



Smithsonian
Institution

**Information Security:
Opportunities to Reduce the Risk
of Unauthorized Access to the
Smithsonian Institution's Publicly
Accessible Websites**

**Office of the Inspector General
OIG-A-17-05
September 27, 2017**



In Brief

Information Security: Opportunities to Reduce the Risk of Unauthorized Access to the Smithsonian Institution's Publicly Accessible Websites

OIG-A-17-05, September 27, 2017

What **OIG** Did

The objective of this audit was to assess to what extent the Smithsonian had processes in place to prevent, detect, and resolve security vulnerabilities on the Smithsonian's publicly accessible websites. The audit focused on obtaining an inventory of publicly accessible websites; conducting vulnerability testing, which included an in-depth test of websites to simulate a focused attack by a skilled adversary; and reviewing the Smithsonian's policies, procedures, and processes to manage website security.

Background

The Smithsonian's websites help the Smithsonian in achieving its goal of providing broader access to exhibitions, research, programs, collections, and digital assets. The Smithsonian's web presence also allows the public to make purchases from its online stores, sign up to be a volunteer, or apply for an internship. In fiscal year 2016, more than 134 million people visited the Smithsonian's public websites.

What **OIG** Found

Publicly accessible websites pose significant risk to the Smithsonian Institution (Smithsonian) because anyone with an Internet connection could target a website to gain access to its stored data or gain entry into its network. In fact, two of the Smithsonian's information systems were compromised in 2016 due to website vulnerabilities. In one case, the compromise led to the disclosure of personal data for more than 1,000 researchers.

The Office of the Inspector General (OIG) determined that the Smithsonian had elements of the key processes in place to prevent, detect, and resolve website vulnerabilities. However, the Smithsonian needs to consistently apply those processes to resolve vulnerabilities, maintain its website inventory, and monitor websites for new threats. Specifically, Smithsonian websites were at increased risk of unauthorized access due to unresolved security vulnerabilities. In November 2016, OIG found that information technology security staff had identified 10,855 high, medium, and low vulnerabilities in websites and supporting information systems that system administrators had not resolved within the required time frames.

In addition, the inventory of publicly accessible websites was incomplete. For example, the OIG identified 36 websites that did not appear in the Office of the Chief Information Officer's website inventory and were not being scanned for security vulnerabilities. Finally, website owners did not always monitor security logs for indicators of attack. The OIG found that responsible staff for 6 of 10 websites reviewed could not provide evidence that they reviewed website security logs for indicators of attack during the 2 months selected for testing. Until these issues are resolved, the Smithsonian's publicly accessible websites are at heightened risk of unauthorized access.

What **OIG** Recommended

The OIG made four recommendations to enhance website security. Management agreed with all four recommendations.

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
Office of the Inspector General

Memo

Date: September 27, 2017

To: Deron Burba, Chief Information Officer

Cc: Albert Horvath, Under Secretary for Finance and Administration/Chief
Financial Officer (OUSF&A)
Greg Bettwy, Chief of Staff, Office of the Secretary
Porter N. Wilkinson, Chief of Staff to the Board of Regents
Judith Leonard, General Counsel
Cindy Zarate, Executive Officer, OUSF&A
Carmen Iannacone, Chief Technology Officer
Juliette Sheppard, Director of IT Security
Danee Gaines-Adams, Privacy Officer

From: Cathy L. Helm, Inspector General 

Subject: *Information Security: Opportunities to Reduce the Risk of Unauthorized Access to the Smithsonian Institution's Publicly Accessible Websites (OIG-A-17-05)*

This memorandum transmits our final audit report on the Smithsonian's website application security. The objective of this audit was to assess to what extent the Smithsonian had processes in place to prevent, detect, and resolve security vulnerabilities on the Smithsonian's publicly accessible websites. The audit focused on obtaining an inventory of publicly accessible websites; conducting vulnerability testing, which included an in-depth test of websites to simulate a focused attack by a skilled adversary; and reviewing the Smithsonian's policies, procedures, and processes to manage website security.

We made four recommendations for Smithsonian management to enhance website security. Management agreed with all four recommendations.

We appreciate the courtesy and cooperation of all Smithsonian management and staff during this audit. If you have any questions, please call me or Joan Mockeridge, Assistant Inspector General for Audits, at (202) 633-7050.

TABLE OF CONTENTS

INTRODUCTION..... 3

BACKGROUND 4

RESULTS OF THE AUDIT 6

 Websites are at Increased Risk of Unauthorized Access Due to Unresolved Security Vulnerabilities..... 6

 The Inventory of Publicly Accessible Websites is Incomplete 12

 Website Owners Did Not Always Monitor Security Logs for Indicators of Attack 12

CONCLUSION 13

RECOMMENDATIONS 13

MANAGEMENT RESPONSE AND OIG EVALUATION 14

APPENDIX I: OBJECTIVE, SCOPE, AND METHODOLOGY 15

APPENDIX II: MANAGEMENT RESPONSE..... 19

FIGURES

Figure 1: Illustration of Website Security Vulnerabilities..... 5

Figure 2: Number of Security Vulnerabilities in Information Systems Supporting the Smithsonian Institution’s Publicly Accessible Websites That Were Not Resolved within Required Time Frames, as of November 21, 2016 8

Figure 3: Compliance Pass Rates for the Seven Selected Smithsonian Institution-Owned Servers in October 2016 10

ABBREVIATIONS

CIGIE	Council of the Inspectors General on Integrity and Efficiency
IT	Information Technology
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
Smithsonian	Smithsonian Institution

INTRODUCTION

Publicly accessible websites pose significant risk to an organization because anyone with an Internet connection could target a website to gain access to its stored data or gain entry into the organization's network. In a 2016 report, one research firm determined that the frequency of website attacks was rising and that websites accounted for about 40 percent of all confirmed data breaches in their study.¹

The Smithsonian Institution (Smithsonian) develops and maintains more than 500 publicly accessible websites to share information with the public, collaborate and conduct business with entities outside of the Smithsonian, and provide remote access to the Smithsonian's networks. Websites like *si.edu* provide access around the world to museum collections, research, and education resources. More complex websites, like *SmithsonianStore.com*, allow for interactive experiences, online shopping, volunteer sign-up, and donations.

More complex websites may allow the user to submit or retrieve information. Such user-submitted information can sometimes be personal, like credit card numbers, passwords, or job applications. Collecting and storing that information necessitates a program to protect it from unauthorized access. The Smithsonian has established an information security program to support and manage the security of its websites. The program includes processes like monitoring for security vulnerabilities, configuring information systems to prevent common attacks, and making sure new websites are secure.

The objective of this audit was to assess to what extent the Smithsonian had processes in place to prevent, detect, and resolve security vulnerabilities on the Smithsonian's publicly accessible websites. The audit consisted of four phases: (1) obtaining a complete inventory of the Smithsonian's publicly accessible websites; (2) conducting a vulnerability scan of the websites identified in phase one, including their supporting systems; (3) doing an in-depth test of websites to simulate a focused attack by a skilled adversary; and (4) reviewing the security program's policies, procedures, and processes used to manage website security. See appendix I for more information about the Smithsonian Office of the Inspector General's (OIG) objective, scope, and methodology.

The Smithsonian OIG contracted with an information technology (IT) security company to perform phases one through three, and OIG staff performed phase four. The audit included a review of publicly accessible websites for the period May 2016 through September 2017. This audit also supported a broader, government-wide assessment, coordinated by the Council of the Inspectors General on Integrity and Efficiency (CIGIE).

¹ Verizon, *2016 Data Breach Investigations Report* (Verizon, Basking Ridge, NJ: April 2016).

OIG conducted this performance audit in accordance with generally accepted government auditing standards. Those standards required that OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on the audit objective. OIG believes that the evidence obtained provides a reasonable basis for the findings and conclusions based on its audit objective.

BACKGROUND

The Smithsonian includes 19 museums, the National Zoological Park, nine research centers, and numerous research programs. Research is carried out in the museums and other facilities throughout the world. In fiscal year 2016, the public made more than 29 million visits to the Smithsonian museums and zoo, and more than 134 million people visited the Smithsonian's public websites.² In addition to federal appropriations, the Smithsonian receives private support, external grants and contracts, income from investments, and income from various business activities. Business activities include Smithsonian magazines and other publications; online catalogs; and theaters, retail shops, and food services.

The Smithsonian's websites serve a national and international audience. The reach of the Internet helps the Smithsonian in achieving its goal of providing broader access to exhibitions, research, programs, collections, and digital assets. The Smithsonian's web presence also provides services like allowing the public to make purchases (*SmithsonianStore.com*), sign up to be a volunteer (*evansvol.si.edu*), or apply for an internship (*solaa.si.edu*).

To manage Smithsonian websites, the Office of the Chief Information Officer (OCIO) establishes technical standards, designates preferred website design and content management products, operates the web infrastructure, registers domain names, and ensures that security controls are in place. Units throughout the Smithsonian, such as museums and research centers, generally develop and publish websites using the centralized infrastructure maintained by OCIO. In some cases, units manage their own web infrastructure, such as the Smithsonian Astrophysical Observatory and the Smithsonian Tropical Research Institute, or use contractors for website development and website hosting.

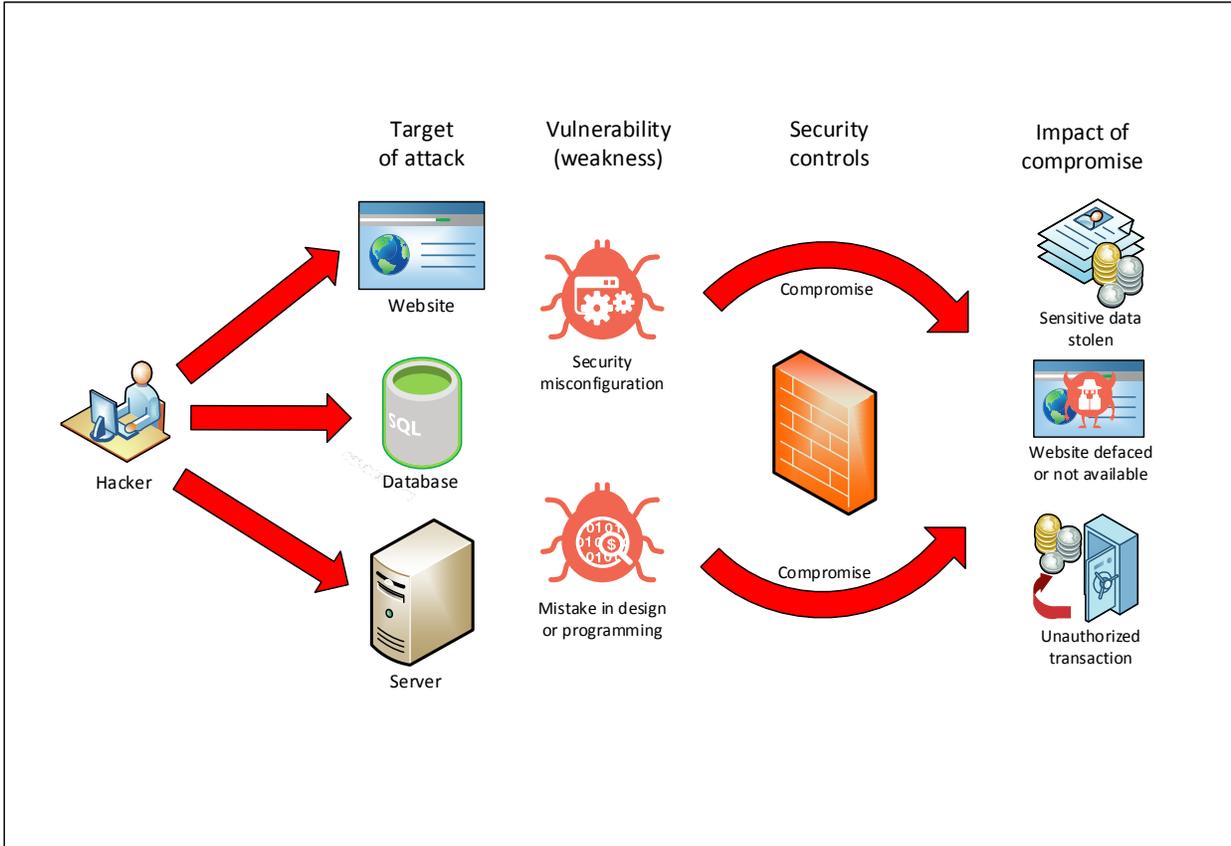
Website Security Vulnerabilities

A website security vulnerability is a weakness, such as a design mistake, programming mistake, or security misconfiguration that provides an attacker with a means to compromise the website. Such vulnerabilities can be present in the website itself or the

² Smithsonian Institution, *Smithsonian Dashboard*, accessed May 4, 2017.

underlying systems that support the website, like database and application servers. A compromise means unauthorized access to data (confidentiality), unauthorized or altered transactions (integrity), or unplanned system downtime (availability). See figure 1 for an illustration of website security vulnerabilities.³

Figure 1: Illustration of Website Security Vulnerabilities



Source: OIG analysis of the OWASP's Top 10 – 2013 report.

For example, a common vulnerability is that a website accepts information from the user without verifying that the information is safe to process. Such a vulnerability could allow an attacker to trick the website into processing unsafe code that instructs the website to perform unauthorized actions like displaying other users' data.

³ Open Web Application Security Project, *OWASP Top 10 – 2013: The Ten Most Critical Web Application Security Risks*, Version 2013 (OWASP Foundation: June 12, 2013).

RESULTS OF THE AUDIT

During this audit, OIG determined that the Smithsonian had elements of the key processes in place to prevent, detect, and resolve website vulnerabilities. For example, the Smithsonian had established website security policies, security training requirements for staff, and contract provisions for website security when maintained by an outside contractor. In addition, OCIO had an effective process to verify that new websites were free of high-risk vulnerabilities when the websites were brought online and to prevent some common website security attacks. However, OIG identified opportunities to further reduce the risk of unauthorized access by focusing on more timely resolution of known vulnerabilities, maintaining a complete inventory of websites, and monitoring websites for indicators of attack.

Websites Are at Increased Risk of Unauthorized Access Due to Unresolved Security Vulnerabilities

Smithsonian policy calls for prompt mitigation of vulnerabilities in publicly accessible websites to maintain the confidentiality, integrity, and availability of the Smithsonian's information systems and data. However, OIG's analysis showed that in November 2016, the Smithsonian's publicly accessible websites and supporting information systems were at greater risk of compromise due to a high number of security vulnerabilities that were not resolved within required time frames. For example, 7,550 high and medium severity vulnerabilities had been identified for more than 90 days without resolution. Under Smithsonian policy, these should have been resolved within 30 days. In addition, OCIO has not yet fully implemented a process to keep systems in compliance with its security configuration standards, leading to unknown security vulnerabilities. In late 2016, the Smithsonian saw the effect of not resolving vulnerabilities when hackers successfully compromised two publicly accessible websites, one of which led to hackers accessing the personal data of more than 1,000 researchers, including names, addresses, and phone numbers.

Unresolved Security Vulnerabilities Increase the Risk of Unauthorized Access to the Smithsonian's Publicly Accessible Websites

Smithsonian policy requires that IT security staff identify vulnerabilities and provide reports of those vulnerabilities to system administrators who manage the computer system, including the operating system and application.⁴ The same policy requires that system administrators take action to resolve vulnerabilities within defined time frames

⁴ Smithsonian Institution, *Vulnerability Management Program*, Technical Note IT-930-TN33 (Washington, D.C.: July 6, 2015).

based on the severity of the vulnerability. The policy requires resolution of critical severity vulnerabilities in 3 days, high severity vulnerabilities in 2 weeks, medium severity vulnerabilities in 1 month, and low severity vulnerabilities in 3 months.⁵

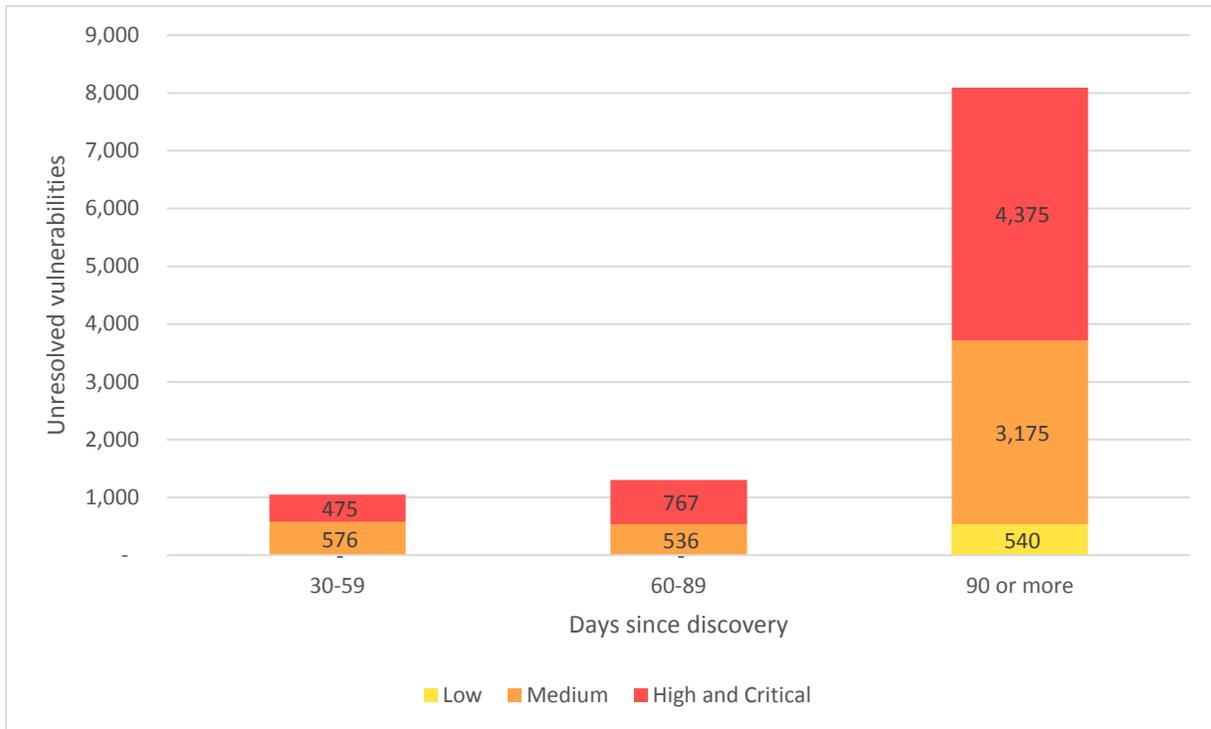
In November 2016, OIG found that IT security staff had identified 10,855 high, medium, and low severity vulnerabilities in websites and supporting information systems that system administrators had not resolved in accordance with the required time frames. For websites, OIG analysis showed that 68 percent (411 of 607) of high severity vulnerabilities were not resolved within 2 weeks, as required. For information systems that support websites, such as web servers and database servers, OIG analysis showed that 9,904 high and medium severity vulnerabilities were not resolved within 30 days, and an additional 540 low severity vulnerabilities were not resolved within 90 days as required.⁶ Moreover, 7,550 (76 percent) of those high and medium severity vulnerabilities were more than 90 days old. When vulnerabilities are not resolved within required time frames, IT security staff must deal with a growing workload of the known unresolved vulnerabilities and the new vulnerabilities identified through periodic scanning, resulting in a backlog and increasing the risk of compromising the known vulnerability.

See figure 2 for a detailed breakdown of the backlog of vulnerabilities not addressed within required time frames, as of November 21, 2016. The report used by OIG for this analysis did not provide enough detailed information to separate critical vulnerabilities from high vulnerabilities. In addition, not enough detailed information was available to identify critical vulnerabilities between 4 and 30 days old and high severity vulnerabilities between 14 and 30 days old.

⁵ The severity of a vulnerability is determined by the software tools that OCIO uses to periodically scan websites and supporting systems

⁶ The report used by OIG for this analysis did not provide sufficient information to identify high severity vulnerabilities between 14 and 30 days old.

Figure 2: Number of Security Vulnerabilities in Information Systems Supporting the Smithsonian Institution’s Publicly Accessible Websites That Were Not Resolved within Required Time Frames, as of November 21, 2016



Source: OIG analysis of the Smithsonian Institution’s security vulnerability data, as of November 2016.

Note: The report used by OIG for this analysis did not provide enough detailed information to separate critical vulnerabilities from high vulnerabilities. In addition, not enough detailed information was available to identify critical vulnerabilities between 4 and 30 days old and high severity vulnerabilities between 14 and 30 days old.

Likewise, penetration testing⁷ efforts conducted by OIG’s IT security contractor identified high severity vulnerabilities, one of which allowed the OIG contractor to breach a website from the Internet and gain access to personal data. The OIG contractor scanned 242 websites in September 2016 and identified 92 high severity website vulnerabilities. The OIG contractor then used discovered vulnerabilities, along with manual testing techniques, to replicate a focused attack by an external hacker. Through this focused security testing, the OIG contractor gained access to personal data (names, addresses, and contact information) in one of those websites by using a previously undetected high severity vulnerability. The OIG contractor also identified medium vulnerabilities in two other websites, but the vulnerabilities did not allow the OIG contractor to access data on these two websites.

According to the Director of IT Security, OCIO and other units’ technical support staff are working to resolve the backlog of vulnerabilities as resources allow, but there is not

⁷ According to the National Institute of Standards and Technology, penetration testing is a methodology whereby testers attempt to circumvent or defeat security controls.

a formal plan with an established timetable for when the backlog will be remedied. The Director of IT Security stated that there are a variety of hurdles to reducing the backlog, including limited staffing, insufficient funding to replace obsolete products, and coordination issues among support teams in OCIO and other Smithsonian units.

In late 2016, two publicly accessible websites were compromised through vulnerabilities. One resulted in the theft of more than 1,000 researchers' personal data, including names, addresses, and phone numbers. However, the majority of stolen data did not include sensitive personal information such as credit card or Social Security numbers. Nevertheless, the breach still necessitated that the Smithsonian notify the affected individuals. In addition, a second compromised website allowed hackers to add hidden web pages that advertised counterfeit products on a popular Internet search engine. By using the Smithsonian's name, the advertisements reached a broader audience and made the products appear to be endorsed by the Smithsonian.

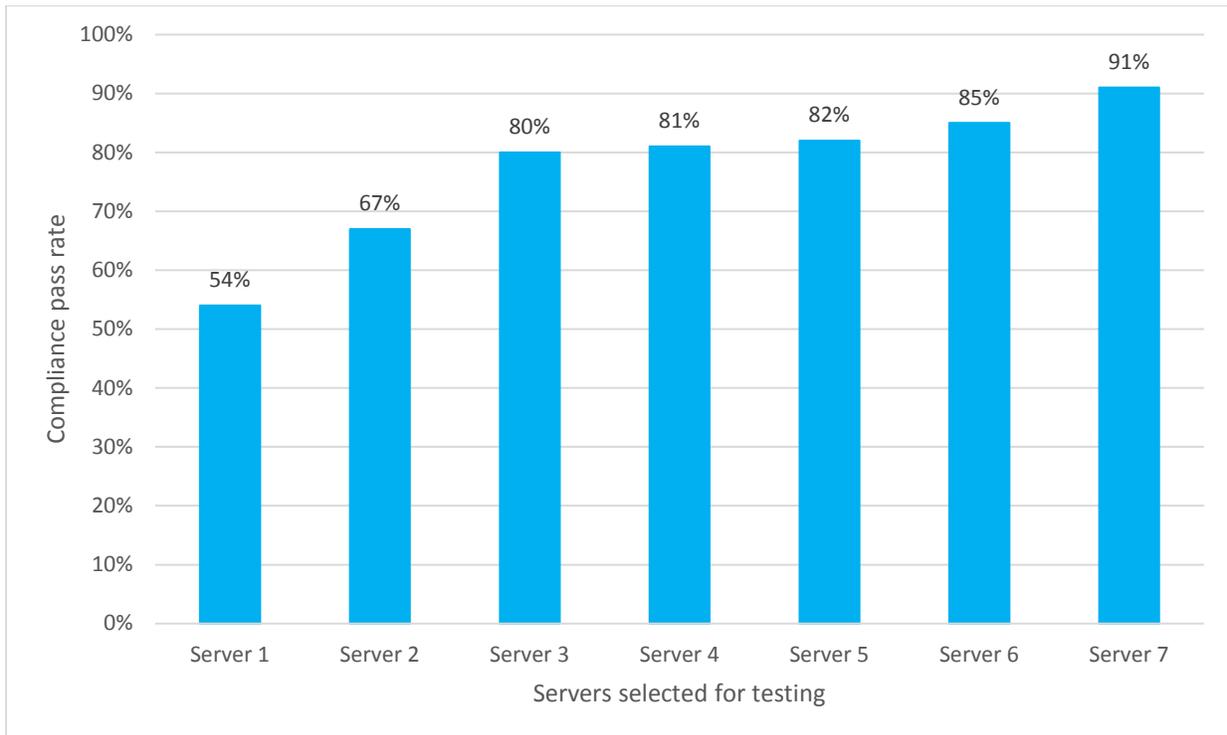
Unsecure System Settings Contribute to Website Security Vulnerabilities

Smithsonian technical standards and guidelines require that information system owners, such as OCIO and units, maintain a secure configuration on their systems by complying with a baseline security configuration standard and periodically verifying that the system continues to comply with the baseline standard, which is referred to as "configuration management."⁸ The baseline standard includes settings such as configuring the system to track failed login attempts and enforcing minimum password complexity standards. Securing the system's configuration helps to prevent security vulnerabilities and reduce the impact of a compromise.

To test compliance with baseline standards for publicly accessible websites in October 2016, OIG obtained and evaluated security baseline compliance reports for seven Smithsonian-owned servers that supported publicly accessible websites. These seven servers were selected because the websites they supported (1) required users to log in with a username and password and (2) potentially contained personal information of the users. The compliance reports list security settings with a pass/fail indicator, which identifies whether the server's security settings either meet (pass) or do not meet (fail) the approved baseline standard. OIG determined that none of the seven servers was in full compliance with the baseline standards. As shown in figure 3, pass rates for the individual servers ranged from a low of 54 percent to a high of 91 percent. Not complying with the baseline security standards introduces security vulnerabilities that may be used by hackers to gain unauthorized access to data, create unauthorized transactions, or cause unplanned system downtime.

⁸ Smithsonian Institution, *Security Controls Manual*, Technical Standards & Guidelines, IT-930-02 (Washington, D.C.: January, 2014).

Figure 3: Compliance Pass Rates for the Seven Selected Smithsonian Institution-Owned Servers in October 2016



Source: OIG analysis of the servers' October 2016 compliance reports.

At the time of this review, OIG had an open audit recommendation related to conducting compliance assessments against baseline security configuration standards.⁹ OCIO was working to address that recommendation by selecting and implementing a tool to scan for compliance against the baseline standards. OIG closed this recommendation in January 2017 when OCIO began using its selected tool to perform scans to better ensure compliance with baseline standards.

Minimum Password Complexity Standards for User Accounts Were Not Consistently Enforced

Smithsonian technical standards and guidelines require that information systems, such as publicly accessible websites, enforce minimum password complexity standards and protect passwords from unauthorized disclosure when stored. Specifically, the standard requires a minimum length of eight characters with at least one number, one special character, and a combination of upper and lower case letters.¹⁰

⁹ Smithsonian Office of the Inspector General, *Fiscal year 2014 Independent Evaluation of the Smithsonian Institution's Information Security Program*, OIG-A-16-02 (Washington, D.C.: Dec. 17, 2015).

¹⁰ IT-930-02.

Complex passwords are important because complexity increases the difficulty for an unauthorized user to discover a password through guessing. Each additional complexity factor, such as adding numbers or special characters, adds more possible combinations. For example, a password with a one-character length that only includes lower-case letters takes a maximum of 26 guesses (a through z), whereas a password with a two-character length takes 676 guesses (26 multiplied by 26). If the website stores the password in plain text, then the number of guesses is zero because a human can read it.

To determine if password complexity requirements were properly enforced, OIG reviewed 10 of 46 publicly accessible websites. The 10 websites were selected because they (1) required users to log in with a username and password and (2) potentially contained personal information of the users. OIG found that four websites properly enforced password complexity requirements and that six websites did not. For the six websites that did not properly enforce password complexity requirements, issues included not enforcing any password complexity requirements, not enforcing the correct minimum length (seven instead of eight characters), and not requiring all of the character types (e.g., upper case, lower case, number, special characters).

In addition, 2 of the 10 selected websites did not protect the stored passwords from unauthorized disclosure. This is typically done by making the passwords unreadable through encryption. However, OIG found that these two websites stored passwords in plain text, meaning that anyone with access to the storage files could read the password.

In the fiscal year 2014 information security program audit, OIG reported that OCIO needed to improve its security assessment and authorization process, which ensures compliance with IT security policies, such as password complexity, before an information system is authorized for use.^{11,12} As identified in that report, the Security Testing and Evaluation reports, which summarize the results of security controls testing, were inaccurate and incomplete. At the time this report was issued, OCIO was still working to address OIG's recommendation to strengthen the assessment and authorization process. OCIO's resolution of that issue is targeted for September 30, 2017.

¹¹ OIG-A-16-02.

¹² Assessment and authorization is an IT security process that assesses the security controls of an information system and, if the controls sufficiently reduce risk, authorizes that system for use by the organization.

The Inventory of Publicly Accessible Websites Is Incomplete

OCIO guidance requires that all information systems, including websites, be included in the IT security system inventory.¹³ An accurate inventory is critical for the information security program, in part because it provides a basis for OCIO to assess information security risk and to configure tools for ongoing security monitoring. For example, if a website or information system is not in the inventory, it may be excluded from security vulnerability scanning.

During this audit, OIG independently developed an inventory of Smithsonian-owned websites through a review of public website registration data and automated scanning of Smithsonian-owned Internet addresses. OIG compared that inventory against OCIO's website inventory and noted that, of the 523 websites identified by OIG,¹⁴ 101 (19 percent) did not appear in the OCIO inventory. In conducting follow-up, OIG determined that 65 of the 101 websites were included in vulnerability scanning tools, even though the websites were not in the inventory. However, 36 websites were not in the tools and so were not scanned for security vulnerabilities, increasing the risk of vulnerabilities in the websites that were not included in the inventory or vulnerability scanning tools remaining unidentified and unresolved.

Website Owners Did Not Always Monitor Security Logs for Indicators of Attack

A critical part of an information security program is identifying unauthorized activities, particularly for publicly accessible systems that can be targeted by individuals outside the organization. An effective log review helps to promptly detect and respond to unauthorized activities by quickly identifying a potential threat and forwarding it to IT security staff for follow-up. Smithsonian guidance requires that staff with system administration roles and responsibilities review security logs to detect unauthorized activities or anomalies and to report the results of reviews to OCIO monthly.¹⁵ Two examples of activity the reviewer may look for are (1) hundreds of failed logins followed by a successful login, which may indicate password guessing; or (2) the addition of new data fields to a database when none were planned, possibly indicating unauthorized access.

¹³ Smithsonian Institution, *IT Security System Inventory*, Technical Note IT-930-TN34 (Washington, D.C.: Aug. 18, 2015).

¹⁴ This number includes Internet addresses that redirect the user to a different website listed on the OIG-developed inventory and websites that were not being used for displaying content, also known as placeholders.

¹⁵ Smithsonian Institution, *Auditing & Accountability*, Technical Note IT-930-TN02 (Washington, D.C.: Oct. 17, 2006).

For 4 of 10 websites reviewed, OIG found that responsible staff reviewed log files as required. However, for the remaining six websites reviewed, responsible staff could not provide evidence that they had performed security log reviews during May and August 2016. Staff for five of those six websites indicated that they do not perform security log reviews. A staff member for the sixth site indicated that he performed reviews but did not document the results and thus could not provide evidence.

In the fiscal years 2014 and 2015 information security program audits, OIG reported security weaknesses related to security log collection and analysis.^{16,17} Since those reports were issued, OCIO has defined a log collection and analysis strategy to collect more security logs and automate the alerting of suspicious actions. While that strategy added the necessary tools for automating log collection and analysis, it did not specifically identify website security logs for collection, analysis, and automated alerting of suspicious activities. At the time of this review, OCIO had not fully implemented the strategy, which had a target completion date of July 2018.

CONCLUSION

Publicly accessible websites pose significant risk to the Smithsonian because anyone with an Internet connection could target a website to gain access to its stored data or gain entry into its network. In fact, two Smithsonian information systems were compromised in 2016 due to website vulnerabilities. In one case, the compromise led to the disclosure of personal data for more than 1,000 researchers. While the Smithsonian has elements of the key processes in place to reduce the risk of website vulnerabilities, it needs consistently applied processes to resolve vulnerabilities, maintain an accurate and complete website inventory, keep passwords safe, and monitor websites for new threats. In the meantime, the Smithsonian's publicly accessible websites are at heightened risk of unauthorized access.

RECOMMENDATIONS

To further strengthen the security of the Smithsonian's publicly accessible websites, OIG recommends that the Chief Information Officer do the following:

1. Determine the root cause of the untimely resolution of vulnerabilities that has created a backlog and then develop and implement a plan to (1) resolve the root cause so that vulnerabilities are resolved timely going forward, and (2) remediate the

¹⁶ OIG-A-16-02.

¹⁷ Smithsonian Office of the Inspector General, *Fiscal Year 2015 Independent Evaluation of the Smithsonian Institution's Information Security Program*, OIG-A-16-11 (Washington, D.C.: Sept. 30, 2016).

existing backlog with a focus on expeditious milestones for resolving critical and high vulnerabilities.

2. Establish and implement procedures to inventory websites, maintain the inventory going forward, and periodically ensure that all websites are included in the vulnerability scanning tools.
3. As part of the assessment and authorization process, ensure that individual website owners configure their systems to meet Smithsonian password complexity standards or, where not possible, work with the website owners to determine other ways to reduce the risk of weak passwords and password storage.
4. Develop and implement a plan to include website security logs in the automated log monitoring tool and configure the tool to automatically alert security staff when suspicious website activity occurs.

MANAGEMENT RESPONSE AND OIG EVALUATION

OIG provided a draft of this report to Smithsonian management for review and comment. Smithsonian management provided written comments, which are found in appendix II. Smithsonian management concurred with all four recommendations that OIG made in its draft report. OIG evaluated management's response and determined that their planned actions address the intent of the four recommendations.

Appendix I

OBJECTIVE, SCOPE, AND METHODOLOGY

The Smithsonian Institution's (Smithsonian) Office of the Inspector General (OIG) conducted this performance audit to assess to what extent the Smithsonian had processes in place to prevent, detect, and resolve security vulnerabilities on the Smithsonian's publicly accessible websites. The scope of the audit included publicly accessible websites and information systems that supported publicly accessible websites, such as database and application servers.

OIG's methodology included four phases: (1) obtaining a complete inventory of the Smithsonian's publicly accessible websites; (2) conducting a vulnerability scan of the websites identified in phase one, including their supporting systems; (3) doing an in-depth test of websites to simulate a focused attack by a skilled adversary; and (4) reviewing the security program's policies, procedures, and processes used to manage website security. The Smithsonian's OIG contracted with an information technology (IT) security company to perform phases one through three, and OIG staff performed phase four.

Phase One – Inventory of Publicly Accessible Websites

To establish a complete inventory of the Smithsonian's publicly accessible websites, the Office of the Chief Information Officer (OCIO) provided the contractor with nine known network address ranges and 47 known websites. The contractor performed open source research against that list to identify additional network ranges and domain names that the contractor could directly attribute to the Smithsonian.

Research included techniques like querying public services, such as the Internet Corporation for Assigned Names and Numbers. Once the contractor had a comprehensive list of websites and network ranges, they performed automated network scanning against the full list to identify individual systems and services that responded to their scanning. The contractor created an inventory of all responding systems hosting websites.

Phase Two – Website and Network Vulnerability Scanning

This phase consisted of two distinct automated scanning activities across the inventory identified in phase one: (1) network scanning to identify vulnerabilities in the underlying IT infrastructure that supports the website and (2) website scanning to identify vulnerabilities within the website itself. The contractor conducted network scanning using the Smithsonian's vulnerability scanner, which allowed them to get authenticated scan results. "Authenticated results" means that the scanner has a login and password to more thoroughly scan a system.

The contractor performed website vulnerability scanning from outside the Smithsonian network using a combination of scanning tools. The contractor focused these tools on identifying common website weaknesses and misconfigurations with an emphasis on the Open Web Application Security Project's Top Ten application vulnerabilities,¹⁸ which were

1. injection,
2. broken authentication and session management,
3. cross-site scripting,
4. insecure direct object references,
5. security misconfiguration,
6. sensitive data exposure,
7. missing function-level access control,
8. cross-site request forgery,
9. using known vulnerable components, and
10. unvalidated redirects and forwards.

The scope for phase two included network systems owned or hosted by the Smithsonian and systems hosted by third parties where OIG had permission to scan their network.

In total, the contractor included 34 internal systems in network vulnerability scanning and 242 websites in website vulnerability scanning. The 34 internal systems hosted approximately 180 websites.

Phase Three – In-Depth Manual Website Review

Using the inventory from phase one and the results of scanning in phase two, OIG, in consultation with the contractor and OCIO, selected three websites for an in-depth manual assessment. OIG selected websites based on complexity, such as user interactivity or data entry, and the use of sensitive personal information, such as Social Security or credit card numbers. As this was a judgmental, not a statistical, sample, the results cannot be projected over the population of all websites.

The contractor designed testing in this phase to emulate a real-world attacker, which allowed them to demonstrate the true risk posed to the Smithsonian's publicly accessible websites and servers. The contractor's manual website penetration testing techniques followed industry-tested practices and expanded upon automated scanning. Testing attempted to identify common classes of website security vulnerabilities such as those in the Open Web Application Security Project's Top Ten. The contractor attempted to exploit any such vulnerabilities as a demonstration and validation of the severity posed by discovered vulnerabilities.

¹⁸ Open Web Application Security Project, *OWASP Top 10 – 2013: The Ten Most Critical Web Application Security Risks*, Version 2013 (OWASP Foundation: June 12, 2013).

Phase Four – Program Review

To review the information security program for website security, OIG considered the relevant risks faced by 523 publicly accessible websites and identified the controls that Smithsonian management had put in place to mitigate those risks. This included the following five process areas that support website security:

- **Security configuration management** – OIG obtained configuration files for the 10 selected websites to verify that the website stored passwords securely, required sufficient complexity, and logged required security events. This process also included OIG’s review of the security staff’s periodic security configuration review and OIG’s verification that the Smithsonian’s load balancer¹⁹ was properly configured for security monitoring and updates.
- **Vulnerability management** – OIG obtained and reviewed screenshots and reports to verify that OCIO security staff had properly configured vulnerability scanning tools to include all websites and to accurately identify security vulnerabilities. OIG also obtained vulnerability aging reports to verify that security administrators had resolved vulnerabilities within policy defined time frames. The aging report calculated how many days had elapsed between the discovery of the vulnerability on a system and the date the report was generated. OIG further obtained and reviewed supporting evidence to verify that OCIO had conducted periodic vulnerability scanning on Payment Card Industry Data Security Standard certified systems that accept credit cards.
- **System development** – OIG obtained and reviewed policies and procedures to verify that OCIO had established secure software coding standards and training requirements for internal development of websites. OIG also reviewed 25 new websites that went through the Technology Review Board²⁰ during the period January through November 2016. For these websites, OIG reviewed materials presented to the Technology Review Board to verify that security staff had scanned for and resolved high severity security vulnerabilities prior to publishing the website to the public.
- **Information security management** – OIG obtained and reviewed policies and procedures to verify that the Smithsonian had established a policy framework for managing website security. OIG also obtained and reviewed evidence that security staff had periodically reviewed security logs for unauthorized access or activities. Further, OIG obtained and reviewed configuration screenshots to verify that OCIO had configured the vulnerability scanning tool to identify unknown systems through discovery scanning.

¹⁹ A load balancer is a device that distributes network or application traffic across servers to increase capacity, reliability, and performance.

²⁰ The Technology Review Board evaluates the progress of information technology projects at the Smithsonian with the objective of improving project success, improving system quality, and ensuring that risk is reduced to an acceptable level.

- **Website contracts** – For 3 externally developed or hosted websites from the OIG sample of 10, OIG obtained and reviewed contracts or service agreements to verify that the agreement adequately addressed website security.

The total population of websites identified by OIG for this phase consisted of 46 publicly accessible websites that required users to login for access. OIG selected 10 of those websites for testing, focusing the selection on websites that were complex or likely to include sensitive personal information. As this was a judgmental, not a statistical, sample, the results cannot be projected over the population of all websites. Due to security concerns, OIG will not list the specific websites selected for testing.

OIG conducted this performance audit in Washington, D.C., and Herndon, VA, from May 2016 through September 2017 in accordance with generally accepted government auditing standards. Those standards required that OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on the audit objective. OIG believes that the evidence obtained provides a reasonable basis for the findings and conclusions based on its audit objective.

Appendix II

MANAGEMENT RESPONSE



Smithsonian Institution

Office of the Chief Information Officer

Date: August 25, 2017

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 Benton, Acting 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
Matthew Jenkins, Acting Director, System Architecture & Product Assurance
Cindy Zarate, Office of the Chief Financial Officer
Stone Kelly, Office of Planning, Management and Budget

Subject: OCIO Response to "Opportunities to Reduce Risk of Unauthorized Access to Publicly Accessible Websites"

Thank you for the opportunity to comment on the report "Opportunities to Reduce Risk of Unauthorized Access to Publicly Accessible Websites"

Management concurs with most all of the findings and has already made significant progress on completing the recommended actions. 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, .

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

- 1. Determine the root cause of the untimely resolution of vulnerabilities that has created a backlog and then develop and implement a plan to: (1) resolve the root cause so that vulnerabilities are resolved timely going forward; and (2) remediate the existing backlog with a focus on expeditious milestones for resolving critical and high vulnerabilities.**

OCIO established a web vulnerability working group in spring of 2017 which has worked on prioritizing and resolving website related vulnerabilities. Vulnerability dashboards have been created for both application and host level vulnerabilities related to websites and web applications. These dashboards are used to identify high priority targets and to track progress in remediation. Since this effort was started, web application vulnerabilities have been reduced by 37% (with High (critical) categorization vulnerabilities reduced by 72%) and web host vulnerabilities in the DMZ have been reduced by approximately 60%. The working group will continue its efforts on a routine basis to address existing vulnerabilities and to ensure that new vulnerabilities are addressed in a timely fashion going forward. We expect to complete remediation of all high and medium risk website vulnerabilities that are in violation of the Smithsonian's required remediation timeframes (except where approved risk-based waivers are approved) by April 30, 2018.

- 2. Establish and implement procedures to inventory websites, maintain the inventory of websites going forward, and periodically ensure that all websites are included in the vulnerability scanning tools.**

Based on standard industry definitions, the Smithsonian considers a "website" to be a stand-alone set of html pages, content and links that is published (served) and maintained as an independent unit. As such, it can be accessed via a domain URL and scanned independently by robots or security scanning tools.¹

We define a "Smithsonian-owned website" as a website for which the Smithsonian controls and manages all of the following: the domain/URL; hosting (serving); code updates; content updates; maintenance and patching.

The Smithsonian website inventory that was reviewed by the auditors was based on these definitions and intentionally did not include the following (some of which may show up in other lists):

- Parked Domains (i.e. internet domain names that are registered for the purpose of reserving the name but without that domain being associated with any services such as a website or e-mail, although a non-search-indexed HTML marker page may be served as a placeholder.) Since there is no actual website but only a reserved name, we did not include these in the website inventory.
- URL Forwarding (aka URL Redirect) where a web page is made available under more than one URL address. When a web browser attempts to open a URL that has been redirected, a page with a different URL is opened. In these cases, SI only listed the site once in our inventory rather than duplicating it for each name that redirects to that same site.

¹ Compiled from definitions provided on W3C, Wikipedia and other common sources.

- Domain Forwarding (aka Domain Redirection) when all pages in a URL domain are redirected to a different domain. When a domain is set to forward visitors to another website, the domain's name does not stay in the web browser's URL bar. Instead, the new page's URL is displayed. Multiple URLs and/or domains may forward or redirect to a single URL or website. These were not included in our inventory because a domain redirect does not constitute a website but is a forward to a website.
- Websites that are not owned by the Smithsonian (which may include sites to which the Smithsonian contributes content but which are actually owned, managed, and/or hosted by a consortium, university or other external entity with which the Smithsonian has a relationship).

Also, because the scope of the audit was specified as “public websites”, we interpreted the scope to be websites SI publishes for index by Google, Bing and other search engines for public consumption, and therefore did not include non-search-indexed, non-public URLs (such as SI staff remote access portals) in the inventory. While these applications use web services, they are not considered “public websites”.

Based on a review of the inventory list compiled by the auditors, we believe that most of the entries on the auditor’s inventory that were not on the SI website inventory are ones that fall into these excluded categories that we consider to not be “Smithsonian websites”.

However, to address the audit finding, OCIO has performed a reconciliation of the following inventory lists to ensure that all of the above items are being tracked:

- Web Services Division (WSD) Website Inventory – list of websites that appear on the WSD SharePoint site. This is the inventory list that was reviewed by the audit
- Domain List – list of individual internet domains registered to Smithsonian units
- Web Audit list – The list provided by OIG that was compiled by the auditors as part of this audit.
- Webtrends master list – The list of public websites used to report Webtrends website-visitor data to Smithsonian management and the SI Dashboard
- Smithsonian Enterprises (SE) domain list – The list of domains registered separately by Smithsonian Enterprises

We will provide the results of this reconciliation to OIG at the end of August 2017.

OCIO has also reviewed all the actual websites listed in the WSD inventory and the audit list and added any missing ones to the web vulnerability scans. As part of the Technical Review Board (TRB) review of new websites, a clean vulnerability scan is required, which also facilitates the addition of that new website to the scanning list. However, OCIO will perform

a periodic reconciliation of the scanning list against the inventory list to ensure that no new websites have been missed by the TRB process. The OCIO Web Services Division will maintain this list on an ongoing basis.

3. As part of the assessment and authorization process, ensure that individual website owners configure their systems to meet Smithsonian password complexity standards or, where not possible, work with the website owners to determine other ways to reduce the risk of weak passwords and password storage.

For web servers, the password configurations are configured via server configuration baselines and verified using the configuration baseline scans, so we believe there are no password configuration issues with the web servers.

Website password rules are configured separately from the servers the websites are hosted on, and are configured separately on each website.

Many Smithsonian websites, including new sites using SI's centrally hosted Drupal and WordPress infrastructure, use secure LDAP to authenticate website administrators and other Smithsonian accounts against the Smithsonian Active Directory for administrative and content editing functions. In these cases, the Smithsonian password policies are automatically enforced by Active Directory Group Policy.

For websites that do not utilize Active Directory and for external user accounts that are not stored in Active Directory, we cannot centrally manage or verify password complexity rules within the websites. There is no mechanism to scan for website password configuration parameters using any tools that we have.

The external user accounts on many of the websites do not provide users with access to any sensitive data and do not provide them with the ability to modify website content. In these cases, the risk resulting from less secure passwords is low and may not merit the effort to enforce more stringent requirements.

OCIO will reach out to the owner of each website that is not using secure LDAP for administrative functions to discuss the possibility of transitioning to secure LDAP. For those websites that cannot use LDAP or which have external user accounts with access to sensitive information or content editing functions, OCIO will advise website owners on implementation of appropriate password configurations. OCIO will also work with website owners to document any necessary waivers from SI password policies. These activities will be completed by June 30, 2018.

4. Develop and implement a plan to include website security logs in the automated log monitoring tool and configure the tool to automatically alert security staff when suspicious website activity occurs.

The Smithsonian's central Drupal and WordPress web environment, which hosts almost 100 websites, already sends security logs to Splunk. There is also an existing Splunk dashboard that is used to closely monitor this environment.

Additionally, logs from the enterprise firewalls, F5 web application firewall appliances, and

other devices that monitor traffic to the websites hosted in the Smithsonian DMZ are also already sent to Splunk.

As part of the implementation of the Information Security Continuous Monitoring (ISCM) Strategy, OCIO will work with website owners to configure the forwarding of additional appropriate log information from websites hosted in the Smithsonian DMZ to Splunk, where the data will be incorporated into enterprise security monitoring alerts and dashboards. This will be completed by August 31, 2018.



Smithsonian Institution
Office of the Inspector General

HOTLINE

202-252-0321

oighotline@oig.si.edu

<http://www.si.edu/oig>

or write to

Office of the Inspector General
P.O. Box 37012, MRC 524
Washington, D.C. 20013-7012

The Office of the Inspector General investigates allegations of waste, fraud, abuse, gross mismanagement, employee and contractor misconduct, and criminal and civil violations of law that have an impact on the Smithsonian's programs and operations.

If requested, anonymity is assured to the extent permitted by law. Although you may remain anonymous, we encourage you to provide us with your contact information. The ability to gather additional information from you may be the key to effectively pursuing your allegation.