



# National Archives and Records Administration

8601 Adelphi Road  
College Park, Maryland 20740-6001

Date : September 4, 2008

Reply to

Attn of : Office of Inspector General (OIG)

Subject : Management Letter No. 08-14, Work-at-Home System Project

To : Martha Morphy, Assistant Archivist for Information  
Services (NH)

The purpose of this management letter is to inform you that the strategy employed in the development of the Work-at-Home System (WAHS) exposes NARA to security vulnerabilities that could result in the compromise of the agency's computer network.

We are currently reviewing project documentation for the Work-at-Home System (WAHS), the objective of which is to enhance NARA's remote access capabilities while satisfying an Office of Management and Budget (OMB) mandate. The WAHS, which consists of several commercial-off-the-shelf (COTS) software packages, will implement an Information Technology (IT) infrastructure system that will 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 include 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<sup>1</sup> as mandated by the OMB Memorandum 06-16, *Protection of Sensitive Agency Information*.

System requirements documentation states that "The system *shall* exchange all data between remote users and NARANET using an encrypted link." However, we noted that system implementation plans call for utilizing a strategy that introduces a security vulnerability into NARANet, the agency's computer network.

Redacted pursuant to FOIA Exemptions b(2) and b(5)

2

5

4

<sup>1</sup> An *authentication factor* is a piece of information and process used to authenticate or verify a person's identity for security purposes. *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.

<sup>2</sup> Redacted pursuant to FOIA Exemption b(2)

<sup>3</sup> Redacted pursuant to FOIA Exemption b(2)

<sup>4</sup> Redacted pursuant to FOIA Exemption b(2)

----- Redacted pursuant to FOIA Exemptions b(2) and b(5)-----

----- Redacted pursuant to FOIA Exemptions b(2) and b(5)-----

5  
----- Redacted pursuant to FOIA Exemptions b(2) and b(5)-----

----- Redacted pursuant to FOIA Exemptions b(2) and b(5)-----  
6  
-----

5  
----- Redacted pursuant to FOIA Exemption b(2)-----

6  
----- Redacted pursuant to FOIA Exemption b(2)-----

7  
----- Redacted pursuant to FOIA Exemption b(2)-----

Using these secure protocols is a critical part of maintaining system integrity. To eliminate the security vulnerabilities associated with --- Redacted, b(5)--- we suggest that NH officials revise their strategy, slow the pace of the project effort, and implement a secure ----- Redacted, b(5)-----

Paul Brachfeld  
Inspector General

cc: N (A. Weinstein)



# National Archives and Records Administration

8601 Adelphi Road  
College Park, Maryland 20740-6001

Date: **SEP 17 2008**

To: Office of Inspector General (OIG)

From: Office of Information Services (NH)

Subject: Management Letter No. 08-14, Work-at-Home Project

In response to your Management Letter, we are writing to clarify possible misunderstandings of the Work-at-Home project (WAHS) technical implementation.

Overall, the Management Letter indicated that the use of LDAP presented security vulnerabilities to NARANet. With security controls in place, we believe the risk estimation was overly stated. Most important, the Management Letter suggestion that the project be delayed has been overtaken by events. The initial test phase has now been completed and the project is moving ahead with secured LDAP (LDAPS) implementation.

We would like to clarify several of the technical statements made in the Management Letter.

1. The Management Letter stated: "...However, we noted that system implementation plans call for utilizing a strategy that introduces a security vulnerability into NARANet, the agency's computer network."

\_\_\_\_\_ b(2) \_\_\_\_\_ . [emphasis ours]."

The \_\_\_\_\_ b(2) \_\_\_\_\_ was in fact encrypted.

\_\_\_\_\_ b(2) \_\_\_\_\_

2. \_\_\_\_\_ b(2) \_\_\_\_\_


\_\_\_\_\_ This design element was fully accepted in the system security plan, risk assessment and POA&M for the system.

3. The test accounts involved were "dummy" accounts with predefined access privileges to the test system. This is a normal procedure for any system test activity. Additionally, \_\_\_\_\_ b(2) \_\_\_\_\_, and if a third party gained knowledge of or possession of the test user IDs and passwords, the same third party will not be able to gain access to the system because \_\_\_\_\_ b(2) \_\_\_\_\_.

4. The risk of \_\_\_\_\_ b(2) \_\_\_\_\_, and thereby gaining access to network services is mitigated by the nature of the system \_\_\_\_\_ b(2) \_\_\_\_\_.

\_\_\_\_\_ b(2) \_\_\_\_\_  
\_\_\_\_\_. With these characteristics, it is nearly impossible to discover  
and break the \_\_\_\_\_  
\_\_\_\_\_ b(2) \_\_\_\_\_. This risk is a residual risk for  
any system that utilizes a \_\_\_\_\_ b(2) \_\_\_\_\_  
\_\_\_\_\_, and is strongly mitigated by the physical access controls, management controls,  
and technical controls that are in-place for \_\_\_\_\_ b(2) \_\_\_\_\_

If you have any questions about our response or wish to discuss the project further, please  
contact \_\_\_\_\_ b(2) \_\_\_\_\_ or \_\_\_\_\_ b(2) \_\_\_\_\_ can be reached at 301-837-\_\_\_\_ or email at  
\_\_\_\_\_ @nara.gov, and \_\_\_\_\_ can be reached at 301-837-\_\_\_\_ or email at  
\_\_\_\_\_ @nara.gov.

  
MARTHA MORPHY  
Assistant Archivist for Information Services