Smithsonian Institution
Office of the Inspector General

In Brief

Smithsonian Enterprises: Audit of the Effectiveness of the Information Security Program

Report Number OIG-A-16-05, March 25, 2016

What OIG Did

OIG contracted with an independent public accounting firm, Crowe Horwath LLP (Crowe), to conduct this audit. The audit objective was to evaluate the effectiveness of Smithsonian Enterprises' (SE) information security program and practices as well as SE's compliance with the Payment Card Industry Data Security Standard (PCI DSS).

Background

In 1998, the Smithsonian organized its various business activities into a centralized entity known as SE. SE operates a variety of revenue-generating activities including museum stores, a mail-order gift catalog and websites, three IMAX theaters, magazines, licensing, and media.

Crowe completed an information security risk assessment on a sample of servers and network devices across the SE corporate and retail networks, which are a subset of Smithsonian's corporate network (SInet). Crowe completed an internal penetration assessment across SInet and the SE corporate and retail environments, testing approximately 5,000 devices (servers, workstations, and printers) for vulnerabilities. Crowe also completed a PCI DSS gap assessment.

What Was Found

Crowe found that improvements are needed to address vulnerabilities in four key areas: (1) identity and access management, (2) configuration management, (3) information stored on unencrypted laptops and backup tapes, and (4) unsupported systems.

Identity and access management is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons. In its testing, Crowe was able to guess the passwords for some user accounts and to identify multiple accounts that shared the same password. Furthermore, Crowe found that the SE corporate network could be at risk due to systems with weak passwords on the Smithsonian network, SInet.

Configuration management is a collection of activities focused on establishing and maintaining the integrity of information technology products and information systems. This is accomplished through control of processes for initializing, changing, and monitoring the configurations of those products and systems. Crowe found that SE was utilizing insecure communication protocols on its networks. Additionally, a component of point-of-sale system had a vulnerability that could be used to harvest credit card data, known as skimming.

Information stored on laptop computers and backup tapes can be vulnerable to breaches in confidentiality and integrity. SE adopted an industry standard in 2014 to encrypt new laptops to prevent unauthorized access. However, Crowe found that only 16 of 104 existing laptops were encrypted because employees were encouraged, not required, to have existing laptops encrypted. Crowe also found that backup tapes sent for off-site storage were not encrypted.

Unsupported systems are those that need to be replaced because support for the systems' components is no longer available from the developer, vendor, or manufacturer. Crowe identified some systems were using obsolete, unsupported software. In addition, some servers on the SInet network were running unsupported operating systems, and a network monitoring device was outdated and not receiving updates.

What Was Recommended

Crowe made recommendations to strengthen password requirements, disable insecure communications protocols, disable an insecure card reader function, encrypt mobile media, and replace or update servers that had unsupported operating systems. Smithsonian management concurred with the findings and said that they have addressed or plan to address all the recommendations.

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

Crowe Horwath

The Unique Alternative to the Big Four®

Smithsonian Enterprises

Audit of the Effectiveness of the Information Security Program

Performed by Crowe Horwath LLP
March 2016

Smithsonian Enterprises

Audit of the Effectiveness of the Information Security Program

Table of Contents

I. Introduction

This report presents the results of the audit of the information security program of Smithsonian Enterprises (SE) conducted by Crowe Horwath LLP (Crowe), an independent audit, advisory, and public accounting firm.

The objective of this audit was to evaluate the effectiveness of Smithsonian Enterprises' (SE) information security program and practices as well as SE's compliance with the Payment Card Industry Data Security Standard (PCI DSS). We did this through (1) an information security risk assessment; (2) an internal penetration assessment; and, (3) a Payment Card Industry Data Security Standard ("PCI DSS") gap assessment.

Information Security Risk Assessment – We evaluated SE's security controls through a series of interviews, documentation reviews, process walk-throughs, and detailed testing on a sample basis. Testing was performed around the following areas:

- Policies and Procedures
- Network Access Procedures
- Network Operations
- Windows and Active Directory Security
- Anti-Virus Security
- Workstation Security
- Network Architecture Security
- SQL Server Security

Internal Penetration Assessment – We evaluated SE's ability to resist attacks from internal threats and from outsiders able to gain access to the internal network. During the assessment, we passively monitored network traffic, performed scans to identify potential targets, completed vulnerability scans of target systems, manually verified vulnerabilities, and evaluated the potential impact of the verified vulnerabilities.

Payment Card Industry Data Security Standard ("PCI DSS") Gap Assessment – We evaluated SE's controls in place to satisfy the requirements within the PCI DSS. This was completed through a series of interviews, documentation reviews, process walk-throughs, and detailed testing on a sample basis.

Appendix A contains a detailed outline of our objective, scope, and methodology.

Appendix B contains management responses from SE and the Smithsonian Office of the Chief Information Officer. Management concurred with our recommendations.

II. Background

The Smithsonian was founded in 1846 according to the will of Englishman James Smithson, who bequeathed the whole of his property to the United States with the mission "to found at Washington, under the name of the Smithsonian Institution, an establishment for the increase and diffusion of knowledge." In the 160 plus years since that time the Smithsonian has grown into the world's largest museum and research complex of museums, research centers, and offices to include 19 museums, the National Zoological Park, and 9 research centers.

In 1998, the Smithsonian organized the various business activities into a centralized business entity, now known as Smithsonian Enterprises. Smithsonian Enterprises operates a variety of revenue generating activities including museum stores, the mail-order gift catalog and websites, three IMAX theaters, the Smithsonian and Air and Space magazines, licensing, media, and others. As an entity established for the purpose of generating income for the Smithsonian, Smithsonian Enterprises operates with substantial flexibility and independence from the Smithsonian.

The Smithsonian Office of the Inspector General engaged Crowe to conduct an audit to evaluate the effectiveness of the Smithsonian Enterprises information security program and practices.

This audit considered practices and standards including:

- Smithsonian Enterprises information security and privacy policies and procedures;
- the Payment Card Industry Data Security Standard ("PCI DSS"), version 3.0; and,
- National Institute of Standards and Technology ("NIST") information security policies, procedures, and standards.

III. Results of Audit

We completed a detailed information security risk assessment that encompassed a sample of 6 servers and 5 network devices across the corporate and retail networks. In addition, we completed an internal penetration assessment across the Smithsonian's SInet, and the SE corporate and retail environments, testing approximately 5,000 devices (including servers, workstations, printers, and other devices) for vulnerabilities. This report presents our findings and recommendations for SE's information security program.

Finding #1: *Identity and Access Management*

Identity and access management is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons.

According to NIST guidance on identity and access management,[1] organizations should enforce complex, strong passwords and password lifetime restrictions and prohibit password reuse. Organizations should also change default passwords before system components are installed. Further, organizations should employ the principle of least privilege, allowing only the access required for users or system services to accomplish their assigned tasks in accordance with their organization's mission and business functions.[2] PCI DSS requires all users have a unique ID before they are allowed access to system components or cardholder data and that there are no shared or generic IDs.[3] As a result of our testing, we found issues with both password management and the enforcement of least privilege.

Weak Passwords

During testing, we were able to guess the passwords for 13 user accounts out of approximately 9,775 active accounts on the Smithsonian's networks. One non-administrative account was using a password that was the same as the username. In addition, we found that the initial password created for new user accounts and password resets was the same for all employees. Weak and easily guessable passwords increase the likelihood that an attacker can successfully guess credentials and obtain access to network resources.

Shared Passwords

SE did not have a process in place to create unique passwords or enforce unique passwords for all accounts on SE's networks. During testing of password controls on SE's network, we identified five passwords for administrator accounts on one network that were the same passwords as for administrator and service accounts on another network. We also determined that one domain user account had the same password as the password for a local administrator account on multiple workstations. Forty-four servers were configured with the same password, and the password for a database administrator account was the same as the password for a local administrator account on multiple workstations. Shared accounts are also used for the initial login in the retail environment for point-of-sale systems, and while this is mitigated through the use of unique application accounts to track individual user activity, the controls are not documented. When user accounts in multiple systems use the same passwords, the

[1] NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Appendix F, "IA-5: Authenticator Management." [[Q: Assumed this was referring to the info in Appendix F: Security Control Catalog, so I set this up (and others that follow) so it directs readers to the correct section in the publication.]]

[2] NIST Special Publication 800-53, Revision 4, Appendix F, "AC-6: Least Privilege."

[3] Payment Card Industry (PCI) Data Security Standard, Version 3.0, *Requirements and Security Assessment Procedures*, "Requirement 8: Identify and authenticate access to system components."

compromise of one system can allow an attacker or unauthorized user to compromise other systems. Although NIST guidance indicates that this is a supplemental control that is not required, we consider this to be a significant risk. SE should consider implementing safeguards to manage the risk of compromise due to individuals having accounts on multiple systems.

The SE corporate network resides on the Smithsonian's network, SInet, which enforces password policies. As a consequence, the SE corporate network may be at risk due to systems with weak passwords on the Smithsonian's SInet.

Recommendations

To strengthen identity and access management, we recommend that the Smithsonian CIO:

1. Require all SI and SE accounts to use unique, complex passwords consisting of at least eight characters, containing numbers, letters, and special characters. Whenever a new password is created, whether for a new user or password change request, it should follow the same password parameters.

We recommend that SE:

2. Document the compensating controls to satisfy the PCI DSS control objectives for identity and access management to include the following key points:
    - Constraints
    - Objective
    - Identified Risk
    - Definition of Compensating Controls
    - Validation of Compensating Controls
    - Maintenance

3. Train users of the SE corporate network to use complex passwords.

Finding #2: ***Configuration Management***

NIST defines configuration management as a collection of activities focused on establishing and maintaining the integrity of information technology products and information systems through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.[4] According to NIST guidance on configuration management, the organization should establish configuration settings that reflect the most restrictive necessary,[5] providing only essential capabilities.[6] As a result of our testing, we found issues with insecure communications protocols and an insecure point of sale keyboard.

Insecure Communication Protocols

SE was utilizing insecure communication protocols on its networks. These protocols are susceptible to network redirection–based attacks that can be used to intercept traffic between computers. Leveraging this vulnerability, we were able to intercept traffic containing username and password information, which could be used to log in to SE servers and network shares. This is also in violation of PCI DSS 3.0 Section

[4] NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Appendix F, "IA-5: Authenticator Management."
[5] NIST Special Publication 800-53, Revision 4, Appendix F, "CM-6: Configuration Settings."
[6] NIST Special Publication 800-53, Revision 4, Appendix F, "CM-7: Least Functionality."

1.1.6.b[7], which requires the organization to identify allowed insecure services, protocols, and ports and verify that security features are documented for each.

Insecure Technology Solutions
SE was utilizing a point of sale keyboard in the theater point of sale system, which can have issues in which a card swipe produces clear text of the payment card track data. This may be used to harvest credit card data, similar to a "skimming" approach. This is also in violation of PCI DSS 3.0 Section 3.4[8] which requires that the data be rendered unreadable.

The SE corporate network resides on the Smithsonian SInet network, where there are shared firewalls, routers and switches. Any network element managed by SI must be changed by SI.

Recommendations
To strengthen configuration management, we recommend that SE:

4. In coordination with the Smithsonian CIO, identify and disable all insecure protocols on the network to protect against network-based attacks.
5. Consider disabling the keyboard magnetic reader when the point of sale application is not waiting to process a card number.

Finding #3: ***Protection of Information at Rest***

According to NIST guidance, an organization needs to address the confidentiality and integrity of information at rest, such as that stored on laptop computers or on backup tapes. If a laptop computer or backup tape is lost or stolen, unauthorized users can easily obtain the information contained on them.[9] For example, a laptop computer was stolen from an employee of another government organization in 2006. That laptop computer contained unencrypted sensitive information for about 26.5 million people. The organization settled a lawsuit for $20 million and had to provide credit monitoring for those affected.[10] One of the methods to manage this risk is to encrypt the information. If the information is properly encrypted, it is impossible, or at least impractical, for an unauthorized user to access it. The Smithsonian issued policies requiring devices containing sensitive data be encrypted.[11]

Unencrypted Systems and Media
SE adopted an industry standard solution to encrypt new laptops; however, existing laptops were not required to be encrypted. Employees were encouraged to bring their laptops to SE's information technology department to get encrypted, but it was not required. As such, only 16 out of 104 (15.4%) existing laptops were encrypted. In addition, SE was not encrypting backup tapes that were taken to offsite storage.

---

[7] PCI DSS 3.0 Section 1.1.6.b- Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service.
[8] PCI DSS 3.0 Section 3.4- Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs)
[9] NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Appendix F, "SC-28: Protection of Information at Rest."
[10] *VA will pay $20 million to settle lawsuit over stolen laptop's data,* retrieved from http://www.cnn.com/2009/POLITICS/01/27/va.data.theft/ on September 18, 2015.
[11] Smithsonian IT-930-TN28, *Encrypting Sensitive Information on Mobile Devices and Removable Media,* June 25, 2014.

Recommendations

To strengthen protection measures, we recommend that SE:

6. Encrypt all mobile media, including laptops and backup tapes, to protect against unauthorized information disclosure in the event of loss or theft.

Finding #4: *Unsupported System Components*

According to NIST guidance, an organization needs to replace information system components when support for the components is no longer available from the developer, vendor, or manufacturer.[12] Support for information system components generally includes software patches to address security vulnerabilities. Unsupported components provide an opportunity for attackers to exploit newly discovered security weaknesses. Organizations need to plan to replace system components before they become unsupported. This is also in violation of PCI DSS 3.0 Section 6.2[13], which requires that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches.

Outdated Technology Platforms

We performed a vulnerability scan of the whole SInet network of which SE is a subset. We found outdated systems and software across the network. We identified 625 systems (out of a total of 11,460) running operating systems that were unsupported and no longer received security updates. In addition, the system monitoring internal and external traffic for potentially malicious activity was outdated and had not received any new updates since July 2013. SE Management stated in December 2015 that there were no outdated systems on the SE network as they have been remediated since the scan was performed. According to SE management, the outdated systems belong to other units of the Smithsonian and not to SE. However, these vulnerable outdated systems could be the starting point for an attack against SE.

Recommendations

To protect the unsupported system components, we recommend that the Smithsonian CIO:

7. Update all servers and workstations to operating systems that are supported by the vendor. If a system cannot be upgraded, it should be replaced or segmented from the rest of the network and enhanced hardening and monitoring controls should be implemented.

[12] NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Appendix F, "SA-22: Unsupported System Components."
[13] PCI DSS 3.0 6.2: ensure all system components are protected from known vulnerabilities by installing applicable vendor-supplied security patches.

IV. Appendix A – Objective, Scope, and Methodology

The objective of this audit was to evaluate the effectiveness of Smithsonian Enterprises' (SE) information security program and practices as well as SE's compliance with the Payment Card Industry Data Security Standard (PCI DSS). We did this by assessing SE's compliance with (1) its security policies, standards, and guidelines; (2) the standards and guidelines promulgated by the National Institute of Standards and Technology; and (3) PCI DSS version 3.0.

This audit was prepared based on information available as of September 20, 2015.

Crowe Horwath LLP (Crowe) audited SE's information security program and PCI compliance on behalf of the Office of the Inspector General (OIG). Our work covered all three project tasks: information security risk assessment, internal penetration assessment, and PCI DSS gap assessment.

Our methodology included a series of interviews, documentation reviews, process walk-throughs, and detailed testing on a sample basis. An information security risk assessment was performed around the following areas:

- Policies and Procedures
- Network Access Procedures
- Network Operations
- Windows and Active Directory Security
- Anti-Virus Security
- Workstation Security
- Network Architecture Security
- SQL Server Security

The internal penetration assessment was conducted through detailed testing of the Smithsonian's SInet network and SE's network systems. Crowe was provided a list of approximately 40 active subnetworks on the internal network to include in testing. Over the course of the assessment, approximately 5,000 devices (including servers, workstations, printers and other devices) were identified on the internal network and were assessed for vulnerabilities.

The PCI DSS gap assessment was completed through a series of interviews, documentation reviews, process walk-throughs, and detailed testing on a sample basis. We evaluated the current control environment against PCI DSS version 3.0.

We provided other low to moderate risk issues that offer additional opportunities for improvement to management at the conclusion of the engagement. We provided detailed testing results to management to assist them in addressing the identified vulnerabilities.

The specific procedures performed were based on the concepts of selective testing. Although Crowe's testing was performed in some areas without exception, Crowe can provide no assurance that exceptions would not have been detected had procedures been changed or expanded.

It should also be recognized that internal controls are designed to provide reasonable, but not absolute, assurance that errors and irregularities will not occur and that procedures are performed in accordance with management's intentions. There are inherent limitations that should be recognized in considering the potential effectiveness of any system of internal controls. In the performance of most control procedures, errors can result from misunderstanding of instructions, mistakes in judgment, carelessness, or other factors. Internal control procedures can be circumvented intentionally by management with respect to the execution and recording of transactions or with respect to the estimates and judgments required in the processing of data. Controls may become ineffective due to newly identified business or technology exposures. Further, the projection of any evaluation of internal control to future periods is subject to the risk that the procedures may become inadequate because of changes in conditions and that the degree of compliance with procedures may deteriorate.

We conducted the fieldwork for this performance audit in Washington, DC, from February 2015 through March 2015. We conducted our audit in accordance with generally accepted government auditing standards (GAGAS) issued by the Comptroller General of the United States. 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. Because of inherent limitations of an audit, together with the inherent limitations of internal control, an unavoidable risk that some material misstatements or material non-compliance may not be detected exists, even though the audit is properly planned and performed in accordance with applicable standards. An audit is not designed to detect error or fraud that is immaterial to the performance audit objectives.

V. Appendix B – Management's Response

Smithsonian Enterprises

Christopher A. Liedel
President

Date: February 11, 2016

To: Cathy L. Helm, Inspector General

From: Christopher A. Liedel, President, Smithsonian Enterprises

Cc: Al Horvath, Under Secretary for Finance and Administration / Chief Financial Officer
William Hoyt, Office of Inspector General
Bruce Gallus, Office of Inspector General
Bruce Dauer, Chief Financial Officer, Smithsonian Enterprises
Grace Clark, Chief Information Officer, Smithsonian Enterprises

Subject: Smithsonian Enterprises' (SE) Response to SE Audit of the Effectiveness of the Information Security Program

Thank you for the opportunity to comment on the Smithsonian Enterprises Audit of the Effectiveness of the Information Security Program. This document is the SE Management Response to the "Audit of the Effectiveness of the Information Security Program" recommendations dated February 2016.

Please direct any questions you may have regarding the SE response to Grace Clark, gclark@si.edu, 202-633-4952.

Smithsonian Enterprises
Office of the President
600 Maryland Ave SW, MRC 513
Washington DC 20024
202-633-5169 Telephone
202-633-6083 Fax

Finding #1: ***Identity and Access Management***

Recommendations

To strengthen identity and access management, we recommend that the Smithsonian CIO:

1. Require all SI and SE accounts to use unique, complex passwords consisting of at least eight characters, containing numbers, letters, and special characters. Whenever a new password is created, whether for a new user or password change request, it should follow the same password parameters.

SE Management Response: We concur with this finding.

- **All domain accounts already meet complex password requirements listed above. (Completed)**
- **All local administrator account passwords have been changed to unique complex passwords for each individual server. (Completed)**
- **We will implement a procedural change to ensure all new passwords created are unique and meet complex password requirements listed above. (Estimated Completion March 31, 2016)**

We recommend that SE:

2. Document the compensating controls to satisfy the PCI DSS control objectives for identity and access management to include the following key points:
   - Constraints
   - Objective
   - Identified Risk
   - Definition of Compensating Controls
   - Validation of Compensating Controls
   - Maintenance

SE Management Response: We concur with this finding.

- **A compensating control document has been created that outlines SE's use of generic accounts in the SE Retail domain. (Completed)**

3. Train users of the SE corporate network to use complex passwords.

SE Management Response: We concur with this finding.

-A new Computer Security Awareness training module was implemented this year that trains users on how to create appropriate complex passwords.

2

This training was developed by OCIO and is currently rolled out to all computer users. (Completed)

Finding #2: ***Configuration Management***

Recommendations
To strengthen configuration management, we recommend that SE:

4. In coordination with the Smithsonian CIO, identify and disable all insecure protocols on the network to protect against network-based attacks.

SE Management Response: We concur with this finding.

- **SE will remove NETBIOS, TELNET, LLMNR and IPv6 from the SE Retail domain. In the case this has unforeseen negative effects, we will remediate as required. (Estimated Completion March 31st, 2016)**
- **SE will work with OCIO to develop a plan to remove insecure protocols from the overall network. Protocols to be addressed will be NETBIOS, TELNET, LLMNR and IPv6. (Estimated Completion August 2016)**

5. Consider disabling the keyboard magnetic reader when the point of sale application is not waiting to process a card number.

SE Management Response: We concur with this finding.

- **SE has implemented new pinpads in all of the Theater locations which allowed us to disable the Cherry key board magnetic readers. This is complete in all retail locations. (Completed)**

Finding #3: ***Protection of Information at Rest***

Recommendations
To strengthen protection measures, we recommend that SE:

6. Encrypt all mobile media, including laptops and backup tapes, to protect against unauthorized information disclosure in the event of loss or theft.

SE Management Response: We concur with this finding.

- **SE Backup tapes are now encrypted. (Completed)**
- **Laptops are being encrypted as we replace older laptops with new models. We have identified employees whose job descriptions handle sensitive data on a regular basis and expedited the process to replace their laptops with new encrypted laptops (HR, payroll, finance and accounting). (Currently 41**

3

of 105 laptops are encrypted. Estimated Completion for all laptops to be encrypted is August 2017)

Finding #4: ***Unsupported System Components***

Recommendations

To protect the unsupported system components, we recommend that the Smithsonian CIO:

7. Update all servers and workstations to operating systems that are supported by the vendor. If a system cannot be upgraded, it should be replaced or segmented from the rest of the network and enhanced hardening and monitoring controls should be implemented.

SE Management Response: We concur with this finding.

- **All SE Servers and workstations are updated and current to vendor supported operating systems. (Completed)**

4

Smithsonian Institution

Office of the Chief Information Officer

Date: February 29, 2016

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
Juliette Sheppard, Director of IT Security
Carmen Iannacone, Chief Technology Officer
Grace Clark, SE Chief Information Officer
Cindy Zarate, Office of the Chief Financial Officer
Stone Kelly, Office of Planning, Management and Budget

Subject: OCIO Response to Smithsonian Enterprises Audit of the Effectiveness of the Information Security Program

Thank you for the opportunity to comment on the Smithsonian Enterprises Audit of the Effectiveness of the Information Security Program. This memorandum documents the OCIO response to the three recommendations made to the Smithsonian Chief Information Officer. Smithsonian Enterprises is responding separately to the other recommendations in the report.

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

OIG Recommendation: To strengthen identity and access management, we recommend that the Smithsonian CIO: Require all SI and SE accounts to use unique, complex passwords consisting of at least eight characters, containing numbers, letters, and special characters. Whenever a new password is created, whether for a new user or password change request, it should follow the same password parameters.

The following Active Directory account password complexity rules are enforced by group policy:

- Enforce password history: 24 passwords remembered
- Maximum password age: 90 days
- Minimum password length: 8 characters
- Password must meet complexity requirements: Enabled
- Store passwords using reversible encryption: Disabled

Password complexity requirements

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least six characters in length
- Contain characters from three of the following four categories:
- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, $, #, %)

The requirements are enforced whenever passwords are created or changed (including temporary passwords).

Additionally, in October 2014 OCIO added password generation procedures documented in technical note IT-960-TN12, *Active Directory Account and Password Requests*, for creating temporary passwords for new accounts or password resets that ensures unique passwords. A random password is either created by the technician or generated by clicking the password generator button next to the password field in the ActiveRoles Server management software used to create and manage accounts.

OCIO has reminded SE of the policy and provided a link to the technical note IT-960-TN12 on Prism.

Estimated Completion Date: Already completed

OIG Recommendation: To strengthen configuration management, we recommend that SE: In coordination with the Smithsonian CIO, identify and disable all insecure protocols on the network to protect against network-based attacks.

In 2015 OCIO eliminated the Windows Internet Name Service (WINS) and has begun testing the elimination of NetBIOS. Assuming that the testing does not encounter significant issues or dependencies that require re-architecture of the network environment, OCIO plans to complete a phased removal of NetBIOS from the SI network by August 31, 2016.

OCIO has been actively working in 2015 to eliminate the use of Telnet. We expect to complete the elimination of Telnet by August 31, 2016.

There is a government mandate for use of IPv6 by federal organizations, so its use is required. Additionally, we are proactively working towards enterprise IPv6 usage to ensure sufficient address space for our complex architecture. IPv6 is not inherently less secure than IPv4 and does not present significant risk. Vulnerabilities and threats to IPv6 enabled devices are detected and remediated using the same SI risk management processes as IPv4 devices.

Estimated Completion Date: August 31, 2016

Recommendation: To protect the unsupported system components, we recommend that the Smithsonian CIO: Update all servers and workstations to operating systems that are supported by the vendor. If a system cannot be upgraded, it should be replaced or segmented from the rest of the network and enhanced hardening and monitoring controls should be implemented.

The elimination of obsolete operating systems has been a significant focus over the past year.

Significant effort was required to upgrade or retire Windows 2003 servers prior to the end of support in July 2015. Most of this activity occurred after the February 2015 – March 2015 time period when the fieldwork for the audit was conducted. Most Windows 2003 machines were replaced or decommissioned. However, where justified, temporary waivers (with a migration plan) have been documented. The few Windows 2000 machines detected by the audit were also included in this effort.

A similar effort for Windows XP was performed in 2014. Where justified, temporary waivers (including mitigations where appropriate) were documented. Where possible, XP systems that have waivers are blocked from the internet (or the network in general) if such connectivity is not needed for the purpose for which XP needs to be retained. All other XP machines were blocked (by MAC address) from the network. Since then, OCIO has been periodically checking for the presence of non-waivered XP machines on the network using both the Nexpose vulnerability scanner and the McAfee ePO tools, and adding any newly detected XP devices to the blocking list.

Estimated Completion Date: Already completed