AUDIT OF NARA'S WORK-AT-HOME SYSTEM

OIG Audit Report No. 09-15

September 29, 2009

EXECUTIVE SUMMARY

The National Archives and Records Administration (NARA) Office of Inspector General (OIG) completed an audit of NARA's Work at Home System (WAHS). The WAHS was initiated to enhance NARA's remote access capabilities while satisfying the Office of Management and Budget (OMB) mandate for two-factor authentication[1]. During this audit, we assessed NARA's efforts in developing this system to determine whether the WAHS was developed in accordance with NARA requirements and would meet OMB technical requirements.

In June 2006, OMB issued memorandum M-06-16, *Protection of Sensitive Agency Information*, requiring all departments and agencies to only allow remote access with two-factor authentication where one of the factors was proved by a device[2] separate from the computer gaining access. The intention of this mandate was to ensure additional controls were in place when information, particularly Personally Identifiable Information (PII), is accessed from outside of an agency's physical location. Additional controls are needed to compensate for the lack of physical security controls, such as locks, badges, and security guards, which are present at agency locations. This safeguard along with others were to be reviewed and in place within 45 days of the memorandum. NARA had been working on the WAHS since 2007 to meet this two-factor authentication mandate.

Our review found that because of the significant delay in the implementation of the WAHS, NARA was not in compliance with the two-factor authentication requirements mandated by OMB. The WAHS was a high-priority project to be completed within a very short timeframe. However, the requirements of NARA's IT Investment Management Process[3] were not followed resulting in significant program delays, cost overruns, and failure to meet OMB defined requirements. This overarching condition has left NARA information vulnerable, restricted telecommuting, and impacted NARA's budget through cost overruns and lease of equipment to include tokens, at a cost of over $200,000, which could not be deployed. Further, by not fully defining system requirements, critical technical challenges still needed to be addressed before the system could be fully operational and meet the intent of OMB requirements. Consequently, a system originally estimated to cost $500,000 has now escalated to over $1.23 million and is still far from full implementation.

Our audit identified several improvements to be made in the development and deployment of the WAHS. We made seven recommendations to ensure the system meets OMB requirements and improves the security of remote access to PII and NARA proprietary information.

---

[1] An authentication factor is a piece of information and process used to authenticate or verify a person's identity requesting access. Two-factor authentication is a system wherein two different factors are used to authenticate. Using two factors as opposed to one delivers a higher level of authentication assurance.
[2] Examples of separate devices include USB tokens and smart cards.
[3] NARA's IT Investment Management Process is detailed in Interim Guidance 801-2, *Review of IT Investments*.

BACKGROUND

Effective project management is essential in obtaining the right equipment and systems to accomplish NARA's mission. Specifically, system development projects must be managed and tracked to ensure cost, schedule, and performance goals are met. If systems are not adequately and properly managed, NARA could end up with overpriced systems that do not meet NARA requirements or mission.

The OIG has repeatedly found that NARA systems are not always developed in accordance with NARA guidelines; system projects are not always effectively managed and monitored; and proper system acceptance activities may not occur prior to the agency accepting delivery of a system. As a result, the OIG has listed project management and system development activities as one of NARA's top ten challenges noting that the agency is challenged with planning projects, developing adequately defined requirements, analyzing and testing to support acquisition and development of systems, and oversight to ensure effective or efficient results within costs.

The Office of Information Services (NH) is responsible for administering NARA's information resources management programs, projects, processes, and infrastructure, including the overall operation of NARA's Information Technology (IT) Investment Management process. Within NH, the Capital Planning and Investment Process (CPIC) is directed by IT Policy and Administration Division (NHP). NHP ensures that all NARA IT initiatives are properly planned, costed, reviewed, and approved by the senior staff before significant funds are expended. The proposals and product plans required to complete this process are described in NARA Interim Guidance 801-2, *Review of Information Technology Investments* (NARA 801).

Also within NH, the Systems Development Division (NHV) provides project management leadership for the requirements collection, development and major enhancements of IT applications and systems. NHV Project Managers are responsible for cost, schedule, quality, communications, and risk management of these projects. Project Managers are also responsible for ensuring new IT systems or major modifications to IT systems conform to the Systems Development Lifecycle Handbook and the Systems Development Guidelines.

The WAHS, which consisted of several commercial-off-the-shelf (COTS) software packages, was expected to implement an IT infrastructure system that would enable secure, remote access to selected General Service Systems (GSS) that reside on NARANet to include: GroupWise e-mail access, file access to shared and personal drives, access to NARA@Work content, access to Microsoft Office 2003 applications, and access to the Internet. System capabilities included the need to (1) support the Work-at-Home initiative as part of the agency's Comprehensive Emergency Management (CEMP) and Continuity of Operations Plan (COOP) activities, and (2) implement two-factor authentication as mandated by the OMB Memorandum 06-16, *Protection of Sensitive Agency Information.*

OBJECTIVE, SCOPE, METHODOLOGY

The objective of this audit was to determine whether the WAHS was developed in accordance with NARA requirements and efficiently and effectively met the requirements of the OMB memorandum M-06-16, *Protection of Sensitive Agency Information*. Specifically, we sought to determine whether the project proposal, plan, and approval were completed in accordance with NARA requirements and whether technical requirements were developed to meet OMB requirements for remote access. The audit was limited to the development, testing, pilot, and implementation of the WAHS.

We examined applicable laws, regulations, and NARA guidance, including (a) OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*; (b) Clinger-Cohen Act; (c) Homeland Security Presidential Directive (HSPD) -12; (d) National Institute of Standards and Technology (NIST) Special Publication 800-53, *Recommended Security controls for Federal Information Systems*; (e) Federal Information Processing Standards Publication (FIPS PUB) 140-2, *Security Requirements for Cryptographic Modules*; (f) NARA Interim Guidance 801-2, *Review of Information Technology Investments*; and (g) Supplement to NARA 801-2, *System Engineering Capital Planning Investment Management Decide Process*.

To accomplish our objective, we met with the WAHS Project Manager and other NARA officials involved with the WAHS project. We reviewed the WAHS project proposals and other system development documents such as the Concept of Operations and Initial Requirements Specification, Design Specification, and monthly Capital Planning and Investment Process reports. We also reviewed Requests for Changes (RFCs) and Requests for Work (RFWs) related to the WAHS and meeting minutes of various NARA IT committees.

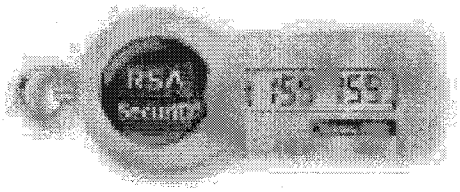
Our audit work was performed at Archives II in College Park, MD between December 2008 and June 2009. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

FINDINGS AND RECOMMENDATIONS

NARA Was Not Compliant with OMB Mandated Two-Factor Authentication

NARA was not in compliance with the two-factor authentication requirements for remote access mandated by OMB in June 2006. This occurred because NARA failed to meet several established deadlines to implement the WAHS, which was intended to meet the OMB mandate. Consequently, NARA's email system remained vulnerable to network and hacker attacks and NARA was unable to protect PII and NARA proprietary information from being distributed or compromised over its network and email system.

In June 2006, OMB issued memorandum M-06-16, *Protection of Sensitive Agency Information*, requiring all departments and agencies to only allow remote access with two-factor authentication where one of the factors was provided by a device, such as a RSA token, separate from the computer gaining access. The specific intent of this mandate was to compensate for the protections offered by the physical security controls when information was removed from or accessed outside of the agency locations. This safeguard along with others were to be reviewed and in place within 45 days of the June 23, 2006 memorandum.



Example of a RSA Token

At the time of our audit, NARA was not in compliance with the two-factor authentication requirements for remote access mandated by OMB. NARA did not have an enterprise-level remote access solution in place for its Work-at-Home or telework staff and NARA employees were unable to access NARA's intranet or shared drives from remote locations. Instead, NARA had two remote access solutions in place; however, neither were designed or priced to provide remote access for the entire NARA work force. Their purpose and use were intended for restricted access by NARA IT operations staff and specific IT operations contract personnel for purposes of keeping the NARA information infrastructure, application servers, and other components operational. ----------
---
----------Redacted pursuant to FOIA Exemption "high" b(2)----------
---

In 2007, NARA began developing WAHS to meet the OMB requirement for two-factor authentication. However, due to a demonstrated lack of sound project management, this system has not been fully implemented. The Project Plan schedule showed that the WAHS would be deployed in September 2008, but the project did not meet this deadline. In an updated schedule, the deployment of the WAHS is schedule to be completed in December 2009, 15 months after the original deployment date. Other deadlines in the project have been missed, including deadlines relating to user testing. Originally, WAHS was to be piloted with an advanced testing group of 50 NARA users by April 30, 2008; however, this was not completed until September 2008 and only 18 testers were included. Also, in a revised schedule, additional NH user testing was to be

completed by January 7, 2009 and testing of users outside of NH was to be completed by March 19, 2009. However, the additional NH testing was not completed until February 20, 2009 and as of May 21, 2009, testing outside of NH had not been completed. Successful user testing is important because it ensures the system meets defined acceptance criteria and operational objectives.

Without the WAHS in place, NARA continues to manage its remote access systems in their current state and is unable to provide two-factor authentication for remote access. ---------- Redacted pursuant to FOIA Exemption "high" b(2)----------.

Additionally, by not having an enterprise-level remote access solution in place, telework capabilities for NARA employees have been limited. NARA has over 2,700 employees who are eligible to work from home. However, some NARA employees were not able to work from home because of the lack of a secure remote access system. As the workforce continues to move away from traditional work times and locations, more employees will require easy, regular access to email and calendars. Further, the Office of Personnel Management has emphasized the importance of being telework ready, in order to continue essential operations during all phases of a pandemic influenza. Specifically, agencies need to implement and maintain a robust IT system with the necessary infrastructure including, bandwidth and VPN access to accommodate a sudden spike in remote usage of systems.

Finally, during the audit, NARA's current Nortel Virtual Private Network[4] (VPN) solution suddenly experienced an outage. By not fully deploying the WAHS, the replacement for the Nortel VPN, NARA did not have a remote access system to replace ---- Redacted pursuant to FOIA Exemption "high" b(2)---. Thus, NARA employees continued to not have secure remote access capabilities and ---------- Redacted pursuant to FOIA Exemption "high" b(2)----------.

Recommendation 1

We recommend the CIO ensure a system is put in place which meets the requirements for remote access with two-factor authentication.

Recommendation 2

We recommend the CIO discontinue or phase out any remote access which does not require two-factor authentication.

Recommendation 3

[4] The Nortel VPN provides remote access capabilities for some NARA users. This access requires a properly configured NARA-issued laptop. The WAHS was developed to replace the Nortel VPN and greatly enhance the security of NARA's remote access.

We recommend the CIO monitor the WAHS to ensure the established milestones and deadlines are met.

Management Comment(s)

Management concurred with recommendations.

NARA Did Not Follow IT Investment Management Requirements

In developing the WAHS, NARA did not follow all of the requirements of NARA's IT Investment Management Process. This occurred because management did not enforce the use of the process outlined in NARA 801 and the project proposal was not verified to ensure that proposal information was complete and adequately supported. Consequently, the approved solution was not adequately planned which contributed to the project falling behind schedule and wasting limited resources. Further, alternatives were not completely vetted prior to the approval of the WAHS and NARA may not have chosen the best alternative for remote access with two-factor authentication.

The Clinger-Cohen Act required each agency to design and implement a process for maximizing the value and assessing and managing the risks of their information technology acquisitions. The act also required each agency to establish effective and efficient capital planning processes for selecting, managing, and evaluating the results of all of its major investments in information systems. To meet the requirements of the Clinger-Cohen Act, NARA developed its IT Investment Management Process, which was documented in NARA's Interim Guidance 801-2, *Review of Information Technology (IT) Investments* (NARA 801). One of the phases of this process is the Decide Process, which is described in the supplement to NARA 801, *System Engineering Capital Planning Investment Management Decide Process*. The Decide Process was intended to help ensure NARA (1) selects the best mix of IT investments to support NARA's strategic goals and (2) thoroughly analyzes an investment before a significant amount of resources are expended for those investments.

In the Decide Phase, projects being proposed for funding are reviewed and initially screened to (1) eliminate proposals that do not warrant further development and (2) ensure that full proposals are reviewed at the most appropriate organizational level. Critical aspects of this phase are management understanding, participation, and decision-making driven by accurate, up-to-date data, and an emphasis on using IT to efficiently achieve strategic goals. Proposals that pass the screening process have their costs, benefits, and risks analyzed in-depth. This analysis is documented in a "Full Proposal". In general, Full Proposals assemble and analyze data collected and documented in system development lifecycle deliverables, such as Concept of Operations, Requirements Document, and Analysis of Alternatives. The supplement to NARA 801 provides the template and details the requirements for a Full Proposal.

We found the WAHS was not developed or approved in accordance with these Federal and NARA requirements. Particularly, we noted deficiencies in the project proposal, risk assessment, approval process, and authorized spending.

Project Proposal

Prior to the approval of the WAHS, a project proposal was prepared using the appropriate template in NARA 801. However, the project proposal did not include all necessary information and in some cases misleading or incorrect information was included in the proposal. The following critical information was missing in the project proposal:

- The Design Overview section did not describe a technically feasible design, which could be accomplished within the time constraints of the project.
- The Assumptions and Constraints section did not address critical planning items such as scope, schedule, workload, dependencies, technology, users, stakeholders, interfaces, funding, and security.
- Security requirements and costs were not identified and integrated into the overall lifecycle cost of the investment and included in the investment's Cost Benefit Analysis (CBA) worksheet.

Misleading or incorrect information was also included in the Analysis of Alternatives, Project Benefits, and Acquisition Strategy sections. Specifically, the Analysis of Alternatives section stated that the selected alternative was "already proven and tightly integrated with the Citrix Access Suite currently in use at NARA". According to the Project Sponsor, this was based on the results of two other organizations (U.S. Patent Trade Office and Department of Treasury) that had successful results using Citrix and RSA tokens. However, both of these organizations had Microsoft exclusive operating environments, whereas NARA has a mixture of Novell and Microsoft operating environments. NARA's Novell system is not widely used in industry or government and offices, such as the Presidential Libraries, often run into interoperability problems with their strategic partners. Therefore, the statement could have been misleading to decision makers selecting the best alternative.

Also, in the discussion of Project Benefits, it stated NARA must implement the WAHS capability to satisfy an OMB mandate and comply with Homeland Security Presidential Directive - 12[5] (HSPD-12). However, the selected alternative did not meet the requirements of HSPD-12, which mandated the use of a Personal Identity Verification (PIV) to gain both physical and logical access to federally controlled information systems.

Finally, the acquisition strategy section of the project proposal should discuss how competition will be sought, promoted, and sustained. However, competition was not addressed in this section of the WAHS proposal. Instead, the proposal only stated that

[5]The purpose of this directive was to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors.

two existing contracts would be used to address the scope of this effort. This approach may have been acceptable; however, additional funding, totaling over $190,000, was required for one of the contractors to complete the needed tasks. This additional funding was not anticipated and was provided to the contractor through Technical Direction Letters, with a total ceiling price of $427,324. Therefore, the acquisition strategy for the WAHS did not thoroughly seek, promote, or sustain competition.

Having complete and accurate information in the project proposal is crucial because, once a project proposal has been reviewed and approved, it becomes the Product Plan. This plan should incorporate (1) changes recommended as part of the proposal approval process and (2) the milestone review schedule established by the CIO.

Risk Assessment

The overall WAHS project risk assessment was also incorrect. According to NARA guidance, the highest risk factor in the areas of Technical Deployment, IT Architecture Impact, and Legal Regulations determines the overall project risk. Originally, the WAHS project was given a medium risk rating, even though its Technical Deployment[6] was rated as high. Since the WAHS was considered an enterprise-wide project, this rating was appropriate. Therefore, the WAHS should have been rated as a high risk project.

Approval of Project

Because of the incorrect project risk rating, the WAHS proposal **was not** submitted to Information Technology Executive Committee (ITEC) for formal discussion, review, or scrutiny. ITEC was established to set the overall direction and polices governing NARA's information technology infrastructure and is responsible for prioritizing and advocating the rollout of major information technology initiatives. Also, as Chairman of ITEC, the Archivist or designated representative, is responsible for approving changes in direction or adoption of emerging technologies. According to the ITEC Secretary, any proposal with a high risk rating is required to be approved by ITEC. However, since the initial WAHS project proposal was incorrectly rated as "medium", the WAHS was not formally reviewed, scrutinized, and approved by the members of ITEC prior to its approval.

After the WAHS proposal was approved, senior NH officials were asked if other alternatives were considered for the WAHS. The response was that no other alternatives were considered because the cost factor only approached $500,000. This was based on incorrect information or a misconception given the project's three year outsourcing costs totaled over $700,000 and the ten year total costs were over $5.2 million.

Project Spending

[6] Technical deployment refers to the scope of project use from an organizational viewpoint.

Finally, NARA's Decide Process requires projects to be thoroughly analyzed before a significant amount of resources are expended. The pilot of the WAHS was authorized to spend up to $150,000. However, prior to the official approval of the WAHS, over $500,000 had already been spent on the project.

These deficiencies occurred because the controls outlined in the NARA 801 were not effectively implemented or enforced. Not only did the Proposal Development Team develop an incomplete project proposal, but NARA management did not enforce the process outlined in NARA 801 to ensure that an adequate project proposal was developed and approved. The proposal was reviewed and approved by the Architecture Review Board (ARB) and the Business Architecture Working Group (BAWG) even though some members of the BAWG had not completed their review. Also, since the project was assigned an incorrect risk rating, it was not reviewed at the most appropriate organization level. The WAHS was not formally discussed at an ITEC meeting until after it was approved. Further, during these reviews, emphasis was not placed on finding or considering other alternatives; the only option presented throughout the process was approved. Thus, it appeared that management did not thoroughly review and question the project, prior to its approval.

Additionally, the project proposal was not verified, as required by NARA 801, to ensure it was adequately supported and the Decide Process was being executed as intended. During the time the WAHS proposal was developed and approved, the position for the NHP Capital Planning Branch (NHPC) Chief was vacant. The NHPC Branch Chief is responsible for documenting, executing, reporting, and managing IT Capital Planning functions as defined in NARA 801. With this position vacant and limited personnel in NHP, management had no assurance that the proposal data was adequately supported and the Decide Process was followed as intended.

Another NARA 801 control not properly followed was the preparation and review of monthly status reports. These reports were prepared by the project manager and were intended to provide information on accomplishments, problems encountered, actions required, schedule, costs, risks, and action items. In addition, these reports should be used to understand the condition of projects and change the course of a project when necessary. However, the monthly reports for the WAHS provided little to no information regarding the project and its status. Further, problems, such as missed deadlines, additional risk factors, extra project spending, were not always identified or corrected during the review of these reports.

By not following NARA 801 requirements, the WAHS was not adequately planned causing the project to fall behind schedule and waste limited resources. Since the approved project proposal becomes the Product Plan, the deficiencies in the proposal were carried forward to the Project Plan and the project quickly fell behind schedule. Originally, the WAHS was to be deployed by September 2008; however, this deadline was not met due to additional technical requirements associated with the Novell Identify

Management (IDM) drivers that were not identified during project planning. This also led to the break-fix[7] which was discovered during the production testing.

By not meeting the deployment deadline, the WAHS wasted limited resources. For example, in April 2008 NARA paid the full yearly maintenance cost of $215,000 for 3,000 RSA tokens; however, only a small portion (approximately 50) of these tokens were distributed and used as part of user testing. In June 2009, NARA had planned to pay another $235,000 for the renewed maintenance of these tokens even though the system will not be fully deployed until at least December 2009. Since our audit, management has lowered the number of tokens needed to 1,500 decreasing the yearly maintenance cost to $143,100.

Furthermore, by not following established requirements, alternatives were not completely vetted prior to the approval of the WAHS. The impact of not fully vetting significant enterprise architecture, information technology infrastructure and applications developments can be profound. Specifically, NARA may not have chosen the best option and limited resources could have been put to better use. One of the discounted alternatives would have met the requirements of HSPD-12, but was not chosen because it would have taken longer to implement. Instead, the selected alternative, which does not meet HSPD-12 requirements and was only supposed to cost $500,000, has now expended over $1.23 million and still is not operational.

Recommendation 4

We recommend the CIO ensure that the deficiencies noted in the project plan are corrected.

Recommendation 5

We recommend the CIO reevaluate the WAHS to ensure it is the best alternative to provide remote access with two-factor authentication.

Recommendation 6

We recommend the CIO enhance the controls in the IT Investment Management Process. With the issuance of the new NARA 801, we recommend the CIO specify who is responsible for verification activities in the IT Investment Management Process and controls to correct unfulfilled business requirements and variances in costs and schedule.

Management Comment(s)

Management concurred with recommendations.

---

[7] A break-fix occurs when a supporting technology fails in the normal course of its function and needs intervention by some support organization.

Major Technical Challenges Remain

Even though the WAHS reached the deployment stage, major technical challenges remained to efficiently and effectively meet all OMB and NIST requirements. This occurred because the WAHS requirements were not adequately defined prior to the development of the WAHS. ---------- Redacted pursuant to FOIA Exemption "high" b(2)----------.

In addition to requiring two-factor authentication, OMB memorandum M-06-16 required agencies to take additional actions for the protection of PII, including:

- Implement NIST Special Publication 800-53 security controls requiring authenticated virtual private network (VPN) connection for remote access to PII.
- Implement NIST Special Publication 800-53 security controls ensuring that information is transported only in encrypted form for instances where PII is transported to a remote site.

Since the NARANet contains PII and other proprietary information, these requirements should have been met by the WAHS, by requiring an authenticated VPN connection and ensuring information is transported in an encrypted form. The specific intent of these requirements is to compensate for the physical security controls not present when sensitive information is removed or accessed from outside of the agency location. -------- ---------- Redacted pursuant to FOIA Exemption "high" b(2)---------- ---------- ---------- ----------.

While the WAHS was designed to meet the OMB two-factor authentication requirement, we found major technical challenges remain for the WAHS to efficiently and effectively meet all OMB and NIST security requirements for remote access. Specifically, the WAHS has not fully demonstrated how it will meet the requirements associated with VPN connections, encryption, monitoring and reviewing remote access connections, and token distribution.

VPN Connection

At the time of our audit, questions remained in whether the VPN connection for the WAHS would meet all security requirements. The WAHS included two separate types of remote access for NARA users. One type provided remote access to virtualized applications[8] with selected functionalities of NARANet, including access to email, shared

[8] Virtualized applications provide remote users controlled access to selected applications and data. When a remote user logs into the remote access system, they are presented with the same desktop setup they normally see on their office computer thereby creating a virtual office desktop. The server "virtualizes" the desktop by passing only screen pixels, keystrokes, and mouse movements over the wire to the remote computer instead of the actual data itself. The process is transparent to end users and their experience is the same as if they were using desktop applications locally on their computer.

and personal drives, and Microsoft Office applications. The other was to provide Secure Sockets Layer[9] (SSL) VPN capability to selected remote users. The initial design intended to only provide this secure VPN connection to certain users to perform system administration functions remotely. Later, it was decided to extend this VPN capability to additional WAHS users, who needed to access systems beyond email, shared and personal drives, and Microsoft Office applications. However, these users had to use a NARA-issued laptop, even though this was not specified in the original requirements for the WAHS. NARA has over 2,700 employees who are eligible to work from home and it may not be efficient and is an undetermined cost to require each of these employees to use a NARA-issued laptop for remote access, especially considering most do not work from home on a regular basis.

Further, management had not yet determined what interrogation factor should be used to verify if a NARA furnished laptop is connecting to the Access Gateway to allow VPN connectivity. An interrogation factor allows for the WAHS to establish an authenticated connection, as required by NIST. However, a determination had not been made as to what attribute would be common to all versions of the NARA baseline image, yet unique to NARA computers for authentication. Also, even though the WAHS had reached the deployment phase, the VPN capability had not been tested by a group of users. Therefore, NARA lacked assurance that the WAHS would meet the security requirements for VPN connections.

Encryption

For instances where PII is transported to a remote site, agencies were to implement security controls ensuring information is transported only in encrypted form. These controls included the use of a validated cryptography.[10] NIST provides standards that should be used by Federal organizations when implementing cryptographic-based security systems to protect sensitive or valuable data. These standards are documented in Federal Information Processing Standards Publication (FIPS PUB 140-2), *Security Requirements for Cryptographic Modules* and are applicable to all Federal agencies that use cryptographic-based security systems. In addition, NIST requires organizations to authorize, monitor, and control all methods of remote access to the information system. Specifically, organizations should employ automated mechanisms to facilitate the monitoring and control of remote access methods; use cryptography to protect the confidentiality and integrity of remote access sessions; and control all remote accesses through a limited number of managed access control points.

However, it is uncertain whether the WAHS will meet each of these requirements. Specifically, procedures have not been put in place to monitor the effectiveness of installed encryption technologies. Also, at the time of the audit, a decision had not been

[9] Secure Sockets Layer (SSL), is a cryptographic protocol that provides secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging, and other data transfers.

[10] Cryptography deals with the transformation of ordinary text (plaintext) into coded form (ciphertext) by encryption and transformation of ciphertext into plaintext by decryption.

made on how to recognize an approved NARA laptop or user and an unapproved NARA laptop or user. Further, in order for encryption to be successful, both ends of the connection must be determined to be secure. However, NARA had not developed a way to validate that a secure internet browser was being used by the remote user. These encryption technologies and controls provide agencies with a method of protecting sensitive information and can reduce the occurrence of data breaches.

Token Distribution

At the time of our audit, the WAHS did not have any procedures in place to manage, assign, distribute, and revoke RSA tokens for users. NIST requires that the organization manages information system authenticators (tokens) by establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators. These procedures need to be established prior to the WAHS being rolled out enterprise wide. Of particular importance are the responsibilities of managing the tokens at the NARA field offices. If not properly accounted for, these tokens could end up in the hands of someone who is not authorized to access the WAHS.

Other Security Concerns

During the audit, we noted that a point of entry into NARANet was established for contractors to remotely manage one of the WAHS servers. NIST requires organizations to authorize, monitor, and control any remotely executed maintenance and diagnostic activities. However, controls still needed to be established for this connection. Originally, the system design did not include a firewall to protect NARANet, but a firewall was later added. The connection was not identified or detailed in the Security Plan and records were not maintained for all remote maintenance and diagnostic activities, as required by NIST. In addition, a SAS 70[11] audit had not been completed for the contractor. The SAS 70 audit process includes an in-depth audit examination of the effectiveness of a service organization's internal controls. Benefits of a SAS 70 audit include the following:

- Assurance that internal controls within the data center are in place, are suitably designed, and are operating effectively;
- Assurance that physical access, IT infrastructure, data and network are secured against certain threats; and
- Assurance that the data center's control policies and procedures have been evaluated and reviewed by an independent third party.

The OMB and NIST requirements were not met because system requirements were not adequately defined prior to the start of the project. The Design Specification listed the appropriate NIST controls that were applicable to the WAHS. However, plans were not completed to discuss how each of these controls would be addressed and implemented.

[11] Statement on Auditing Standards No. 70, Service Organizations, can be helpful in examining the quality of a potential business partner's information security controls.

For example, the Concept of Operations states the system shall exchange all data using an encrypted link, but did not discus how these would be accomplished. The technical aspects of the WAHS were not fully developed prior to the approval and development of the project.

---------- Redacted pursuant to FOIA Exemption "high" b(2)----------
---

---.

Recommendation 7

We recommend the CIO ensure the WAHS meets OMB and NIST requirements prior to full implementation.

Management Comment(s)

Management concurred with recommendation.

National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

Date: September 25, 2009

To: OIG

From: NH

Subject: Comments on OIG Draft Report 09-15,
Audit of NARA's Work-At-Home System

Thank you for the opportunity to comment on this draft report. We concur with the recommendations in the draft report and will proceed with an action plan to address them once we have received the final report.

Martha Morphy

MARTHA MORPHY
Assistant Archivist for Information Services