NATIONAL ARCHIVES

OFFICE *of* INSPECTOR GENERAL

Date : January 31, 2011

Reply to Attn of : Office of Inspector General (OIG)

Subject : Audit Memorandum No. 11-09: Follow-up of NARA's Work at Home System (WAHS)

To : David S. Ferriero, Archivist of the United States

In 2010, the OIG initiated follow up audit work to the previously issued Audit of NARA's Work at Home System[1] (WAHS). We initiated this work as a result of concerns regarding the number of RSA tokens[2] managed and paid for by the National Archives and Records Administration (NARA). Specifically, in the previous audit, we found NARA paid a yearly maintenance cost of $215,000 for 3,000 RSA tokens in April 2008; even though only a significantly small portion, approximately 50 tokens, were distributed and being used as part of the user testing. Then, in June 2009 NARA planned to pay another $235,000 for the renewed maintenance of these 3,000 tokens, despite that the system would not be fully deployed until at least December 2009. Recognizing that 3,000 tokens may not be needed, management lowered the number of tokens to 1,500, decreasing the yearly maintenance cost to $143,100.

Given these and other concerns in NARA's management and monitoring of the RSA tokens, we sought to determine whether the RSA tokens were fully utilized; whether terminated employees were still assigned tokens for remote access; and whether token holders were susceptible to social engineering. To meet these objectives, we examined applicable laws, regulations, and NARA guidance; met with the Office of Information Services (NH) officials; compared a list of current token holders with a list of former NARA employees; and analyzed applicable contract documentation. In addition, we conducted random phone surveys with a sample of token holders.

[1] Audit of NARA's Work-at-Home System (OIG Audit Report No. 09-15) issued September 29, 2009.

[2] RSA tokens are the hardware devices used by NARA to provide two-factor authentication for remote access to meet the requirements outlined in the Office of Management and Budget (OMB) memorandum M-06-16, *Protection of Sensitive Agency Information*. This token provides a random numeric code that is used in conjunction with the user's identification and password.

Initially, we found weaknesses in NARA's management of RSA tokens. However, due to higher audit priorities, our audit work was placed on hold and in the interim, improvements were made in the management of these tokens. For example, in March 2010, we found that only 726 of the 1,500 tokens had been distributed to users of the WAHS. However, after the initial implementation of two-factor authentication[3] on NARA web mail in April 2010, more NARANet[4] users began to request RSA tokens. In fact, additional RSA tokens needed to be purchased to fulfill these requests. Thus in May 2010, NARA increased the number of tokens provided by the contractor from 1,500 to 2,250, resulting in a total annual cost of $155,142 from June 2010 to July 2011. As of January 2011, 1,791 tokens of the 2,250 have been distributed to NARANet users. The remaining tokens (approximately 450 or 20%) are in inventory for new user requests and replacement of lost or stolen tokens.

Also, in March 2010, we identified seven former NARA employees who were still assigned RSA tokens. Accounts for these terminated employees should have been disabled or removed to prevent their access to NARA's information resources. We later found that these seven former employees were no longer assigned tokens. Further, from a sample of lost or stolen tokens, we found that such tokens had been disabled. Improvements in NARA's account management and inventory of RSA tokens may have aided in identifying and disabling these accounts.

The National Institute of Standards and Technology (NIST) requires organizations to establish administrative procedures for information system authentications, such as tokens. These procedures should cover processes for revoking authenticators. NARA's Exit Clearance Procedures have incorporated the deactivation of RSA tokens. Specifically, the Exit Clearance forms include the return of RSA tokens and the termination of remote access to NARANet, if applicable. Tokens and remote access accounts for terminated employees should continue to be disabled or removed in a timely manner. Otherwise, former employees who continue to have remote access to critical or sensitive resources could pose a major threat to the agency, as would individuals who may have left under unfavorable circumstances.

Finally, during phone surveys with token holders in March and April 2010, we used social engineering techniques[5] to try to obtain users' personal identification numbers (PINs). User created PINs, in combination with the number displayed on the users' RSA tokens, are needed to access the WAHS. During our phone surveys, we were able to get one token holder to divulge her PIN and another would have given her PIN, but stated it was written down at home and she could not remember it. Both NIST and the Government Accountability Office (GAO) stress the importance of safeguarding passwords and authenticators, such as RSA tokens. Token holders need to be sufficiently informed of their responsibility in safeguarding their PINs and RSA tokens. Disclosure of sensitive information, such as PINs, could be used to gain unauthorized access to NARA systems, which could lead to identity theft and loss of sensitive information.

---

[3] Two-factor authentication is a system wherein two different factors are used to authenticate a person's identity. Using two factors as oppose to one delivers a higher level of authentication assurance.

[4] NARANet is NARA's private, secure, internal network that supports all intra-NARA network communications. This includes workstations, account management, hardware, and software.

[5] Social engineering is the act of manipulating people into performing actions or divulging confidential information.

In response to our efforts, NH was made aware of our attempts to obtain token holder PINs and other information. Subsequently, NARANet Services sent out a warning email on April 7, 2010 to all NARANet Users. This email instructed users if they received a call from someone conducting a survey about token use or from anyone asking to validate their PIN over the phone, to contact the help desk and report the incident. The email did include specific contact information for the NARANet help desk; however, the email did not instruct or educate employees to never disclose sensitive information, such as their PIN over the phone. An email such as this could have provided NARA officials with an extra opportunity to remind NARA employees of the importance of protecting sensitive information.

Both NIST and GAO emphasize that users should be aware of their responsibility in taking reasonable measures to safeguard passwords and authentications, such as tokens. Typical means for establishing and maintaining security awareness include comprehensive security orientation and refresher programs, which help to communicate security guidelines to new and existing employees and contractors. Also, agencies can require users to periodically sign a statement acknowledging their awareness and acceptance of responsibility for securing devices and following all organization policies, including maintaining confidentiality of passwords.

Social engineering was addressed in NARA's 2010 Annual Security Refresher Training for NARANet. This training defined social engineering, discussed its threats, and provided an example of a telephone conversation leading to the disclosure of a user's network password. Since this training is a yearly requirement, it was not provided to token holders until August 2010, four months after our phone surveys. More frequent reminders may be needed to prevent token holders from disclosing sensitive information. Without adequate training and continuous reminders, users are susceptible to divulging sensitive information over the phone to an unknown source.

Currently, NARA does not require token holders to sign an acknowledgement statement for the security and protection of their token and remote access. Instead, when users pick up their tokens, they are required to sign NARA Form 6032, *Pick-up and Delivery Receipt*, to indicate they have received their token. This is a general equipment form and does not address the user's responsibility or accountability for the device. The latest Federal Information System Management Act (FISMA) reporting guidance[6] encourages the use of remote access user agreements and rules of behavior. These statements would require users to sign a statement acknowledging their awareness and acceptance of responsibility for security.

Our audit work began in March 2010 and was completed in January 2011. Fieldwork was performed at Archives II in College Park, Maryland. We conducted this performance audit in accordance with generally accepted government audit standards. These 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.

---

[6] OMB Memorandum, M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.

Currently, we are not making any recommendations. However, we suggest NARA continue to monitor the usage of RSA tokens; terminate and collect tokens of former employees; disable lost or stolen tokens; and provide continual reminders of the risks and tactics of social engineering. Also, we encourage NH to consider using acknowledgment statements for token holders to accept the responsibility for security and following all organizational policies for remote access.

Should you have questions regarding this assignment, please contact me at 301-837-1532 or James Springs, Assistant Inspector General for Audit at 301-837-3018.

Paul Brachfeld
Inspector General