Smithsonian Institution
Office of the Inspector General

In Brief

Fiscal Year 2015 Independent Evaluation of the Smithsonian Institution's Information Security Program

Report Number OIG-A-16-11, September 30, 2016

What OIG Did

The Office of the Inspector General (OIG) contracted with an independent public accounting firm, CliftonLarsonAllen LLP, to conduct this audit. The objective of this audit was to determine the extent to which the Smithsonian Institution's information security program and practices complied with Federal Information Security Modernization Act (FISMA) requirements, Department of Homeland Security (DHS) reporting requirements, and applicable Office of Management and Budget and National Institute of Standards and Technology guidance.

Background

FISMA was enacted in 2002 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.

FISMA requires organizations to adopt a risk-based, life-cycle approach to improving information security that includes annual security program reviews, independent OIG evaluations, and reporting to DHS and the Congress.

What Was Found

According to CliftonLarsonAllen LLP (CLA), the Smithsonian generally exercised effective management and oversight of its information security program. However, CLA found areas in the information security program that require strengthening. Specifically, CLA found control deficiencies in

- identity management and user access,
- incident response monitoring,
- risk management,
- contractor systems oversight, and
- role-based security training.

For example, CLA identified that 17.9 percent of users had been granted local administrator access on desktop workstations. Administrative access allows the user to perform actions that would otherwise be restricted, such as installing software and changing security settings. Misuse of local administrator access, either intentionally or unintentionally by authorized users, can have significant adverse impacts, such as installing malicious software throughout the organization's network.

In addition, CLA identified a lack of automated analysis and alerting of possible security incidents, such as suspected or actual computer system breaches, from the security monitoring system. This system correlates and analyzes system logs to identify potential security incidents. Without automated analysis and alerting, the ability to detect and respond to security incidents is hindered.

Finally, CLA found that the Smithsonian needs to continue to focus on fully implementing recommendations from prior years, such as maintaining an accurate inventory of hardware and software, establishing a continuous monitoring strategy, and managing system security configurations.

What Was Recommended

CLA made 11 recommendations to address the control deficiencies noted above. Key recommendations included reducing the number of users with desktop administrator access and ensuring that providing alerts for security events is automated. Smithsonian management generally concurred with CLA's recommendations and proposed corrective actions.

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

Smithsonian Institution

Federal Information Security Modernization Act

Audit for Fiscal Year 2015

Table of Contents

Abbreviations

CLA	CliftonLarsonAllen
DHS	Department of Homeland Security
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
HRMS	Human Resources Management System
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
SI	Smithsonian Institution
SIA CMS	Smithsonian Institution Archives Collection Management System
SINet	Smithsonian Institution Network
SOLAA	Smithsonian Online Academic Appointment System

Introduction

The objective of this audit was to determine the extent to which Smithsonian Institution's information security program and practices complied with Federal Information Security Modernization Act (FISMA) requirements[1], Department of Homeland Security (DHS) reporting requirements, and applicable Office of Management and Budget (OMB) and National Institute for Standards and Technology (NIST) guidance. The Smithsonian Institution (SI) Office of Inspector General (OIG) contracted with the independent accounting firm CliftonLarsonAllen LLP to perform the fiscal year (FY) 2015 FISMA audit.

Results In Brief

This report represents the results of our audit of the Smithsonian's information security program and practices. We found that the Smithsonian generally exercised effective management and oversight of the Smithsonian information security program. However, we found areas in the information security program that require strengthening.

Overview

Information security is a high-risk area Government-wide. Congress passed Title III of the E-Government Act of 2002 (Public Law 107-347) as amended[2] in an effort to strengthen Federal information security programs and practices. FISMA provides a comprehensive framework to ensure the effectiveness of security controls over information resources that support Federal operations and assets. CLA assessed SI's information security program through inquiries, observations, and tests of selected controls of three major applications and the general support system. In FY 2015, CLA identified specific deficiencies in these areas:

1. Identity Management and Access Controls
2. Incident Response and Monitoring
3. Risk Management
4. Contractor Systems Oversight
5. Role-based Security Training

This report contains a total of 11 new recommendations for improving SI's information security program. The appendix addresses the status of prior recommendations. SI successfully implemented 14 recommendations in FY 2015.

---

[1] *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).*

[2] *The Federal Information Security Modernization Act of 2014 - Amends the FISMA Act of 2002 to: (1) re-establish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.*

CLA audited the information security program and practices of the following SI systems, during FY 2015:

1. *Smithsonian Institution Network (SINet)* – SINet provides the core capability to the rest of Smithsonian's major applications and miscellaneous IT systems that support the mission and objectives of Smithsonian Institution. The shared infrastructure consist of the hosting environment (servers), numerous productivity applications (email, SharePoint, communication services), SI websites and end user's desktop environment.
2. *Smithsonian Online Academic Appointment System (SOLAA)* – SOLAA provides one common portal and process to accept all academic appointment applications from the public and to provide abilities for the Smithsonian staff to centrally process applications supporting individual units. The system generates required documents for registration of academic appointments and processing of stipend appointments.
3. *Human Resources Management System (HRMS)* – HRMS is used to manage human resource information successfully. Managers throughout the SI will use the Enterprise Resource Planning HRMS system for proactive decision making to manage human capital, and core activities including: recruitment, benefits administration, and electronic transmittal of personnel actions.
4. *Smithsonian Institution Archives Collection Management System (SIA CMS)* – SIA CMS manages the majority of its collections and their associated business processes. It has four major functions: collection registration, collection asset management, process tracking, customer (researcher) service management and metrics.

Results of Audit

Finding 1 Identity Management and Access Controls

The audit team identified security weaknesses in SI's identity management and access controls. SI's Technical Standards & Guidelines IT-930-02, *Security Controls Manual,* provides comprehensive guidelines for authenticating users and protecting SI's critical systems from unauthorized disclosure, modification, or destruction. We identified information security control weaknesses in these areas which impact SINet, SOLAA and HRMS:

- Least Privilege
- Access Management
- Remote Access

Least Privilege

SI has adopted the "principle of least privilege." Least privilege refers to the security objective of granting users only those accesses they need to perform their official duties. However, our testing noted that the "principle of least privilege" was not fully implemented.

We noted that SI has granted 1,768 users Local Administrator access in Active Directory, which equates to 17.9% of 9,871 Active Directory accounts with local administrator rights. The number of Local Administrator access is more than necessary to administer the workstations assigned to the common user. SI was not in compliance with NIST SP 800-53 Rev 4, *AC-2 Account Management* and *AC-6 Least Privilege.*

Furthermore, SI was not in compliance with NIST SP 800-53 Rev 4, *AC-2 Account Management, AC2(j) defines the frequency to review accounts for compliance with account management requirements* and *AC2(j){2} reviews accounts for compliance with account management*. Smithsonian did not perform a recertification of Local Administrator accounts in FY 2015. The review of 25 sample items confirmed there was no recertification of Local Administrators access in FY 2015.

Administrative privileges on SI's workstations allow access to resources that are unavailable to most users and permit the execution of actions that would otherwise be restricted. When such privileges are administered improperly, granted widely, and not closely audited, attackers are able to utilize them to attack the operating system or other devices on the network by installing malicious software. Misuse of Local Administrators access, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations.

Access Management

Access management is the process of adding, changing, and removing user access to the network and various applications. We reviewed 145 users and noted that the process specified in Technical Note IT-960-TN12, *Active Directory Account and Password Request,* was not always followed. Specifically, we noted the following:

- Completed access request forms are not always on file for active users. Our testing of VPN, Citrix, and Active Directory users noted that 8 of 45 did not have an access request form on file. In addition, one VPN user had approved their own access. Additionally, two Active Directory users had access that could not be verified for appropriateness because management could not provide adequate support.
- Accounts are not always disabled after 90 days of inactivity.
    - CLA noted the accounts for 54 Active Directory users were still active after 90 days of inactivity. Additional follow-up on three of these users noted one continued to have access after 120 days of inactivity.
    - CLA noted that 71 SOLAA users had not logged in for over 90 days. CLA performed a discrepancy test and selected a sample of five users. Management could not provide adequate documentation supporting why these five accounts remained active.

      CLA recommended that management put a process in place to disable such accounts. Management determined that since the system is typically only used once a year, this would cause issues. To resolve the recommendation, management formally requested an exception to the 90 day policy, which was granted by the CIO on 6/3/2016.
- Unnecessary accounts are active in SOLAA. CLA noted that 1,028 SOLAA users had no login information. Follow-up with management determined that these are supervisor accounts that are not used for login, but exist in the system so the supervisor can be associated with other individuals. However, when CLA selected a sample of 15 to perform a discrepancy test, CLA noted that four of these accounts were activated and never used (no login recorded).

Unauthorized or inappropriate access exposes SI to the risk of incompatible roles being assigned or controls being bypassed. We also found instances of inactive SINet and SOLAA accounts not disabled after exceeding the allowed timeframe for inactivity. An account that is inactive for a protracted period may not be needed. Eliminating unnecessary accounts from SI's environment reduces the risk of such accounts being exploited.

Remote Access

OMB M-06-16, *Protection of Sensitive Agency Information*, recommends a time-out function for remote access and mobile devices that requires users to re-authenticate after 30 minutes of inactivity. Per review of remote access configurations, we noted that configurations allowed remote accounts to remain idle over the recommended timeframe. Inactive accounts could be accessed by unauthorized users to conduct unauthorized transactions.

Recommendations:

We recommend that the Chief Information Officer (CIO):

SINet

1. On a defined frequency, review the current use of local administrator access to ensure access is granted with proper justification and need. In cases where there is a need, split the local administrator privilege into a separate account and remove the privileges for file server/website access. Ensure users with local administrator privilege receive adequate training and understand the responsibilities for having local administrator privilege, such as not using their local administrator access for routine, everyday access and login.
2. Ensure access requests are properly documented, justified, and authorized prior to granting access.
3. Implement an automated control to disable/remove stale accounts.
4. Maintain proper configurations for idle connection time outs and confirm configurations are set properly at least annually.

SOLAA

5. We recommend that the system owner develop and implement procedures to manage SOLAA supervisor accounts in accordance with SI's policies.

Finding 2 Incident Response and Monitoring

SI's incident response program needs improvement. SI uses an application to log and manage security events in its environment. The application can be used to analyze data from several log sources, correlate security events among log entries, identify and prioritize significant events, and initiate responses to security events.

However, SI's security event log management application was not properly configured to provide alerts to SI's security staff of possible security events for review and analysis. By not ensuring adequate communication of incidents or having automated alert mechanism in place, SI's ability to detect, identify, and respond to suspected or actual breaches of a computer application system or network is impaired.

Further, SI did not report all incidents to the United States Computer Emergency Readiness Team (US-CERT) within the appropriate timeframe it established within IT-930-TN30, *IT Security Incident Response Procedures*. Management did not provide adequate oversight for ensuring the Security Operations Center (SOC) reported incidents to US-CERT within the established timeframes. Timely notification is important because incidents reported to US-CERT are correlated with other agencies' reports to identify real-time, zero-day incidents.

Recommendation:

We recommend that the CIO:

6. Ensure that security events are correlated and alerts are automated if an incident or abnormal activity is detected.
7. Provide management oversight to ensure incidents are reported in US-CERT in SI's established timeframes.

Finding 3 Risk Management

SI does not have a complete inventory of systems operated on its behalf by contractors, other government agencies, or other third parties, including the SI's systems and services residing in public, hybrid, or private cloud. Technical Note IT-930-TN34, *IT Security System Inventory*, requires SI to have a comprehensive and accurate system inventory. Our testing also noted that SI did not identify system interfaces in the inventory of Smithsonian-operated systems. Without an accurate inventory of systems and system interfaces, SI cannot ensure it is applying appropriate security controls nor can it verify all security controls that protect SI information are effective.

Recommendations:

We recommend that the CIO:

8. Complete the implementation of the system inventorying process as outlined in the Technical Note IT-930-TN34, *IT Security System Inventory*.

Finding 4 Contractor Systems Oversight

In FY 2015, SI did not fully implement contractor oversight procedures as required by FISMA. According to FISMA, Section 3544, an agency should ensure adequate information security for systems that support its operations, including those provided by another agency, contractor, or other source. In addition, SI's Technical Standards & Guidelines IT-930-02, *Security Controls Manual,* provides requirements on contractor systems oversight and the establishment of security requirements for all outsourced information system services. In spite of these requirements, CLA identified two deficiencies in SI's contractor oversight activities in FY 2015. Specifically:

- SI did not have an effective program and practices to provide guidance on contracting and monitoring cloud computing services and to ensure services are performed effectively, efficiently, and securely.
- SI did not provide signed interconnection security agreements.

For two cloud systems, the terms and conditions includes a blanket statement that requires the contractor to comply with applicable Federal, State and local laws; executive orders; rules; and regulations applicable to the performance under the contract. However, the terms and conditions did not provide proper direction for Smithsonian personnel to monitor the performance nor security of the host cloud environment. Without implementing effective oversight mechanisms, SI cannot ensure that contractor security controls adequately protect sensitive systems and data in accordance with its information security requirements.

Recommendations:

We recommend that the CIO:

9. Develop and implement policies and procedures, including contract terms and conditions, for monitoring security controls performed by cloud system providers.
10. Review interconnection security agreements to ensure that all documented connections have an agreement in place and that the agreement is current and valid.

Finding 5 Role-based Security Training

SI has not fully implemented an effective process to track role-based security training. A robust security awareness and training program is principal to ensuring that people understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them. While broad-based awareness initiatives delivered to the workforce provide the rules of good security practices, high trust/high impact positions (e.g., IT security program managers, security officers, and system administrators) require role-based training. Role-based training provides the information required for an individual to perform the IT security responsibilities specific to the individual's role at the Smithsonian based on their knowledge, skills and abilities.

Our review of 15 individuals with significant IT security responsibilities noted that three had not completed specialized role based security training. Untrained security personnel may not be able to remediate or mitigate risks associated with various security incidents or events.

Smithsonian management recognized the need for such training and published a new Technical Note titled *Specialized Security Training,* which took effect on October 22, 2015. It requires external training certificates to be provided to the Information Technology Security Staff by September 30th of the fiscal year. While it was not in effect during FY 2015, the Security Controls Manual (IT-930-02) required role-based training.

Role-based training should be delivered before the individual is given access to the system, when there are changes to the information system, and on a defined frequency thereafter. Retention of individual training records should be maintained for a defined time period.

Recommendations:

We recommend that the CIO:

11. Fully implement the new IT-930-TN36 *Specialized Security Training* to ensure personnel with significant security responsibilities complete role-based training and meet specialized IT security training requirements.

Appendix A Status of Prior-Year Recommendations, as of August 15, 2016

Appendix A addresses the status of outstanding recommendations not included in the main report and SI's plans for corrective action. As noted in the table below, some recommendations remain in progress, with estimated completion dates still to be determined. The corrective actions outlined below are based on management assertions and results of our audit testing.

Report	Finding	Recommendation	Current Status
FY2012 FISMA Evaluation Report Audit #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.	Open. Target date revised to November 2016.
FY2014 FISMA Evaluation Report Audit #A-16-02 Issued December 14, 2015	We noted weaknesses in the OCIO's security assessment and authorization process in the following areas: baseline security control, common controls, system security plans, and security control assessment. Not addressing these issues could increase the vulnerability of Smithsonian systems to IT security risks.	Strengthen the security assessment and authorization process to align with updated NIST requirements in NIST SP 800-53, Revision 4.	Open. Target date revised to December 2016.
	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.*	Finalize the ISCM strategy in accordance with NIST SP 800-137.	Open. Target date revised to December 2016.
	On a quarterly basis, units are responsible for submitting to the OCIO evidence of their compliance activities to maintain IT security authorization. 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*.	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.	Open. Target date was December 2016.

Report	Finding	Recommendation	Current Status
	The OCIO did not conduct a configuration baseline compliance assessment for SINet in FY 2014.	Conduct baseline compliance assessments in accordance with the TSG IT-930-02 *Security Controls Manual*.	Open. Target date is October 2016.
	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.	Update TN IT-960-TN31 *Security Configuration Management* of Baselines to be consistent with TSG IT-930-02 *Security Controls Manual*.	Open. Target date is October 2016.
	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.	Develop a list of software versions that are no longer supported by the manufacturer and a plan to upgrade or replace them.	Open. Target date revised to December 2016.

Appendix B Background

On December 18, 2014, President Barack Obama signed the Federal Information Security Modernization Act (FISMA), which amends the Federal Information Security Management Act of 2002 to reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices and to set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for 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 provides a comprehensive framework for ensuring effective security controls over information resources supporting Federal operations and assets. The statute also provides a mechanism for improved oversight of Federal agency information security programs. FISMA requires each Federal agency to develop, document, and implement an agency-wide security program. Agency-wide security program plans are also to include procedures for responding to security incidents, and require each agency to notify Congress of a major security incident within seven days.

Federal agencies are to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by the agency. As specified in FISMA, the agency Chief Information Officer or senior official is to oversee the development and maintenance of security operations that continuously monitor and evaluate risks and threats.

FISMA also requires agency Inspectors General to assess the effectiveness of agency information security programs and practices. Guidance has been issued by OMB and by National Institute of Standards and Technology in its 800 series of Special Publications supporting FISMA implementation. In addition, Federal Information Processing Standards was issued to establish agency baseline security requirements.

OMB and DHS provide instructions to Federal agencies and Inspectors General for preparing annual FISMA reports. In October 2015, OMB issued Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*. The memorandum establishes current Administration information security priorities and also provides agencies with Fiscal Year 2015 and 2016 FISMA and Privacy Management reporting guidance. Federal agencies are to focus on implementing the Administration's three cybersecurity priorities:

- Agencies must respond to security posture questions on a quarterly and annual basis.
- Chief Information Officers should submit monthly data through CyberScope, the FISMA reporting application.

- The Chief Information Officers must report to DHS on a quarterly basis, and Inspectors General and Senior Agency Officials for Privacy must report to DHS on an annual basis.
- Agencies must participate in CyberStat accountability sessions and agency interviews conducted by DHS, OMB, and the White House National Security Staff.

DHS reporting instructions also focus on performance metrics related to key control activities such as information security continuous monitoring, configuration management, identity and access management, incident response and reporting, risk management, security training, corrective actions, remote access management, contingency planning, and contractor systems.

In 2015, DHS's FISMA reporting guidance for Inspectors General was updated to remove the security capital planning controls and to include a maturity model to use in assessing the effectiveness of agencies' continuous monitoring programs. SI OIG contracted with the independent accounting firm CliftonLarsonAllen LLP to conduct the annual FISMA audit for FY 2015. SI OIG provided oversight of the contractor's performance.

Appendix C Scope and Methodology

The objective of this audit was to determine the extent to which SI's information security program complied with FISMA requirements and relevant guidelines. CLA's audit team considered Federal Information Processing Standards and National Institute of Standards and Technology guidance during its audit. Audit procedures included reviewing policies and procedures, interviewing employees, reviewing and analyzing records, and reviewing supporting documentation. SI OIG provided oversight of the audit team's performance.

This year's work included evaluation of selected major applications and general support systems. The CLA audit team performed a vulnerability assessment and evaluated management, operational, and technical controls supporting major applications and general support system. We audited the information security program and practices of the following SI systems:

1. Smithsonian Institution Network
2. Smithsonian Online Academic Appointment System
3. Human Resources Management System
4. Smithsonian Institution Archives Collection Management System

We conducted this performance audit in accordance with U. S. generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix D Management Comments

Smithsonian Institution

Office of the Chief Information Officer

Date: September 9, 2016

To: Cathy L. Helm, Inspector General

From: Deron Burba, Chief Information Officer
Juliette Sheppard, Chief Information Security 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
Chuck Mitchell, Office of Inspector General
Joseph Benham, Office of Inspector General
Juliette Sheppard, Director of IT Security
Carmen Iannacone, Chief Technology Officer
Cindy Zarate, Office of the Chief Financial Officer
Stone Kelly, Office of Planning, Management and Budget

Subject: OCIO Response to the report on the FISMA Audit for Fiscal Year 2015

Thank you for the opportunity to comment on the report of the FISMA Audit for Fiscal Year 2015.

The Smithsonian is not required to comply with FISMA because we are not an executive branch agency. However, we apply FISMA standards as best practices to the extent practicable and consistent with the Smithsonian's mission.

Management concurs with most but not all of the findings, and has already completed recommended actions for some 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. **On a defined frequency, review the current use of local administrator access to ensure access is granted with proper justification and need. In cases where there is a need, split the local administrator privilege into a separate account and remove the privileges for file server/website access. Ensure users with local administrator privilege receive adequate training and understand the responsibilities for having local administrator privilege, such as not using their local administrator access for routine, everyday access and login.**

   The Smithsonian will review and update local administrator account management procedures to ensure that these privileges are only granted with appropriate justification and that the need for local administrative privileges is periodically reviewed. We will also evaluate whether there are additional measures that would be appropriate to take in the Smithsonian environment to further mitigate risk. The review and update of procedures for granting and recertifying local administrator privileges will be completed by December 31, 2017

2. **Ensure access requests are properly documented, justified, and authorized prior to granting access.**

   Within the Smithsonian, the majority of access to IT resources is managed via Active Directory (AD) accounts. The Smithsonian is currently in the process of reviewing and updating procedures for granting and modifying AD user accounts, as well as the procedures for granting administration privileges to AD, servers, and network devices. These procedure updates are expected to be completed by August 31, 2017

3. **Implement an automated control to disable/remove stale accounts.**

   The Smithsonian will adjust its procedures for disabling inactive accounts to make the process more automated. We expect to complete this change by December 31, 2016.

4. **Maintain proper configurations for idle connection time outs and confirm configurations are set properly at least annually.**

   As part of the continuous assessment part of the revised Assessment and Authorization Process being implemented, this control will be assessed on an annual basis. This has been documented in the revised IT-930-02 Security Controls Manual. We expect the SINET system for which this was a finding to be migrated to the new A&A process by March 31, 2017.

5. **We recommend that the system owner develop and implement procedures to manage SOLAA supervisor accounts in accordance with SI's policies.**

   The Smithsonian will establish a procedure that periodically identifies the SOLAA supervisor accounts that were activated and resets the identified accounts so that they will not be able to access the SOLAA STAFF system. This is expected to be completed by March 31, 2017.

6. **Ensure that security events are correlated and alerts are automated if an incident or abnormal activity is detected.**

   The Smithsonian has a number of tools that provide automated monitoring and alerts of security event information. Some of these are automatically correlated and some require manual correlation. As part of our ISCM strategy planning, we are evaluating the need for further automation of monitoring, correlation, and alert capabilities. Implementation of additional tools determined to be needed will be dependent on additional budget funding. This will be completed as part of existing IG recommendation A-16-02-3.

7. **Provide management oversight to ensure incidents are reported in US-CERT in SI's established timeframes.**

   Management generally concurs that submitting incidents to US-CERT within the documented timeframes is important, however occasionally there is a low priority incident that doesn't get reported within the timeframes due to either prioritization of more critical tasks or not yet having sufficient incident investigation information to make a useful US-CERT report. Management does not consider this to cause any significant risk because the reports of these types of incidents is only used in US-CERT statistical reporting and does not have any impact on the resolution of the incidents. Further, strict adherence to timeframes could actually increase risk by providing incomplete/misleading information to US-CERT and diverting resources from more critical tasks. Therefore, management believes the risk of missing an occasional US-CERT reporting timeframe for reporting incidents that do not require US-CERT assistance, and do not have an impact on other federal organizations, is and does not warrant an additional layer of control. Expected completion: N/A

8. **Complete the implementation of the system inventorying process as outlined in the Technical Note IT-930-TN34, IT Security System Inventory.**

   Management concurs with the need to conduct a complete inventory of Smithsonian systems. This inventory will be conducted in the new Security Assessment and Authorization (A&A) tool and in accordance with the inventory requirements in the new IT-930-03 A&A Procedures document which replaces IT-930-TN34. The initial SI-wide system inventory is expected to be completed by December 31, 2017

9. **Develop and implement policies and procedures, including contract terms and conditions, for monitoring security controls performed by cloud system providers.**

   The Smithsonian applies the same requirements to all systems whether internally or externally hosted. Security for cloud systems is assessed and monitored using the same Security Assessment and Authorization (A&A), Technical Review Board (TRB), Privacy Assessment, and other relevant processes as other types of systems. The recent revision of the A&A procedures makes the applicability of these requirements to cloud systems more explicit. The implementation of these procedures is included in finding A-16-02-1.

   Additionally, the Smithsonian has drafted an updated set of standard privacy and security contract clauses to be used with all contracts to ensure that compliance with these

requirements is mandatory. The clauses are currently in the approval stage and are expected to be implemented by January 31, 2017.

10. Review interconnection security agreements to ensure that all documented connections have an agreement in place and that the agreement is current and valid.

The Smithsonian requires Interconnection Security Agreements between Smithsonian-hosted systems and externally hosted systems to which they have interconnections. Management will review all documented interconnections to ensure compliance with this requirement and to verify that such agreements are current. We will complete this by August 31, 2017

11. Fully implement the new IT-930-TN36 Specialized Security Training to ensure personnel with significant security responsibilities complete role-based training and meet specialized IT security training requirements.

Management believes this recommendation is already completed. A new policy and process for role-based specialized security training was issued, prior to the audit, to proactively address role based training. The policy specifies training requirements for different roles, as well as tracking and reporting procedures. Additional training courses have been made available for personnel to meet the requirements, as well as recommendations on other acceptable training sources. The list of SI personnel required to complete training and the training requirements for each person have been determined, and their progress in meeting the requirements is being tracked. To date, we have tracked more than 3000 completed training events for the affected personnel. Additionally, periodic status reminders are sent to all affected personnel. Expected completion: Already completed