), Configuration Management (CM), Contingency Planning (CP), Identification and Authentication (IA), and Incident Response (IR)] and noted the following weaknesses in three SSPs:

- SInet SSP—
  - For two controls, CM-9 Configuration Management Plan and IA-7 Cryptographic Module Authentication, details for how to implement them were not documented. As a result, the owner of the control may not consistently apply the control noted in the SSP; and
  - The list of system interconnections between SI systems and external systems was inaccurate. Accordingly, IT staff may not be implementing controls to mitigate security and operational risks associated with external systems connecting to SI systems.
- SInet, ArtCIS, and PANDA SSPs—existing exceptions and waivers were not noted in the implementation details.

Units' Reporting of Results from the Security Assessments Reports and Security Test and Evaluation Reports Needs Improvement

The results of the security control assessment, including recommendations for correcting any weaknesses or deficiencies in the controls, are documented in the security assessment report. The security assessment report is one of three key documents in the security authorization package developed for authorizing officials. The assessment report includes information on the effectiveness of the security controls employed within or inherited by the information system based upon the findings.

We reviewed the security assessment reports (SAR)[2] summary and ST&E reports,[3] which tracked and documented the results of the annual security control assessments for each system. We noted the following issues:

ST&E Reports:

- The SInet ST&E report was not updated to reflect the results of tests and assessment dates of all security controls in FY 2014. The dates in the ST&E still reflected FY 2013 and prior year testing.
- The ArtCIS ST&E report was not updated to reflect the correct assessment dates for the following controls: Access Enforcement, Controlled Maintenance, and Public Access Protections.
- According to the ST&E report, the ArtCIS privacy impact assessment (PIA) was last tested in FY 2010. The system sponsor did not re-test the PIA, assuming it was a common control. The system sponsor incorrectly assumed they were not responsible for testing the PIA. However, the TSG IT-930-02 *Security Controls Manual* did not identify PIA as a common control. As a result, no organization in SI tested the PIA.

SInet, webTA, ArtCIS, and PANDA's ST&E reports did not properly document changes to NIST 800-53 Rev 3 controls that were withdrawn by NIST in SP 800-53 Rev 4. SP 800-53

[1] Security controls may involve aspects of policy, oversight, supervision, manual processes, actions by individuals, or automated mechanisms implemented by information systems/devices. For ease of use in the security control selection and specification process, controls are organized into eighteen families. Each family contains security controls related to the general security topic of the family.
[2] The Security Assessment Report documents the Smithsonian's plan for testing security controls.
[3] The Security Test and Evaluation Report list the NIST SP 800-53 controls and documents the most recent test results.

Rev. 4 includes many changes from SP 800-53 Rev. 3: 295 controls and control enhancements were added while approximately 100 controls and control enhancements were withdrawn or incorporated into others. The ST&E reports, however, did not address these changes. The ST&E reports did not explain how the System Sponsors of these systems should deal with controls that were withdrawn in NIST 800-53 Rev 4. Controls impacted include Security Certification, Contingency Plan Update, System Security Plan Update, and Risk Assessment Update.

SAR Summaries:

- The SInet SAR summary and ST&E reports were inaccurate and incomplete. These reports were not updated to reflect controls tested in FY 2014. The reports still reflected FY 2013 dates for controls tested. These reports are crucial to identify control weaknesses for which corrective actions are to be developed, assigned and implemented. However, management did not adequately review the FY 2014 SInet SAR and ST&E reports to ensure accuracy and completeness, before they approved them.
- The ArtCIS SAR summary identifies security controls that were reviewed and tested annually. However, the SAR summary did not identify the last assessment date for the Privacy Impact Assessment. The ArtCIS ST&E also did not document the test result for Controlled Maintenance.

Finally, discrepancies existed between the ArtCIS SSP, the ST&E report, and information provided by Smithsonian personnel regarding ArtCIS common controls for Controlled Maintenance and Privacy Impact Assessment.

System owners did not consistently document and update their ST&E reports to reflect changes in assessment dates, assessment results, and identified common controls. Management did not perform detailed reviews of the ST&E reports.

Without accurate or properly updated SAR and ST&E reports, management and IT staff are hindered in their ability to ensure that controls are effective and mitigating IT security risks.

Applicable criteria:

- NIST SP 800-53, Revision 4
- TSG IT-930-02, *Security Controls Manual*, version 3.9, dated January 2014
- TSG IT-930-01, *AIS [Automated Information Systems] Security Planning,* dated May 2008

Recommendations:

We recommend that the CIO:

1. Strengthen the security assessment and authorization process to align with updated NIST requirements in NIST SP 800-53, Revision 4.

2. Require system owners to document and maintain a current and accurate listing of all valid exceptions and waivers applicable to the systems we tested (SInet, WebTA, ArtCIS, MGS-STARS, and PANDA).

II. OCIO Needs an Information Security Continuous Monitoring (ISCM) Strategy

An ISCM strategy and program provide ongoing assurance that planned and implemented security controls are aligned with organizational risk tolerance, as well as the ability to provide the information needed to respond to risk in a timely manner. ISCM strategy addresses monitoring and assessment of security controls for effectiveness, and security status monitoring. The ISCM helps to provide situational awareness of the security status of the organization's systems based on information collected from resources (e.g., people, processes, technology, and environment) and the capabilities in place to react as the situation changes.

The OCIO did not have an Information Security Continuous Monitoring (ISCM) strategy in FY 2014. OCIO did not submit a finalized ISCM Strategy to CyberScope on November 14, 2014, as called for in OMB M-15-01 *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices.* Furthermore, OCIO did not finalize its ISCM strategy by February 28, 2014, the deadline established by OMB M-14-03 *Enhancing the Security of Federal Information and Information Systems.*

In accordance with NIST SP 800-137, the OCIO had conducted continuous monitoring activities; however, it did not make documenting an ISCM strategy a high priority. According to the OCIO, it did not have a Director of IT Security to lead the development and establishment of an ISCM strategy after the departure of the previous Director of IT Security in December 2013. According to the OCIO, it currently has a Director of IT Security in place and has been developing an ISCM strategy.

Without a properly documented and implemented entity-wide ISCM strategy and program, the Smithsonian is hindered in its ability to consistently and effectively maintain ongoing awareness of the organization's information security vulnerabilities, and threats to support organizational risk management decisions.

Recommendation:

We recommend that the CIO:

3. Finalize the ISCM strategy in accordance with NIST SP 800-137.

III. OCIO Needs to Improve its Plan of Action and Milestones Process

The plan of action and milestones (POA&M), also referred to as a corrective action plan, is a tool used to remediate security vulnerabilities. The tool identifies tasks that need to be accomplished, details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The goal of a POA&M is to reduce the risk of each vulnerability identified. Agencies are required to update POA&Ms to reflect the current progress of implementing planned remediation efforts.

The OCIO did not adequately review POA&M reports for the five systems we tested, resulting in a lack of assurance that all necessary POA&M requirements and updates were conducted. Further, the POA&M

process had several weaknesses: (1) scheduled completion dates were not documented in the reports; (2) scheduled completion dates were not met; and (3) no justifications or explanations were provided for why completion dates were not met.

POA&Ms for the SInet and PANDA systems did not accurately state whether they were completed, delayed, or in progress. POA&Ms for the five systems we reviewed (SInet, webTA, ArtCIS, MGS STARS, and PANDA) did not explicitly state the resources (e.g., persons, hours, or costs) needed to correct weaknesses as defined in the TSG IT-930-01 *AIS Security Planning.* Further, the resource estimate requirement in the IT-930-TN29, *IT Security POA&Ms* did not meet the same requirements defined in the TSG IT-930-01 *AIS Security Planning*.

Applicable criteria:

- NIST SP 800-53, Revision 4
- TSG IT-930-02, *Security Controls Manual*, version 3.9, dated January 2014
- TSG IT-930-01, *AIS Security Planning*, dated May 2008
- TN IT-930-TN29, *IT Security Plans of Actions and Milestone*, dated June 2010

The OCIO did not have assurance that system POA&Ms were appropriately tracked or maintained, and that resources were available to effectively and efficiently remediate systems' security weaknesses. Sustained management attention is needed to ensure that OCIO staff is reviewing POA&M information from system owners in accordance with NIST requirements.

Recommendations:

We recommend that the CIO:

4. Implement additional controls to ensure the consistent review of POA&Ms for accuracy and completeness.

5. Update the SInet, webTA, ArtCIS, MGS STARS, and PANDA POA&Ms to include cost estimates.

IV. OCIO Needs to Conduct or Document Its Continuous Monitoring Activities

As part of continuous monitoring and compliance, system administrators are required by the *Security Controls Manual* to conduct a monthly review of account management reports and audit and security logs. Account management reports include a summary of new user accounts added, new requests for shared accounts, dormant accounts and disabled or deleted accounts. Audit and security logs are to be reviewed to confirm there were no unusual or suspicious activities during the month. On a quarterly basis, units are responsible for submitting to the OCIO evidence of their compliance activities to maintain IT security authorization.

The OCIO and PANDA system owners did not provide sufficient evidence to demonstrate that adequate continuous monitoring (TN02 *System and Application Audit / Logs Report* and TN04 *Dormant Accounts*) procedures were conducted for the following systems:

- SInet TN02 reports were not provided. According to the OCIO, the former SInet Information System Security Officer reviewed the audit logs regularly and contacted the appropriate personnel when there were issues; however, these reviews were not documented.
- PANDA TN02 reports were not provided. Ellucian, the third party service provider hosting PANDA, used Splunk as an automated monitoring and reporting tool to review system logs; however, we were not provided evidence that quarterly reports were provided to the OCIO.
- PANDA TN04 reports were not provided. We received the monthly PANDA user listings for FY 2014; however, the listings did not demonstrate that periodic reviews were conducted. We performed further analysis and noted that there were users who were not disabled after 90 days of inactivity. We also noted that the March 2014 PANDA user report was generated in June 2014.
- WebTA TN04 reports were not provided. We received the monthly webTA user listings for FY 2014; however, we noted the user listings were the same every month from August 2013 to July 2014. We determined that these webTA user listings did not demonstrate continuous monitoring of webTA accounts.

Limited program and system resources resulted in SInet, webTA, and PANDA not systematically following TSG IT-930-02 Appendix D Continuous Monitoring and Compliance Reports.

Applicable criteria:

- NIST SP 800-53, Revision 4
- TSG IT-930-02, *Security Controls Manual*
- TN IT-930-TN02, *Auditing and Accountability*
- TN IT-930-TN04, *Disabling & Deleting Dormant User Accounts*

Due to a lack of documented monitoring, management has less assurance that system administrators are remediating security vulnerabilities that could expose the Smithsonian's systems to intentional or unintentional damage. Sustained management attention is needed to ensure that OCIO is enforcing its policy for the IT/system administrators (or other responsible personnel as defined in TN IT-930-TN02 and IT-930-TN04) to provide quarterly monitoring and reporting on account management activities and audit log reviews to the Director of IT Security.

Recommendation:

We recommend that the CIO:

6. Implement additional controls to ensure that system sponsors consistently provide to the Director of IT Security quarterly monitoring and reporting on account management activities and audit log reviews.

V. OCIO Needs to Conduct Configuration Baseline Compliance Assessments

Baseline configurations include information about system components and the logical placement of those components within the system architecture. Baseline configuration monitoring identifies undiscovered/undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes, all of which, if not addressed, can expose organizations to increased risk. Using automated

tools helps organizations to efficiently identify when the information system is not consistent with the approved baseline configuration and when remediation actions are necessary.

The OCIO did not conduct a configuration baseline compliance assessment for SInet in FY 2014. Therefore, the OCIO has no assurance that the security configuration of SInet provides the necessary security and protections prescribed by its baseline. Without adequate protections, the Smithsonian is exposed to risk that vulnerabilities can be exploited and systems compromised. According to the Annual Assessment table in OCIO's TSG IT-930-02 *Security Controls Manual*, configuration compliance assessments should be conducted on an annual basis. However, TN IT-960-TN31 *Security Configuration Management of Baselines* did not include a requirement for an annual assessment.

The assessment of configuration baseline compliance is important for establishing and maintaining secure information system configurations, and provides support for managing security risks in information systems. If assessments of baseline compliance of Smithsonian's information systems are not conducted timely, non-compliance could have adverse effects within the system's environment, including alteration of the approved baseline.

Recommendations:

We recommend that the CIO:

7. Conduct baseline compliance assessments in accordance with the TSG IT-930-02 *Security Controls Manual*.

8. Update TN IT-960-TN31 *Security Configuration Management of Baselines* to be consistent with TSG IT-930-02 *Security Controls Manual*.

VI. The Smithsonian Needs to Strengthen Access Controls Management

An organization can protect the resources that support its critical operations from unauthorized access by having controls in place to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. Access controls include those related to identifying and authenticating users, authorizing access needed to perform job duties, encrypting sensitive data, auditing and monitoring system activities, and physically protecting computing resources. Access rights are the permissions that are granted to a user, or to an application, to read, write and erase files in the computer. Access rights can be used to restrict access to particular client or server, to folders within that machine or to specific programs and data files. Furthermore, access controls limit or detect access to computer resources such as data, programs, equipment, and facilities. These controls help to protect these resources against unauthorized or accidental modification, loss, and disclosure.

We found the following weaknesses in access controls for PANDA, MSG STARS, and webTA:

OCIO Needs to Consistently Follow Access Control Procedures for webTA

We found the following weaknesses with the webTA access control process:

- *WebTA Security Forms* were not provided for 3 of the 15 users we selected to review. The WebTA Security Form is a key internal control that is used to request and grant access to WebTA.
- Part 3 – Identification of Account Holder (mandatory) of the *OCIO Network/ Email Account Request* form did not identify one out of 15 users as requiring employee and supervisor access to webTA, and for one out of 15 users the checkbox was not selected to document the user required employee and supervisor access to webTA.
- Appropriateness of webTA permissions could not be determined due to lack of approval documentation for 3 of 15 users.

WebTA is interconnected with the US Department of Agriculture National Finance Center (NFC) system and some OHR staff require access to that system. OHR did not consistently follow access control procedures when granting access to NFC. We reviewed eight user accounts and found weaknesses as follows:

- Access request documentation was not provided for five users. The OHR stated that it was unable to provide documentation due to the retirement of the employee who had originally requested and documented access to NFC. We could not determine whether NFC permissions were appropriate due to a lack of documented approval.
- *Authorization and User Confidentiality Acknowledgement* forms were signed after access was granted for four users. For two users these forms were not provided.

OHR did not consistently retain the access requests and *Authorization and User Confidentiality Acknowledgement* forms.

OA Needs to Effectively Manage User Access to PANDA

The Office of Advancement (OA) had vulnerabilities in its process for managing the PANDA user accounts. We selected 15 PANDA user files and accounts to review, and noted the following access controls weaknesses:

- No evidence was provided to support that appropriate training was completed for the assigned PANDA access rights, as follows:
  - 2 users did not complete training for 1 assigned right
  - 1 user did not complete training for 2 assigned rights
  - 1 user did not complete training for 3 assigned rights
- Seven user accounts were inactive more than 90 days.
- Four user accounts did not have a login date.

PANDA management did not adequately approve users for specific roles in PANDA and accounts were not disabled timely. Access to PANDA was not adequately controlled and protected as it contains personally identifiable information (PII) and other donor information.

OHR Needs to Improve Management of Access to the MGS STARS System

For the MGS STARS system, OHR did not consistently retain access request forms and user agreements. We reviewed 15 MGS STARS users and found that OHR did not retain access request forms and user

agreements for 2 users. Therefore, we could not determine the appropriateness of MGS STARS permissions due for these users due to a lack of approval documentation.

Applicable criteria:

- NIST SP 800-53, Revision 4
- TSG IT-930-02, *Security Control Manual*
- TN IT-930-TN04, *Disabling & Deleting Dormant User Accounts*
- TN IT-960-TN12, *Active Directory Account & Password Requests*
- *PANDA User Access Protocol*

Access to MGS STARS was not adequately controlled and protected as it contains personally identifiable information (PII). Access controls allow an organization to limit and detect access to information systems. Without proper documentation and approval of specific roles, users may gain unauthorized access to various Smithsonian systems and third party applications, exposing these systems to unknown vulnerabilities such as data loss, data manipulation, and system unavailability.

Recommendations:

We recommend that the CIO:

9. Revise the *OCIO Request Form for Network/Email* to ensure the form is consistent with the practice for granting access to webTA.

10. Complete the *webTA Security Form* for all users with privileged access to the webTA system.

We recommend that the PANDA system sponsor:

11. Implement additional controls to consistently grant access after completion of required training as stated in the *PANDA User Access Protocol* and retain training documentation to support a user's system privileges.

12. Assess whether to implement new procedures to disable accounts that have not been logged into for 90 days or accounts that do not have a last-login date in accordance with IT-930-02, *Security Control Manual*.

We recommend that the MGS STARS system sponsor:

13. Implement additional controls to consistently document MGS STARS access requests to include user name, approval, roles, and user agreements.

We recommend that the Director of OHR:

14. Maintain user agreements and access request forms in a central repository for all users with access to NFC.

VII. OCIO Needs to Implement Multi-Factor Authentication for Remote Access

Multi-factor authentication is intended to decrease the probability that a requestor of remote access[4] is presenting false evidence of their identity. The number of factors is important, as it implies a higher probability that presenter identify evidence of who they claim to be. Multi-factor authentication serves to reduce the risk of identity theft and unauthorized access.

We determined that technical controls were not implemented to require multi-factor authentication[5] for remote access. We found that 10 out of the 13 total virtual private network[6] (VPN) groups did not require multi-factor authentication to obtain remote access to the Smithsonian network.

Applicable criteria:

- NIST SP 800-53, Revision 4
- TSG IT-930-02, *Security Controls Manual*

Improperly implemented access controls (user account management) exposes Smithsonian systems to potential unauthorized access, data loss, data manipulation, and system unavailability.

Recommendation:

We recommend that the CIO:

15. Implement technical controls to require multi-factor authentication for all VPN remote access.

VIII. OCIO Needs to Improve Its Patch Management of Identified Vulnerabilities

Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software. From a security perspective, patches can mitigate software vulnerabilities and reduce the opportunities for exploitation. Patches serve other purposes than just fixing flaws; they can also add new features, including security capabilities.

CLA's vulnerability scan during the week of November 17, 2014 of the Smithsonian network (SInet) and four major applications (SInet, webTA, PANDA, and ArtCIS), including servers, databases and devices resulted in the following:

[4] Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Remote access connections established via two-factor authentication where one of the factors is provided by a hardware device separate from the computer gaining access, reduces the risk of identity theft and unauthorized disclosure.

[5] Multi-factor authentication is characteristic of an authentication system or a token that uses more than one authentication factor. A token is something that the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity. The three types of authentication factors are something you know, something you have, and something you are.

[6] NIST SP 800-46, Revision 1, Guide to Enterprise Telework and Remote Access Security states "many remote access methods offer a secure communications tunnel through which information can be transmitted between networks, including public networks such as the Internet. Tunnels are typically established through *virtual private network* (VPN) technologies. Once a VPN tunnel has been established between a teleworker's client device and the organization's VPN gateway, the teleworker can access many of the organization's computing resources through the tunnel. To use a VPN, users must either have the appropriate VPN software on their client devices or be on a network that has a VPN gateway system on it."

- The Office of the Chief Information Officer made improvements in applying patches. However, these weaknesses still existed in FY 2014:
    - OCIO did not patch 23% of its Windows 7 critical vulnerabilities (88 vulnerabilities) within the 90-day patching period for desktops and laptops.
    - OCIO did not patch 54% of Windows 7 high vulnerabilities (1,598 vulnerabilities) within the 90-day patching period for desktops and laptops.

The OCIO has not implemented corrective actions on prior year findings in this area. The OCIO has several obsolete systems that cannot be patched because they are no longer supported by the vendor. Also, the OCIO continues to support versions of software without updating it with available security patches.

Applicable criteria:

- NIST SP 800-40, Revision 3, *Guide to Enterprise Patch Management Technologies*
- M-07-11, *Implementation of the Commonly Accepted Security Configurations for Windows Operating Systems*
- M-07-18, *Ensuring New Acquisitions Include Common Security Configurations*
- M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*
- TSG IT-930-02, *Security Control Manual*
- TN IT-960-TN02, *Patch and Update Management of Desktop Computers*
- TN IT-930-TN08, *Implementing Vendor Software Patches/Fixes*

Patch management, a component of configuration management, is an essential element in mitigating risks associated with software vulnerabilities. In the event critical patches are not applied within a timely manner, Smithsonian is susceptible to increased risks. Sensitive data, systems, and hardware could be exposed by attackers exploiting known vulnerabilities resulting in loss of integrity, confidentiality, and availability. Sustained management attention is needed to continually update all servers and databases to the current patch level in a timely manner in accordance with the TN IT-930-TN08, *Implementing Vendor Software Patches/Fixes*.

Recommendations:

We recommend that the CIO:

16. Update Smithsonian Directive 920, *Life Cycle Management*, to require that legacy systems that are no longer supported are retired and replaced.

17. Develop a list of software versions that are no longer supported by the manufacturer and a plan to upgrade or replace them.

REPORT ON FISCAL YEAR 2014
Independent Audit of the Smithsonian Institution's
Information Security Program

APPENDIX A: STATUS OF PRIOR YEARS' FINDINGS AND RECOMMENDATIONS

The following table presents the open recommendations from prior reports:

Report	Finding	Recommendation	Current Status
FISMA Evaluation Report Audit Number A-10-01 Issued March 15, 2011	The Smithsonian did not effectively enforce its policy as stated in IT-930-TN28 that requires all mobile devices used to store sensitive data to be encrypted.	Implement controls to ensure that all Smithsonian-owned laptops/mobile devices that may be used to store sensitive information are secured with an appropriate encryption technology.	Target date revised to December 2015.
FY2012 FISMA Evaluation Report Audit Number A-12-08 Issued June 03, 2013	Some servers and desktop computers were using outdated software that may no longer be supported by the vendor, or for which security updates may no longer be developed.	Monitor Smithsonian workstations for the presence of unapproved software and timely maintenance of approved software and enforce the existing policy requiring units to maintain products that are approved.	Target date revised to December 2015.
	The Systems Managers for SInet and the NMAH CIS Multi MIMSY system did not consistently provide quarterly monitoring reports to the OCIO. As a result, OCIO could not ensure that these system managers were monitoring the security posture of systems under their custody, as required by Smithsonian policy and FISMA guidance.	We recommend that the system sponsors for SInet and NMAH CIS Multi MIMSY ensure that the system managers provide quarterly monitoring and reporting on account management activities and audit log reviews to the OCIO Security Program.	Target date revised to December 2015.
Management Advisory Regarding Portable Computer Encryption Management Advisory Number M-13-01 Issued March 4, 2013	The controls in place are not adequate to ensure that laptop computers that may contain sensitive information are secured with an appropriate encryption technology. Staff were not knowledgeable about how the equipment they use was configured and expected it to be configured appropriately for its intended use.	Direct Unit IT staff to determine which laptop computers in their inventory may be used to store sensitive data and, with assistance from OCIO, configure those computers with whole drive encryption.	Target date revised to December 2015.
	The controls in place are not adequate to ensure that laptop computers that may contain sensitive information are secured with an appropriate encryption technology. Staff were not knowledgeable about how the equipment they use was configured and expected it to be configured appropriately for its intended use.	Direct Unit IT staff to identify all laptop computers that will not be configured with encryption and clearly indicate to users with a prominent label that those computers must not be used to store sensitive information.	Target date revised to December 2015.

REPORT ON FISCAL YEAR 2014
Independent Audit of the Smithsonian Institution's
Information Security Program

Report	Finding	Recommendation	Current Status
FY2013 FISMA Evaluation Report Audit Number A-13-10 Issued July 09, 2014	We determined that some security patches were not applied in a timely manner and management did not maintain compliance waivers to document the business justification for not installing the patch. Some unpatched critical and high-risk vulnerabilities were more than 12 months old. The five critical and most of the high-risk vulnerabilities on the servers were in older versions of software. This was also the case with the workstation vulnerabilities.	Ensure that IT security staff enforce compliance with patching requirements and, when appropriate, document compliance waivers.	Target date revised to December 2015.
	SAO management did not consistently retain change and configuration documentation. In addition, SAO did not consistently request approval from the Change Control Board for configuration changes for the Scientific Computing Infrastructure (SCI) and High Energy Astrophysics (HEA) systems.	Enforce configuration management procedures for the SCI and HEA systems to include tracking changes, approvals, testing, and implementation in accordance with Smithsonian policy.	Target date revised to July 2015.*
	Management has developed policies for authorizing connections. However, we found that the Smithsonian has not established policies or procedures for detecting and removing unauthorized remote connections. For example, unauthorized connections may include (1) wireless connections to a second network while connected to the Smithsonian network, or (2) an alternative internet service installed by a user to bypass the Smithsonian's firewall or remote access controls.	Develop, document, and implement policies and procedures for detecting and removing unauthorized connections.	Target date revised to December 2015.

NOTE: * The target date was not met. The Smithsonian has not provided a new date.

APPENDIX B: MANAGEMENT'S RESPONSE

Smithsonian Institution

Office of the Chief Information Officer

Date: October 15, 2015

To: Cathy L. Helm, Inspector General

From: Deron Burba, Chief Information Officer

Cc: Al Horvath, Under Secretary for Finance and Administration / Chief Financial Officer
John Lapiana, Deputy Under Secretary for Finance and Administration
Joan Mockeridge, Office of Inspector General
Bruce Gallus, Office of Inspector General
William Hoyt, Office of Inspector General
Joseph Benham, Office of Inspector General
Cindy Zarate, Office of the Chief Financial Officer
Stone Kelly, Office of Planning, Management and Budget
Juliette Sheppard, Director, IT Security
Carmen Iannacone, Director, Office of Information Technology Operations
Curtis Lutz, Director, HR & Admin Systems Division
James Douglas, Director, Office of Human Resources
Deb Chaulk, PANDA Project Manager

Subject: OCIO Response to Fiscal Year 2014 FISMA Independent Draft Evaluation Report

Thank you for the opportunity to comment on the Fiscal Year 2014 FISMA Independent Draft Evaluation Report.

Management concurs with the findings and has already completed the recommended actions for many of them. Please see below for specific responses to each of the recommendations.

Please direct any questions you may have regarding the OCIO response to Juliette Sheppard, sheppardj@si.edu, 202-633-5265.

Chief Information Officer
380 Herndon Parkway
Herndon, VA 20170-4881
MRC 1010
202.633.4901 Telephone
202.312.2804 Fax

1. **Strengthen the security assessment and authorization process to align with updated NIST requirements in NIST SP 800-53, Revision 4.**

   Management concurs with this recommendation.

   OCIO is currently revamping the Assessment and Authorization (A&A) process to align with updated NIST and industry best practices. OCIO has invested in a Governance Risk and Compliance (GRC) tool to streamline and standardize A&A and related processes. In FY15, OCIO developed plans for the new processes to be implemented in the tool, selected the tool, and prepared process configuration information to be implemented in the tool. We expect to implement the tool in the first half of FY16 and then migrate SI systems into the tool as they perform their FY16 annual assessments/ reauthorizations. OCIO also began adding the 800-53 rev 4 controls into the existing System Security Plans in FY15.

   Expected completion: December 31, 2016

2. **Require system owners to document and maintain a current and accurate listing of all valid exceptions and waivers applicable to the systems we tested (SInet, WebTA, ArtCIS, MGS-STARS, and PANDA).**

   Management concurs with this recommendation.

   In December 2014, OCIO issued new Technical Note IT-930-TN01, *IT Security Waivers and Exceptions,* to provide policy, procedures, and templates for IT security waivers and exceptions. In addition to requiring systems to track and maintain copies of their waivers and exceptions, the new process also established a central log and repository for waivers and exceptions. A copy of the new technical note and the log have been provided to OIG.

   Expected completion: Already completed

3. **Finalize the ISCM strategy in accordance with NIST SP 800-137.**

   Management concurs with this recommendation.

   The ISCM strategy will be finalized and implemented in conjunction with the implementation of the updated Assessment and Authorization process in the new GRC tool as described in the response to recommendation #1 above.

   Expected completion: December 31, 2016

4. **Implement additional controls to ensure the consistent review of POA&Ms for accuracy and completeness.**

   Management concurs with this recommendation.

   In June 2015, OCIO issued updated Technical Note IT-930-TN29, *IT Security Plans of Actions and Milestones*, which enhanced POA&M tracking instructions, modified the reporting process, defined risk levels and resource estimate levels, and provided an updated template. A copy of the revised technical note has been provided to OIG.

   Expected completion: Already completed

5. **Update the SInet, webTA, ArtCIS, MGS STARS, and PANDA POA&Ms to include cost estimates.**

   Management concurs with this recommendation.

   In June 2015, OCIO issued updated Technical Note IT-930-TN29, *IT Security Plans of Actions and Milestones*, which includes defined risk levels and resource estimate levels. Copies of the latest quarter POA&Ms for these systems, in the new format showing the cost estimates, have been provided to OIG.

   Expected completion: Already completed

6. **Implement additional controls to ensure that system sponsors consistently provide to the Director of IT Security quarterly monitoring and reporting on account management activities and audit log reviews.**

   Management concurs with this recommendation

   OCIO has been working to address A-12-08-05 which provides a similar recommendation for SInet and NMAH CIS. For the WebTA and PANDA systems that are also cited in the finding, we have provided evidence to OIG of these reviews for the past quarter.

   OCIO will be updating these monitoring and reporting procedures as part of the A&A process re-engineering and ISCM implementation (as discussed in responses to #1 and #3 above). The new GRC tool will provide automated reminders and tracking of these activities.

   Expected completion: As part of A-12-08-05, SINET is scheduled for December 31, 2015. PANDA and WebTA have already been addressed. The automated procedure will be implemented by December 31, 2016.

7. **Conduct baseline compliance assessments in accordance with the TSG IT-930-02 *Security Controls Manual.***

   Management concurs with this recommendation.

   OCIO has implemented the CIS scanning tool for Windows baseline scanning and continues to use BladeLogic and TripWire for certain other systems. However, we are in the process of selecting an enterprise baseline scanning solution to use for all systems. Once selected, we will acquire and deploy the tool, and ensure that scans are implemented in accordance with TSG IT-930-02.

   Expected completion: October 31, 2016

8. **Update TN IT-960-TN31 *Security Configuration Management of Baselines* to be consistent with TSG IT-930-02 *Security Controls Manual.***

   Management concurs with this recommendation.

   OCIO plans to update both IT-930-02. *Security Controls Manual* and IT-960-TN31. *Security*

Configuration Management of Baselines. IT-930-02 will be updated as part of the A&A process improvement discussed in the response to recommendation #1. IT-960-TN31 will be updated in accordance with the implementation of an updated baseline compliance scanning process (discussed in response to recommendation #7). We will ensure the two updated documents are in alignment with one another.

Expected completion: October 31, 2016

9. **Revise the *OCIO Request Form for Network/Email* to ensure the form is consistent with the practice for granting access to webTA.**

   Management concurs with this recommendation.

   Employee WebTA access is automatically assigned via the hiring process. HR inputs the employee into HRMS, the employee is added at NFC via a PAR action, and users are added to the webTA active directory group based on a hire in HRMS. Supervisor access is assigned by the Unit HR Admin. Therefore, OCIO has updated the OCIO Request Form for Network/Email form to remove the WebTA check boxes and replace them with a statement about how access is provided. A copy of the updated form has been provided to OIG.

   Expected completion: Already completed

10. **Complete the *webTA Security Form* for all users with privileged access to the webTA system.**

    Management concurs with this recommendation.

    OCIO currently has a security form which must be completed for all users with privileged access to webTA. A copy of the form has been placed in the IG Evidence share. However, some users were grandfathered access when WebTA was implemented. OCIO is creating a list of all grandfathered users and will document approval for those users.

    Expected completion: December 31, 2015

11. **Implement additional controls to consistently grant access after completion of required training as stated in the *PANDA User Access Protocol* and retain training documentation to support a user's system privileges.**

    Management concurs with this recommendation.

    The Office of Advancement (OA) has updated the process for granting access to PANDA. PANDA access privileges are granted based on completion of specific role-based training courses. The enrollment process for these courses has been updated to require supervisor approval in Moodle. A screenshot showing a sample of Moodle approval for the training, as well as a copy of the process for granting access once training has been completed, have been provided to OIG.

    Expected completion: Already completed.

12. Assess whether to implement new procedures to disable accounts that have not been logged into for 90 days or accounts that do not have a last-login date in accordance with IT-930-02, *Security Control Manual.*

Management concurs with this recommendation.

OA has updated the process for reviewing and disabling inactive accounts. Each month, an account report is run. OA reviews the report to look for any accounts which have not been used for 90 days. Emails are sent to those users requesting that they access their accounts within 10 days to keep them active. Another report is then run at the end of the 10 days, and any remaining unused accounts are deactivated. Additionally, OA now receives information on HR actions and disables accounts for any separated personnel. A copy of the procedure document and the most recent PANDA user report have been provided to OIG.

Expected completion: Already completed.

13. Implement additional controls to consistently document MGS STARS access requests to include user name, approval, roles, and user agreements.

Management concurs with this recommendation.

MGS STARS has an access request process that is consistently followed. The process formerly utilized the HRMS Security Request form but was changed in 2011 to use the STARS User ID Request Form. All MGS STARS users were granted access based on requests performed using the process that was in effect at the time of the request. The users cited as non-compliant in this finding are all ones who were granted access during the old process. All users that have been given access since the new process was initiated have used the new forms.

OHR has reviewed all MGS STARS users and verified that all users have user agreements on file. Copies of the MGS STARS Security Forms for the outstanding users in the audit sample have been provided to OIG.

Expected completion: Already completed

14. Maintain user agreements and access request forms in a central repository for all users with access to NFC.

Management concurs with this recommendation.

OHR has updated their NFC records by ensuring that a user agreement is on file for every user. All SI users with access to NFC are required to complete the Authorization and User Confidentiality Acknowledgement form for NFC.

The process for granting access to NFC is:

- NFC access can be granted to HR Specialists, HR Assistants, Payroll, OCIO personnel for purposes of file transmission, contractors assigned to OCIO and OHR.
- Request received from authorized source (HR manager, OCIO manager)

- Upon receipt of request, OHR Security Officer will complete NFC form 3100 for Payroll Personnel Request or NFC form 3100-R for the Reporting Center and submit via Remedy Console a NFC security system. Requests are profile (role) based (from full access such as HR specialists & assistants) to read-only access for certain screens (IRIS/PINQ).
- Upon notification by NFC that the account has been established, user is sent instructions for NFC login information.
- Upon separation from the SI or should user no longer need access, a request is emailed to OHR Security Officer to submit a request to have the NFC user id deleted.

A copy of the current user list has been provided to OIG. We can provide OIG with copies of the forms for any of the users on the list.

Expected completion: Already completed

15. Implement technical controls to require multi-factor authentication for all VPN remote access.

Management concurs with this recommendation.

In February 2015, OCIO completed the implementation of two factor authentication for all VPN users except for one VPN group who has an approved waiver and groups used for VPN testing. A screenshot of the VPN profile configuration has been provided to OIG.

Expected completion: Already completed

16. Update Smithsonian Directive 920, *Life Cycle Management*, to require that legacy systems that are no longer supported are retired and replaced.

Management concurs in with this recommendation.

Instead of updating SD 920, OCIO has issued updated Technical Note IT-930-TN17, *Secure Use and Maintenance of Software,* which requires the replacement or retirement of software that is no longer supported. A copy of the technical note has been provided to OIG.

Expected completion: Already completed

17. Develop a list of software versions that are no longer supported by the manufacturer and a plan to upgrade or replace them.

Management concurs with the finding but not the recommendation.

OCIO is working with the Smithsonian units to identify the unsupported software most commonly installed on Smithsonian computers and help them develop plans for eliminating or replacing those applications. OCIO will also develop processes for monitoring ongoing compliance with the requirements in IT-930-TN17.

Expected completion: October 31, 2016