



OFFICE of INSPECTOR GENERAL
NATIONAL ARCHIVES and RECORDS ADMINISTRATION
8601 ADELPHI ROAD, COLLEGE PARK, MD 20740-6001
www.archives.gov/oig

March 25, 2016

TO: David S. Ferriero
Archivist of the United States

FROM: James Springs *James Springs*
Inspector General

SUBJECT: *Audit of NARA's Publicly-Accessible Websites*

Attached for your action is our final report, *Audit of National Archives and Records Administration's Publicly-Accessible Websites*. We incorporated the formal comments provided by your office. The report contains seven recommendations aimed at improving the information security controls over NARA's publicly-accessible websites. Your office concurred with the seven recommendations.

In accordance with NARA Directive 1201, *Audits of NARA Programs and Operations*, section S7.m, within 45 days of the date of this memorandum, please provide our office with a written response that includes your (1) corrective action plan and (2) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendations. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

As with all OIG products, we will determine what information is publicly posted on our website from the attached report. Should you or management have any redaction suggestions based on FOIA exemptions, please submit them to my counsel within one week from the date of this letter. Should we receive no response from you or management by this timeframe, we will interpret that as confirmation NARA does not desire any redactions to the posted report.

Consistent with our responsibility under the *Inspector General Act, as amended*, we may provide copies of our report to congressional committees with oversight responsibility over the National Archives and Records Administration.

Please call me with any questions, or your staff may contact Jewel Butler, Assistant Inspector General of Audits, at (301) 837-3000.

NATIONAL ARCHIVES *and*
RECORDS ADMINISTRATION

OFFICE *of*
INSPECTOR GENERAL



Audit of NARA's Publicly-Accessible
Websites

MARCH 25, 2016

OIG Audit Report No. 16-05

Table of Contents

Executive Summary 3

Background..... 5

Objectives, Scope, Methodology 7

Audit Results 9

 NARA Websites at Increased Risk 9

 Website Security Guidance 9

 Website Vulnerability Scanning 10

 Password Encryption 11

 Auto-Complete Functions..... 12

 Password Complexity 12

 User Credentials..... 13

 Password Reset 13

 Reflected Cross-Site Scripting..... 14

 Open Source Intelligence..... 14

 Insecure Configuration of HTTPS 17

 Security Assessment Review 19

Appendix A – Acronyms 21

Appendix B – Management’s Response to the Report..... 22

Appendix C – Report Distribution List 23

Executive Summary

Website vulnerabilities have become a point of emphasis for attackers trying to access an organization's Information Technology infrastructure. Securing publicly-accessible websites is critical to ensuring the security and accessibility of the National Archives and Records Administration's (NARA) Network. In this audit we found management oversight of NARA's publically-accessible website operations needs to be strengthened, and internal controls need to be enhanced, in order to ensure the security and protection of information hosted on NARA websites. This audit was included in the OIG's Annual Audit Plan and was requested by NARA's Chief Information Officer (CIO).

The objective of this audit was to evaluate the security of NARA's publicly-accessible websites. We also evaluated NARA's progress toward implementing Hypertext Transfer Protocol Secure (HTTPS)¹ on all of its websites as required by Office of Management and Budget (OMB) Memorandum M-15-13, and verified NARA conducted a review of security assessments associated with its cloud web hosting initiative.

The NARA's core mission is to provide public access to Federal records. The first goal of NARA's 2014 Strategic Plan, "Make Access Happen," states its objective is to make all records available to the public in digital form to ensure that anyone can explore, discover, and learn from NARA holdings. This cannot adequately happen without NARA's website infrastructure, including its publicly-accessible websites, its content and hosting environments being secured and protections in place commensurate with the risks to confidentiality, integrity, and availability of its publicly-accessible websites.

Our audit found NARA does not provide adequate management and internal controls to ensure the security of its publicly-accessible websites. As a result, NARA has reduced assurance all of the websites the agency is responsible for—including those processing Personally Identifiable Information (PII)—are secure, adequately protected, and/or compliant with federal security standards. In addition, the HTTPS configuration of NARA's websites does not meet federal guidelines. As a result, NARA is not able to guarantee its websites are providing the strongest privacy and integrity protection available to its users.

¹ HTTPS is a combination of Hypertext Transfer Protocol (HTTP) and Transport Layer Security (TLS). TLS is a network protocol that establishes an encrypted connection to an authenticated peer over an untrusted network.

We also found that NARA officials responsible for cloud hosted websites did not review critical security assessments. As a result, NARA's lacks assurance the agency's cloud web hosting environments are adequately secure and compliant with federal security standards.

This report makes 7 recommendations to improve the security surrounding NARA's publicly-accessible websites.

Background

Having a presence on the Internet is important in disseminating information to the public in an efficient and effective manner. This is especially true for the National Archives and Records Administration (NARA), who over the past several years has made making digital records available to the public an increasing focus of their strategic plans. Dating back to the Fiscal Year (FY) 2000 Strategic Plan, NARA has seen the need to provide public access to the Federal Government's records where ever they are located. In NARA's most recent 2014-2018 Strategic Plan, management took this a step further and made making public access to federal records a core goal. The realization of this strategic initiative is dependent, in part, on the ability of NARA's websites to provide public access to the digitized records. NARA relies on its websites for a variety of key functions ranging from providing access to digitized federal records to accepting requests for military personnel records.

The Office of Inspector General (OIG) has conducted a variety of audits focusing on the required elements of providing online access to federal records mainly because of the importance NARA has placed on making access to federal records available to the public. Much of the OIG's focus up to this point has been on NARA's efforts to digitize, store, and transfer federal records.² This is the second³ in a series of audits focusing on NARA's publicly-accessible websites and web hosting environments necessary to make access happen. The first audit in this area focused on NARA's web hosting environment and found NARA did not provide consistent oversight and management of the agency's public facing websites and web hosting environments. In addition, NARA did not require external vendors or partners to conduct and provide security assessments of the systems hosting NARA's websites. However, this audit focuses on the security of NARA's publicly-accessible websites.

Providing access to the Federal Government's records anywhere, anytime requires NARA to develop and publish websites that provide the public with access to NARA holdings. For the purpose of this audit, publicly-accessible websites and services are defined as online resources and services available over Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS) over the public internet that are maintained in whole or in part by the Federal Government and operated by an agency, contractor, or other organization on behalf of the agency.

² Recent related OIG audit products include: Audit Report No. 14-12, "Audit of Selected Aspects of NARA's Digitization Program;" Audit Report No. 15-10, "Audit of NARA's Digitization Partnerships;" and Audit Report No. 15-11, "Audit of NARA's Digitization Storage and Transfer Capabilities."

³ Audit Report No. 16-01, "Audit of NARA's Web Hosting Environment" was the first audit on this topic.

NARA's Office of Innovation ("Innovation") currently manages the agency's Web Program. Innovation, led by NARA's Chief Innovation Officer (CINO), oversees the development and maintenance of NARA's public and employee websites and social media activities. This includes supporting content contributors' development and maintenance of web content as well as ensuring compliance with Federal web design laws and guidelines (such as privacy, accessibility, and the Plain Language Act). However, they are not responsible for actually securing NARA's publicly-accessible websites; that responsibility belongs to NARA's Office of Information Services ("Information Services").

Information Services is responsible for securing NARA's internally hosted publicly-accessible websites and for providing guidance and technical support securing NARA's externally hosted publicly-accessible websites. Information Services is led by NARA's Chief Information Officer (CIO), and in part is responsible for managing NARA's information systems and the agency's nationwide information and telecommunications infrastructure.

Objectives, Scope, Methodology

The objective of this audit was to evaluate the security of NARA's publicly-accessible websites. In addition, we evaluated NARA's progress toward implementing HTTPS on all government websites as required by Office of Management and Budget (OMB) Memorandum M-15-13 "Policy to Require Secure Connections across Federal Websites and Web Services." We also evaluated whether NARA had proper controls in place to ensure security assessments for cloud hosted websites were reviewed prior to a contract being signed.

To accomplish our objective, we reviewed the following guidance: Government Accountability Office (GAO) "Standards for Internal Control in the Federal Government," Federal Information Security Management Act (FISMA) of 2002, National Institute of Standards and Technology Special Publication (NIST SP) 800-53 Revision 4 "Security and Privacy Controls for Federal Information Systems and Organizations," NIST SP 800-95 "Guide to Secure Web Services," DRAFT NIST SP 800-118 "Guide to Enterprise Password Management (DRAFT)," NIST SP 800-44 version 2 "Guidelines on Securing Public Web Servers," NIST SP 800-122 "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," OMB Memorandum M-15-13 "Policy to Require Secure Connections across Federal Websites and Web Services," NARA Directive 804 "Information Technology (IT) Systems Security," NARA Directive 807 "Content Rules and Requirements for NARA Web Sites (Internet, Intranet, and NARA-Hosted Extranets) and Presidential Library Web Sites," and NARA Directive 808 "Content Management for NARA's Main Public Web Site and Intranet." In addition, we reviewed NARA's current and previous strategic plans.

We interviewed NARA personnel from Innovation, Information Services, and Legislative Archives, Presidential Libraries, and Museum Services involved in security of NARA's publicly-accessible websites. We also obtained and analyzed internal documents relating to NARA's current and future implementation of HTTPS on its websites as well as the security of publicly-accessible websites. Finally, we conducted a test of 10 publicly-accessible websites⁴ to determine if NARA websites are vulnerable to external attacks. This test was not a comprehensive test of all the webpages within a specific website.⁵ Rather, it was a proof of

⁴ These websites were judgmentally sampled from the list of 86 websites originally identified during the OIG Audit Report No. 16-01, Audit of NARA's Web Hosting Environment. The OIG selected three internally hosted websites, four externally hosted websites, and three websites hosted by contractors at NARA facilities.

⁵ The OIG did not scan all webpages for a specific website. We judgmentally selected webpages from each website based on the types of webpages that are more susceptible to attacks such as search pages.

concept (POC)⁶ to demonstrate the need for improved security of NARA's publicly-accessible websites.

We used a variety of testing methods to determine if there were security vulnerabilities within the 10 websites. These methods included:

- conducting internet searches about each website to find hidden webpages;
- browsing the website for information that could be used to exploit vulnerabilities within NARA's website or network;
- using free web browser add-ins to gather open source intelligence such as the type of content management system or web server operating system; and
- using web application vulnerability tools to identify vulnerabilities within each website.

Through the use of these testing methods, we identified numerous weaknesses. However, once a weakness was identified, we did not exploit it any further. In addition, we did not try to gain access to NARA's IT infrastructure through the websites or gather personal information from its users.

Our audit work was performed at Archives II in College Park, Maryland between August 2015 and October 2015. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require 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 used judgmental sampling in our audit work; therefore the results of this sample were not used in projecting across the entire population. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

This audit was conducted by Andrew Clements, Senior IT Auditor.

⁶ A POC is a demonstration, the purpose of which is to verify certain concepts or theories have the potential for real-world application.

Audit Results

1. NARA Websites at Increased Risk

NARA's publicly-accessible websites are not adequately secured and properly protected. NARA has not provided adequate management oversight nor implemented strong or effective internal controls to ensure the security of its publicly-accessible websites. FISMA requires agencies 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 systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. FISMA goes on to require each agency head ensure that senior agency officials provide information security for the information and information systems supporting the operations and assets under their control. Without adequate management oversight and strong internal controls, NARA's ability to protect its publicly-accessible websites from the risk of unauthorized use, modification, and disclosure is affected. We identified numerous security deficiencies in NARA's publicly-accessible websites including, but not limited to the following:

- NARA has not developed sufficient security control guidance for websites
- NARA has not fully implemented website vulnerability scanning
- NARA websites are vulnerable to reflected cross-site scripting (XSS)⁷.
- NARA does not protect the confidentiality of the passwords used on its websites.
- Information within NARA websites provide attackers with insight into sensitive files and folders within NARA websites and employee information.

Website Security Guidance

Vulnerabilities within NARA websites leave website users, NARA employees, and NARA systems at increased risk of being the victims of attacks from external entities. Management provided insufficient guidance to website developers for securing NARA's publicly-accessible websites. Government Accountability Office *Standards for Internal Control in the Federal Government* ("GAO Standards") states management should design the entity's information system and related control activities to achieve objectives and respond to risks. Further, management should implement control activities through policies. IT Systems Security guidance—NARA Directive 804—does not go into sufficient detail for securing NARA's

⁷ Reflected (XSS) occur when an attacker injects browser executable code within a single HTTP response. The injected attack is not stored within the application itself; it is non-persistent and only impacts users who open a maliciously crafted link or third-party web page. The attack string is included as part of the crafted Uniform Resource Identifier (URI) or HTTP parameters, improperly processed by the application, and returned to the victim.

websites. Specifically, the IT Security Mechanisms supplement to NARA Directive 804 provides web developers with the following recommendations based on NIST SP 800-44 version 2 for securing NARA's web presence on the internet:

- NARA should implement appropriate security management practices and controls when maintaining and operating a secure Web presence.
- NARA should take steps to ensure [web content]...is adequately protected from unauthorized alteration.
- NARA should ensure appropriate steps are taken to protect Web content from unauthorized access or modification.
- NARA should use active content after carefully balancing the benefits gained against the associated risks.
- NARA must use authentication and cryptographic technologies as appropriate to protect certain types of sensitive data.

For example, NARA does not document how web designers and owners are supposed to adequately protect web content from unauthorized alteration, access, or modification. In addition, NARA websites did not implement authentication and cryptographic technologies that meet NIST SP 800-53 revision 4 requirements. Without sufficient guidance for maintaining a secure web presence, NARA's websites are left vulnerable to external threats.

Website Vulnerability Scanning

NARA does not routinely scan its publicly-accessible websites for vulnerabilities. NARA has not fully implemented their web vulnerability scanner, does not have a documented process to monitor the security controls surrounding their websites, and does not have the expertise to interpret the results from the scanner. GAO Standards state management monitors the internal control system through ongoing monitoring and separate evaluations. Further, management should establish and operate monitoring activities to monitor the internal control system and evaluate the results. Without comprehensive web vulnerability scanner, NARA cannot ensure information security protections are in place commensurate with the risk to the confidentiality⁸, integrity⁹, and availability¹⁰ of NARA's publicly-accessible websites.

In October of 2015, Information Services implemented a website vulnerability scanner capable of identifying specific web vulnerabilities in production. The scanner is designed to analyze web applications and web services for security vulnerabilities such as Structured Query Language

⁸ Confidentiality means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;

⁹ Integrity means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

¹⁰ Availability means ensuring timely and reliable access to and use of information

(SQL) Injection or XSS. However, Information Services has not determined the type of scan or the frequency the scan will be used on its websites and therefore, the scanner use is currently limited. Information Services is being cautious on its full implementation because the web vulnerability scanner can be highly intrusive and is capable of bringing down a website. Even if the vulnerability scanner was fully implemented, Information Services Contractors do not have the necessary expertise to interpret the scanner results.

Prior to the implementation of the website vulnerability scanner, NARA relied on a variety of processes to identify vulnerabilities within their websites. For some of the larger system development projects NARA required a code review to identify vulnerabilities within a website. NARA also relied on network vulnerability scanners employed by NARA and the Department of Homeland Security (DHS). These network vulnerability scanners were designed to identify outdated software versions, missing patches, and misconfigurations, and validate compliance with or deviations from an organization's security policy. While these products could identify some website vulnerabilities, they could not discover them all. Without a fully implemented website vulnerability scanner, NARA is not able to proactively identify risk affecting the confidentiality, integrity and availability of their websites.

Password Encryption

We identified three websites that do not protect user credentials as they are transmitted over the internet. NARA has not encrypted the network traffic to ensure the confidentiality of passwords from external threats is not compromised. The current draft of NIST SP 800-118 states agencies need to take steps to protect the confidentiality, integrity, and availability of passwords so that all authorized users—and no unauthorized users—can use passwords successfully as needed. It goes on to state passwords transmitted over networks should be protected from sniffing threats by encrypting the passwords or the communications containing them, or by other suitable means. As a result, NARA is not able to adequately protect the confidentiality of passwords as they are transmitted over the Internet.

Passwords are a mechanism for agencies to protect data, systems, and networks. NARA websites allow users to login to Administrator accounts or shopping carts with a password. Users who log into these pages are able to change the website content or purchase Presidential memorabilia online. Two of these websites transmitted user credentials over the internet without encryption. The other website used HTTP Basic Authentication¹¹ to transmit unencrypted credentials between the user's computer and web server. While the user's credentials are not transmitted in cleartext, Basic Authentication does not offer much protection for user credentials.

¹¹ Basic Authentication transfers all password information in encoded, rather than encrypted, form. According to NIST SP 800-44 version 2, anyone who knows the standardized encoding scheme can decode the password after capturing it with a network sniffer.

This type of encoded text can easily be decoded using most vulnerability scanning tools. NIST SP 800-53 revision 4 requires information systems that utilize password-based authentication to store and transmit only cryptographically-protected passwords. As a result, anyone monitoring the internet communications for these websites would be able to capture the user's credentials without them knowing about it.

Auto-Complete Functions

We found auto-complete functions were allowed on two NARA websites. Auto-complete is a component of some applications, such as web browsers, that provide password management features for websites. In some cases, these applications essentially provide a built-in password management utility that stores the passwords securely and controls access to them through a user-set master password. In other cases, the stored passwords may be stored less securely and may be provided automatically as needed without any user authentication. NARA should not leave it up to the user to decide whether to store the user's credentials in a web browser due to the uncertainty over the security of passwords.

While DRAFT NIST SP 800-118 does not specifically say organizations should not store passwords in applications, it does say they should carefully consider the risks involved in storing passwords locally outside of password management software and generally should permit only the lowest-risk passwords to be stored in such a manner. An attacker who gains physical or logical control over the user's workstation [would be able] to use the stored passwords without any further steps. As a result, the attacker who gains access to the passwords could deface or worse, bring the website down.

Password Complexity

We identified two websites that do not meet NARA's password complexity requirements for information systems (See Table 1 for more information). The IT Security Requirements supplement to NARA Directive 804 requires all data, the information system shall ... enforce a minimum password complexity of a case sensitive, 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each. NARA is not adhering to its own password complexity requirement. As a result, NARA is not able to ensure the confidentiality and integrity of each website.

Website	Password Configuration Settings				
	Number of Characters	Capital Letter	Lower Case Letter	Number	Special Character
NARA Requirement	8	✓	✓	✓	✓
Website 1	6		✓	✓	
Website 2	1		✓		

Table 1: Password Configuration Settings Comparison

One of the more challenging aspects of ensuring the confidentiality of passwords is the password complexity requirements for external users of the websites. Requiring complex passwords will mitigate an attacker's ability to guess¹² or crack¹³ a user's password. Complex passwords are especially important when a website stores or allows for the entry of personally identifiable information (PII) (e.g. credit card numbers) as these two websites do. NIST SP 800-122 states that it is important to protect the confidentiality of PII in an information system. However, neither of these websites required users to create passwords that meet NARA requirements (See Table 1 for more information). Without the appropriate safeguards to protect websites, NARA is left vulnerable to the theft of PII.

User Credentials

We identified a NARA website that sends cleartext emails with user credentials (username and password) after a new account has been created or password reset. NARA has not implemented the appropriate security controls to protect the confidentiality of PII processed on the website. NIST SP 800-53 revision 4 requires agencies to store and transmit only cryptographically-protected passwords. This is especially critical for a website that processes PII (e.g. credit card information) as this website does. NIST SP 800-122 states organizations should apply appropriate safeguards to protect the confidentiality of PII based on the PII confidentiality impact level. As a result, PII is left vulnerable to external threats should the user's credentials be compromised.

Password Reset

We identified two websites without appropriate security controls to ensure the confidentiality of PII. These two websites do not require users to change their password after it has been reset. As a result, PII is left vulnerable to external entities should the temporary password be

¹² Guessing involves repeatedly attempting to authenticate using default passwords, dictionary words, and other possible passwords.

¹³ Cracking is the process of an attacker recovering cryptographic password hashes and using various analysis methods to attempt to identify a character string that will produce one of these hashes, thereby being the equivalent of the password to the targeted system.

compromised. NIST SP 800-53 revision 4 allows the use of a temporary password for system logons with an immediate change to a permanent password.

Password resets are a mechanism for users who forget their password to create a new one. A password reset is often accomplished by setting a one-time password (OTP), which is a password that is set to expire immediately, and thus can only be used to gain access to a system one time. There are a number of ways users are able to reset passwords including the fully automated mechanism used by these two websites. When a user resets a website password they are required to verify their identity. Once verified, the user is provided a randomly generated password to use on their next login. Typically when a user logs into the website they are required to change their password immediately. However, the user is not required to do so for these websites.

Reflected Cross-Site Scripting

Three out of the ten websites tested were subject to reflected XSS. Generally reflected XSS attacks start with an attacker sending a carefully crafted phishing¹⁴ email to an unsuspecting user telling the user to click on a link. The link would be a modified web address including malicious script imbedded in the link. When the user clicks on the link the attacker's code is executed leaving the user vulnerable to the nefarious nature of the code. Through this type of attack, the attackers could do anything from capturing user credentials and session information to redirecting a user to a malicious website.

While this vulnerability was identified by a vulnerability scanner, we verified that reflected XSS exists within each of the three websites. We used the steps and malicious code provided by the scanner to replicate the issue on each website. We started by adding the code to the website web address in the browser bar. Once the code was submitted the results of the script varied based on the website and the code that was added. In some cases an image icon was added to the webpage while in others a pop-up box appears asking for the user to click a button. Finally, the code was also added to the underlying source code for the print button on the website. When a user clicks on the print button the code is activated and the user is subject to the malicious nature of the code without realizing it. This vulnerability affects NARA's ability to protect the confidentiality and integrity of each website.

Open Source Intelligence

NARA websites provide attackers with information about sensitive webpages through a robots.txt file. Robots.txt is a file that provides web robots¹⁵ with instructions about the webpages that should or should not be scanned on a specific website. While this file could

¹⁴ Phishing is a deceptive computer-based means to trick individuals into disclosing sensitive personal information.

¹⁵ Web Robots (also known as Web Wanderers, Crawlers, or Spiders), are programs that traverse or crawl the Web automatically. Search engines such as Google use them to index the web content, spammers use them to scan for email addresses, and they have many other uses.

provide a benefit if it were used by the robots, NARA should not assume it is being used for its intended purpose. Instead, NARA should assume attackers pay close attention to the sensitive webpages identified in the file. NIST SP 800-44 version 2 states a Web administrator should not specify the names of sensitive files or folders... in a robots.txt file. For example, a robots.txt may say Disallow: /user/login/. This tells the web robot not to crawl and index the /user/login webpage of the website. As a result, if the robot followed the robots.txt instructions a user could not search for that webpage on search engines such as Google or Yahoo!. By providing sensitive information in a robots.txt file, the web designer is informing an attacker there is a login page at /user/login, and allowing easier access to hidden webpages. We reviewed the robots.txt file for four of the ten websites tested. Two of those sites listed sensitive login pages where we identified password vulnerabilities previously mentioned.

We also found NARA published an employee directory to their Freedom of Information Act (FOIA) webpage. The directory included the first and last name plus phone number and email addresses for all federal government employees and contractors that work for NARA. NIST SP 800-44 version 2 states absent compelling reasons, a public web site should not contain . . . this type of information . . . unless necessary to fulfill organizational requirements. NIST SP 800-44 version 2 goes on to state attackers often read the contents of a target organization's Web site to gather intelligence before any attacks. Also, attackers can take advantage of content available on a Web site to craft a social engineering attack or to use individuals' identifying information in identity theft. While this information by itself does not necessarily allow for an attack on NARA's IT infrastructure, it does provide an attacker a starting point for creating an employee's username as well as access to thousands of emails for spamming purposes.

In addition, we found a list of credit card holders on the FOIA webpage. The list includes the names and dollar limits for government credit card holders as well as the approving official. NIST SP 800-44 version 2 goes on to state that financial records (beyond those already publicly available) should not be included on a public website unless there is a compelling reason. When you combine the emails provided in the employee directory with the list of government credit card holders posted on the FOIA webpage, NARA has the beginnings of a spear phishing attack¹⁶. As a result, NARA credit card holders are left vulnerable to external attacks by individuals who are trying to steal credit card information for nefarious reasons.

¹⁶ An e-mail spear-phishing attack involves crafting a convincing e-mail for selected recipients that appears to be from a trusted source and that, when opened, infects the recipient's computer with a virus. Attackers may gather personal information about their target to increase their probability of success.

Recommendations

1. We recommend the CINO coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the:
 - a. CINO coordinate with the CIO on the development of policies and procedures for secure website design and implementation that apply to all NARA publicly-accessible websites.
 - b. CINO coordinate with the CIO to ensure all publicly-accessible websites are compliant with NIST SP 800-53 revision 4.
 - c. CIO regularly (at least quarterly) conducts a comprehensive web vulnerability scan on all NARA publicly-accessible websites.
 - d. CIO documents the process conducting a web vulnerability scan on all publicly-accessible websites.
 - e. CIO provides the necessary training to IT Security personnel to be able to review and interpret the vulnerability scanner results.
 - f. CIO prevents users from saving their credentials in web browsers.
 - g. CIO requires all NARA publicly-accessible websites to apply NARA's password configuration requirements.
 - h. CIO requires all publicly-accessible websites to only send cryptographically protected user credentials.
 - i. CIO requires users to change their passwords after a website password reset.
 - j. CIO analyzes all publicly-accessible websites to determine if they are vulnerable to all variations of cross-site scripting including reflected.
 - k. CINO coordinates with the CIO to review all publicly-accessible websites for any potential information that could affect NARA's IT security posture.
1. NARA General Counsel coordinates with the CIO and CINO on the publishing of the NARA employee directory and Government credit cardholders list to ensure the security of NARA employees is taken into consideration.

2. Insecure Configuration of HTTPS

NARA has not securely and consistently configured HTTPS on its websites. We identified 14 websites that currently implement HTTPS and found 9 of these websites do not meet federal guidelines for secure HTTPS configuration. NARA has not developed any guidance to ensure HTTPS is securely and consistently configured on its websites. According to NIST SP 800-44 version 2 if Secure Socket Layer (SSL)/ Transport Layer Security (TLS) is implemented or used incorrectly, the communications intended to be protected may be vulnerable to a “man in the middle¹⁷” (MITM) attack. The GAO Standards goes on to state management should implement control activities through policies. As a result, NARA is not providing the strongest privacy and integrity protection available to its users as required by OMB Memorandum M-15-13.

In order to improve security for all federal government websites the Federal Chief Information Officer requires all websites to implement HTTPS by December 31, 2016. Although the deadline is later in the year, NARA has already implemented HTTPS on some sites. In validating the HTTPS configuration on NARA’s websites, we utilized the Qualys SSL Labs website to determine if the websites meet current federal guidelines for secure HTTPS configuration. SSL Labs grades websites using an A+ through F scale. Each website is evaluated based on three categories: Protocol support¹⁸, Key exchange support¹⁹, and Cipher support²⁰. The results from the OIG’s scan ranged from 5 websites receiving an A grade to 3 websites failing the scan (See Chart 1 for more information).

¹⁷ An MITM attack occurs when an attacker intercepts communication between two systems. One system would be the system a user would try to access like a web server and the other system would be the user's system. In this case the attacker would intercept the communication between the web server and the user's system. The attacker would start communicating with the web server and the user's system would start communicating with the attacker. As a result, the user's system could be passing confidential information to the attacker even though the user thinks they are communicating with the web server.

¹⁸ These are the protocols such as TLS 1.2 or SSL 3.0 that are supported by an SSL server.

¹⁹ The key exchange phase serves two functions. One is to perform authentication, allowing at least one party to verify the identity of the other party. The other is to ensure the safe generation and exchange of the secret keys that will be used during the remainder of the session.

²⁰ To break a communication session, an attacker can attempt to break the symmetric cipher used for the bulk of the communication. A stronger cipher allows for stronger encryption and thus increases the effort needed to break it.

SSL Labs Website Grades

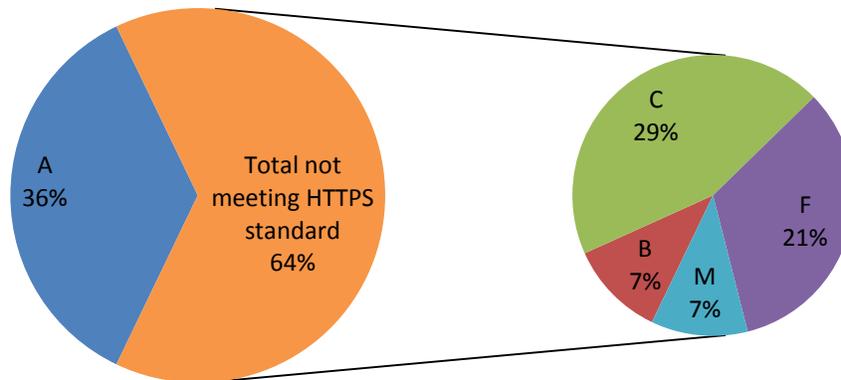


Chart 1: HTTPS configuration grades for NARA websites.

In reviewing the results of the configuration scan we determined that the websites did not meet federal guidelines for a variety of reasons. For example, three websites failed because they could be subject to a MITM attack. Had these websites not been subject to a MITM attack they would have received a C grade because they do not support TLS 1.2.²¹ Another website received a grade of M for mismatch name by SSL Labs. This website would have received an A had the actual website name matched the website name on the encryption certificate.

In an effort to meet the federally mandated HTTPS requirement, NARA established a working group, in June of 2015 tasked with:

- overseeing the conversion of all publicly-accessible websites to meet the HTTPS standard;
- developing and documenting NARA's HTTPS configuration guidance; and
- developing a centralized process for managing existing and new implementations of HTTPS as required by OMB Memorandum M-15-13.

However, as of the end of fieldwork, NARA had not developed internal HTTPS configuration guidance. Without HTTPS configuration guidance, NARA lacks assurance the HTTPS configurations are adequately implemented. Further, the internet traffic protected by encryption may not be as secure as users of the website believe, leaving NARA's websites vulnerable to potential and preventable attacks.

²¹ TLS is a protocol created to provide authentication, confidentiality, and data integrity between two communicating applications, 1.2 is the latest version of this protocol.

Recommendations

We recommend the CIO:

2. Develop guidance for securely configuring HTTPS.
3. Implement secure HTTPS configurations for all publicly-accessible websites
4. Regularly scan (at least quarterly) all publicly-accessible websites to determine if HTTPS is securely configured.

3. Security Assessment Review

Security assessments for cloud web hosting providers were not reviewed. NARA does not have a standard process in place to review security assessments performed on cloud web hosting environments. FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. GAO Standards require management to evaluate and document the results of ongoing monitoring and separate evaluations to identify internal control issues. Management uses this evaluation to determine the effectiveness of the internal control system. By not evaluating the security assessments, NARA lacks assurance the agency's cloud web hosting environments are adequately secured and compliant with FISMA.

During the Audit of NARA's Web Hosting Environment, we determined security assessments were not performed on approximately 60% of external web hosting environments. In that audit, we identified six instances where security assessments were performed on cloud web hosting providers. During this audit, we reviewed the six instances where security assessments were performed on cloud web hosting providers and found only one of the six security assessments was reviewed by a NARA employee. NARA did not provide adequate oversight to ensure the security assessments were reviewed. Security assessments are designed to evaluate the IT security controls surrounding federal IT systems such as a web hosting environment. When NARA does not review security assessments, NARA's ability to ensure the web hosting environments are adequately secure is inhibited due to NARA's lack of insight into the security controls implemented in the environment. As a result, NARA does not have the information necessary to determine how secure the web hosting environments are, even though they store federal information.

Recommendations

We recommend the CIO:

5. Document a process to review all security assessments by a qualified official.
6. Ensure Information Services personnel review all cloud hosting security assessments.
7. Ensure Information Services personnel document their review of the IT security assessments.

Appendix A – Acronyms

CIO	Chief Information Officer
CINO	Chief Innovation Officer
DHS	Department of Homeland Security
FOIA	Freedom of Information Act
FY	Fiscal Year
FISMA	Federal Information Security Management Act
GAO	U.S. Government Accountability Office
GAO Standards	Government Accountability Office <i>Standards for Internal Control in the Federal Government</i>
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
Information Services	Office of Information Services
Innovation	Office of Innovation
IT	Information Technology
MITM	Man in the Middle
NARA	National Archives and Records Administration
NIST SP	National Institute of Standards and Technology Special Publication
OIG	Office of Inspector General
OMB	U.S. Office of Management and Budget
OTP	One-time Password
PII	Personally Identifiable Information
POC	Proof of Concept
TLS	Transport Layer Security
POC	Proof of Concept
SQL	Structured Query Language
SSL	Secure Socket Layer
TLS	Transport Layer Security
URI	Uniform Resource Identifier
XSS	Cross-Site Scripting

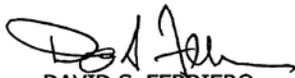
Appendix B – Management’s Response to the Report



Date: MAR 24 2016
To: James Springs, Inspector General
From: David S. Ferriero, Archivist of the United States
Subject: *OIG Draft Audit Report 16-05, Audit of NARA's Publicly-Accessible Websites*

Thank you for the opportunity to provide comments on this draft report. We appreciate your willingness to meet and clarify language in the report.

We concur with the seven recommendations in this audit, and we will address them further in our action plan.



DAVID S. FERRIERO
Archivist of the United States

NATIONAL ARCHIVES *and*
RECORDS ADMINISTRATION
8601 ADELPHI ROAD
COLLEGE PARK, MD 20740-6001
www.archives.gov

Appendix C – Report Distribution List

Archivist of the United States
Deputy Archivist of the United States
Chief Innovation Officer
Chief Information Officer
Chief Operating Officer
Deputy Chief Operating Officer
Executive for Agency Services
Executive for Business Support Services
Executive for Legislative Archives, Presidential Libraries, and Museum Services
Executive for Research Services
Director, National Historical Publications and Records Commission
Audit Liaison

OIG Hotline

To report fraud, waste or abuse, please contact us:

Electronically: <https://www.archives.gov/oig/referral-form/index.html>

Telephone: 301-837-3500 (Washington, D.C. Metro area)
1-800-786-2551 (toll-free and outside the Washington, D.C. Metro area)

Mail: IG Hotline
NARA
P.O.Box 1821
Hyattsville, MD 20788-0821