

**AUDIT OF NARA'S NETWORK INFRASTRUCTURE**

**OIG Report No. 10-07**

**April 28, 2010**

## EXECUTIVE SUMMARY

Networks are collections of interconnected computer systems and devices allowing individuals to share resources, such as computer programs and information. Because sensitive programs and information are stored on or transmitted along networks, effectively securing networks is essential to protecting computing resources and data from unauthorized access, manipulation, and use. Organizations secure their networks, in part, by installing and configuring network devices that permit authorized network service requests, deny unauthorized requests, and limit the services available on the network. Organizations also secure their networks by ensuring appropriate physical and logical access controls are in place to restrict unauthorized access to these network devices.

We audited NARA's network infrastructure to determine whether NARA had effectively implemented appropriate physical security and access controls to protect network resources. In addition, we reviewed whether network components provide adequate network security.

Our review revealed that appropriate physical security and access controls had not been implemented which left network equipment vulnerable to potential compromise, theft, or damage. These weaknesses could jeopardize the availability of NARANet. We also identified several opportunities to improve security and operation of the network. Specifically:

- The Chief Information Officer and her staff were unable to effectively manage and assess the overall network security of NARA's infrastructure because a complete and accurate network diagram was not maintained;
- Improper firewall management and configuration created vulnerabilities in the network and increased the amount of time it takes traffic to pass into the network;
- Firewall log files were not being reviewed to identify inappropriate activity or potential threats;
- Multiple weaknesses in logical access controls increased the risk of unauthorized access to network devices and servers; and
- Additional physical security and environmental controls are needed at NARA Regional Archives, Record Centers, and Presidential Libraries to restrict physical access to computer resources and protect them from intentional or unintentional loss or damage.

This report contains 18 recommendations which, upon implementation, will assist NARA in providing appropriate management and technical controls over the network. In response to a draft of this report, the Assistant Archivist for Information Services concurred with 17 of the 18 recommendations.

## **BACKGROUND**

NARANet is NARA's General Support System that processes, stores and communicates data between NARA employees, vendors, contractors and clients at various NARA locations. According to the current draft version of the System Security Plan for Network Infrastructure, the infrastructure includes but is not limited to firewalls, routers, switches, servers, computers and storage devices used by staff and contractors both internally and remotely. The primary function of NARANet is to facilitate the communication, storage, and processing of agency information for use internally and to provide a completed product and/or service to other Federal agencies and the general public.

NARA's Wide Area Network (WAN) infrastructure connects all NARA Records Centers, Regional Archives, and Presidential Libraries via a Frame Relay Network. This infrastructure integrates and links all locations into one logical NARA Network by providing each site's Local Area Network (LAN) with an integration point to access the WAN. NARA is in the process of replacing the current frame-relay network with a Multi-Protocol Label Switching network.

The Office of Information Services has responsibility for the operation of NARANet as the system owner and is also responsible for security implementation within the system. IT support services are provided by contract. NARA's IT and Telecommunications Support Services (NITTSS) contractor manages and operates NARA's network (NARANet). IT support for the Regional Records Services Facilities and Presidential Libraries are provided by Field Office Systems Administrators (FOSA), who are responsible for providing day-to-day operations and help desk support, systems administration, general maintenance and preventative maintenance support for all systems related to the NARANET environment.

## **PREVIOUS AUDIT REPORTS**

The NARA OIG has issued three reports over the last five years identifying weaknesses related to the network infrastructure. These weaknesses included: a) Lack of firewall policies and procedures and a lack of regular ongoing scanning and testing of NARANet (OIG Report 06-01); b) NARA's controls over system administrator accounts were weak and needed immediate improvement (OIG Report 06-11); and c) unauthorized devices, such as hubs and multifunction copiers were connected to NARANet without approval from the Office of Information Services (OIG Report 07-10).

## **OBJECTIVE, SCOPE, METHODOLOGY**

The objective of our audit was to determine whether NARA had effectively implemented appropriate physical security and access controls to protect network resources. In addition, we were to also review whether network components provide adequate network security.

The audit was conducted at Archives II in College Park, Maryland and selected field offices. To accomplish the audit objectives we interviewed representatives of the Office of Information Services (NH) and IT Support contractors. We reviewed National Institute of Standards and Technology (NIST) Special Publications 800-53 “Recommended Security Controls for Federal Information Systems and Organizations,” Revision 3, August 2009; 800-41 “Guidelines on Firewalls and Firewall Policy,” Revision 1, September 2009; and 800-115 “Technical Guide to Information Security Testing and Assessment,” September 2008. We also reviewed NARA’s IT Security Requirements, version 5.5, May 29, 2009, and NARA IT Security Methodologies for “Access Control,” “Physical and Environmental Protection,” “System and Communication Protection,” and “Identification and Authentication.”

To observe physical security controls protecting network resources we visited five Presidential Libraries – Dwight Eisenhower, Lyndon Johnson, Jimmy Carter, Ronald Reagan, and George Bush; three Record Centers – Washington National Records Center (Suitland, MD), Southeast Region (Ellenwood, GA), and Pacific Region (Riverside, CA); and two Regional Archives facilities – Southeast (Morrow, GA) and Pacific (Laguna Niguel, CA). At each of these facilities we observed the location of network equipment and assessed whether the equipment was adequately protected from interruptions in computer services, physical damage, and theft. For those locations that had a wireless network, we reviewed the controls in place to secure the wireless network. We also visited the data center supporting the Electronic Records Archive (ERA) system located in Rocket Center, W.V. and reviewed physical security and environmental controls over the equipment.

To review access controls in place to protect network resources we reviewed whether system and network administrators were appropriately identified and authenticated. Specifically, we reviewed administrator accounts on the servers located at the field sites we visited. We also reviewed the mechanisms in place used to authenticate to the network routers, switches, and firewalls.

To review the security of network components we attempted to review the placement of routers and switches within the network. Our review in this area was limited by the lack of a complete network drawing. We also reviewed the configuration of the main NARA firewall and determined whether the rulesets were documented. We originally planned to perform vulnerability scans of the network however, NH was unable to provide us with a current listing of IP addresses.

Our audit work was performed between June 2009 and February 2010. 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

### Review of Network Devices

#### **Inaccurate and Incomplete Network Diagram**

The Chief Information Officer (CIO) and her staff were unable to effectively manage and assess the overall network security of NARA's infrastructure. This occurred because a complete and accurate network diagram was not maintained. Specifically, NH officials did not have a process in place to update and maintain an accurate network diagram and believed it was the contractor's responsibility to do so. NIST SP 800-53 requires NARA to maintain a current baseline configuration of NARANet which includes a network topology. By not having a complete network diagram, NH officials are not aware of potential security vulnerabilities that may exist in the network.

Network drawings are important because they show the overall layout of the network infrastructure and where devices are physically located. They also show the relationship and inter-connectivity between devices and where possible intrusive attacks could take place. Therefore, they assist in the management and auditing of the security of the network infrastructure. We requested a current official drawing of the NARANet infrastructure from the Chief Technology Officer (CTO). NH officials provided an "unofficial" topology drawing, stating that the topology was labeled as "unofficial" to distinguish it from nonexistent "official" drawings. In addition, we also obtained a copy of a network infrastructure drawing from the IT Services contractor which illustrated the physical connectivity of the network devices.

We found neither drawing was comprehensive, as all subnets and network equipment were not shown on the diagrams. For example, the connection to NARA's Virtual Private Network (VPN)<sup>1</sup> was not shown on either drawing. The Chief Information Security Officer (CISO) and the CTO believed the VPN switch and gateway for the new remote access system were outside the firewall but could not verify if that was the case. According to NIST SP 800-41, placing the VPN behind the firewall would require VPN traffic to be passed through the firewall while encrypted, preventing the firewall from inspecting the traffic. Additional items not shown on the topology included:

- Connection to the Electronic Records Archive (ERA) system;
- Connection to the Public Access PC's available to researchers;
- Wireless network connections; and
- Location of other firewalls in the internal infrastructure.

We also found the information on the topology drawing was not accurate. For example, the topology identified the webmail and email servers located inside the network. According to NIST SP 800-45, "Guidelines on Electronic Mail Security," locating webmail and email servers inside the network is inadvisable because it exposes internal

---

<sup>1</sup> A Virtual Private Network provides secure network communications across untrusted networks by encrypting traffic.

network components to additional risks. Mail servers are often targets of attackers and once the internal mail server was compromised, the attacker would have access to the internal network. According to the CISO, the webmail server was not located in the internal network, however, the CISO added he would need to check with the IT Services Division (NHT) to make sure his statement was correct.

We identified several potential areas of concern on the network topology:

- NARA uses only one firewall between its internal private network and the outside public network. This solution does not provide redundancy for the network and could affect the availability of NARANet. More reliability could be achieved by implementing high-availability firewalls which allow one firewall to take over for another if the first firewall fails or is taken offline for maintenance. These firewalls are deployed at the same spot in the network topology so that they both have the same external and internal connections.
- NARA allows direct access from another Government agency into the internal network. According to NH officials, the router configuration restricts traffic into the network, however they had not reviewed the router configuration to ensure their assumptions were correct. According to NIST SP 800-41, organizations should use firewalls wherever their internal networks and systems interface with external networks and systems. Placing a firewall between NARA's internal network and the outside agency could prevent unauthorized access to NARA systems and resources and would also log traffic going into and out of our network.
- NARA allows web servers in the Demilitarized Zone (DMZ)<sup>2</sup> to connect directly into the internal network. For example, traffic from the Internet goes into the firewall and is routed to these web servers. Traffic can pass between these web servers and NARA's internal network without first going back through the firewall. According to NIST SP 800-41, all connections from the DMZ to the internal network should go through the firewall so that firewall policies are applied.

NH officials did not have a process in place to update and maintain an accurate network drawing. The network topology we reviewed was created by the previous contractor and has not been updated since the new contractors began managing the network in April 2009. The CISO stated that the network drawings were not updated as often as he would like because he would want the network drawings refreshed every time there was a change in the network such as a new subnet or new device installed.

According to the CISO, the IT Services contractor was responsible for preparing network diagrams however; in reviewing the contract, the CISO found that the contract does not have a schedule for delivering or updating network diagrams on a regular basis. Instead, the CISO stated he would be able to request diagrams and receive them on an ad-hoc

---

<sup>2</sup> The DMZ is a network segment inserted as a "neutral zone" between an organization's private network and the Internet.

basis. According to the CISO, this is acceptable because the cost of maintaining accurate and valid enterprise level diagrams on a continuous basis was not justified by any business need for that level of information. In addition, NH officials believed the high-level topology diagrams were “good enough” for initiating analytical work.

The IT Services contractor created a physical connectivity drawing by hand, logging onto individual devices and using the “show IP route” command. According to the contractor, his drawing was originally created for the network team’s use and not at the request of NH officials. The contractor was not aware of any automated tools at NARA that could be used to create a network diagram even though the Enterprise Architecture lists two tools already in use by NH which could be used to create and maintain network diagrams. The use of automated tools could assist NH in updating and maintaining an accurate topology.

The CISO believed it was possible to maintain network security without accurate network diagrams. We question this assertion because without a current, detailed network topology the CISO lacks critical information necessary to assess the network environment and secure NARA’s IT Infrastructure from potential compromise.

### **Recommendations**

1. The Assistant Archivist for Information Services/CIO should develop a comprehensive topology of the current network environment and maintain the drawing by updating the drawing periodically (i.e. monthly or quarterly).
2. The Assistant Archivist for Information Services/CIO should develop network diagrams for each field office.
3. The Assistant Archivist for Information Services/CIO should assess and document the risks involved with: a) the use of one firewall; b) the direct connection by an external agency into NARA’s internal network; and c) traffic that can pass between a web server and the internal network without first going through the firewall.

### **Management Comments**

The Assistant Archivist for Information Services concurred with the recommendations.

### **Boundary Protection: Firewall Rules and Policy Needs Improvement**

The NARA firewall configuration included numerous unnecessary rules along with two rules which allow all traffic to go through the firewall. This occurred because NH has not created a formal firewall policy to identify the network traffic that needs to pass into and out of NARA's network and did not regularly review the firewall configuration. According to NIST SP 800-41, a firewall policy dictates how firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications, and

content types based on the organization's information security policies. It is important to periodically test to verify that firewall rules are functioning as expected. As a result, NARA's firewall may not have the correct ruleset in place to prevent unauthorized access to its systems and resources. In addition, unnecessary firewall rules in the configuration create latency problems in the network.

Network traffic into and out of NARANet passes through the main NARA firewall. The firewall takes traffic that has not been checked, checks it against the firewall's policy, and then acts accordingly by either passing the traffic along or blocking the traffic.

According to NIST, generally firewalls should block all inbound and outbound traffic that has not been expressly permitted by the firewall policy in order to decrease the risk of an attack and to reduce the volume of traffic carried on the organization's networks. NARA's IT Security Methodology follows this best practice, stating NH shall deny network traffic by default and shall only allow network traffic by exception.

We reviewed the main firewall configuration which defines the rule sets for network traffic and found the "deny all, allow by exception" rule was not always followed. We also identified improvements needed in the configuration of the firewall. Specifically:

- a) The main firewall configuration contained two "permit ip any any" rules on two access control lists which allows all traffic without exception. These statements should not be included in the firewall configuration because they allow all traffic to go through the firewall and do not follow the NARA IT security policy of only permitting traffic by exception.
- b) The configuration for the firewall was almost 50 pages long and contained many unnecessary rules along with text remarks that were not matched with the corresponding rules. According to the Cisco PIX Command Reference Guide, the access lists on the firewall have an implicit deny at the end of the list; so unless explicitly permitted, traffic cannot pass. Instead of using the implicit deny rule, the NARA firewall contained hundreds of rules to deny network traffic to specific IP addresses. Traffic from the outside then has to be checked against each one of these rules to determine if it is a match, increasing the amount of time it takes traffic to pass into the network (if allowed).
- c) The St. Louis firewall configuration did not match the NARA main firewall configuration. As the NARANet failover connection, the St. Louis firewall should have a similar configuration to the NARA main firewall to ensure only traffic permitted is allowed into the network. If a properly configured firewall is not placed at this entry point into NARANet, malicious traffic normally blocked by the main NARA firewall would be able to enter the network. As changes are made to the main firewall configuration, necessary changes should be replicated on the St. Louis firewall.

NH did not regularly review the firewall configuration to uncover rules that were no longer needed or new requirements that needed to be added to the firewall. An NHT official agreed their staff should be periodically reviewing the firewall configuration and stated that in the past it may have been done informally. In addition, NH has not



conducted penetration testing to assess the overall security of their network environment. According to NIST, penetration testing can be used to verify a firewall ruleset is performing as intended. With the award of a new IT Support Services Contract, new network administrators began managing the network devices in April 2009. According to one network administrator, they identified several areas where vulnerabilities existed in the firewall configuration. However, NH had not formally requested a firewall review and the contractor had not submitted any recommendations to make changes to the firewall.

According to NIST SP 800-41, to improve the effectiveness and security of their firewalls, organizations should create rulesets that implement the organization's firewall policy while supporting firewall performance. NARA does not have a formal policy regarding the firewall ruleset and has not documented a list of traffic which should be allowed to pass into and out of the network. We identified confusion between NH offices as to whose responsibility it was to create a firewall policy. Without a firewall policy, network administrators may be unaware of management's expectations for how the firewall should function. To create a ruleset, NARA will need to determine what types of traffic are required, including protocols the firewall may need to use for management purposes.

### **Recommendations**

4. The Assistant Archivist for Information Services/CIO should perform a risk analysis to develop a list of the types of traffic needed by the organization.

### **Management Comments**

The Assistant Archivist for Information Services did not concur with the recommendation, stating they conduct risk assessments system-by-system in the C&A process and do not see a compelling business reason to change this strategy.

### **Audit Response**

According to NIST SP 800-41, before a firewall policy is created, some form of risk analysis should be performed to develop a list of the types of traffic needed by the organization and categorize how they must be secured—including what types of traffic can traverse a firewall under what circumstances. This could be performed as part of the certification and accreditation of NARANet and documented in the system risk assessment. Therefore, the Assistant Archivist for Information Services should reconsider her position on this recommendation.

5. The Assistant Archivist for Information Services/CIO should create a firewall policy to establish rules for inbound and outbound traffic and how the firewall will be managed and updated.

6. The Assistant Archivist for Information Services/CIO should periodically review the firewall configuration and conduct penetration testing at least annually.

7. The Assistant Archivist for Information Services/CIO should review the St. Louis firewall configuration and ensure necessary firewall rules are included.

### **Management Comments**

The Assistant Archivist for Information Services concurred with the recommendations.

### **Firewall Logs Not Reviewed and Assessed**

Firewall log files were not being reviewed to identify potential threats. This occurred because the server on which the logs were recorded was removed in June 2009 to be replaced by a new product however, the CIO has not assigned responsibility for reviewing the logs. According to NIST SP 800-41, firewall logs and alerts should be continuously monitored to identify threats. By not reviewing the firewall logs, NARA may not know if attacks or other inappropriate activity have occurred.

According to NIST SP 800-41, logging is a critical step in preventing and recovering from failures as well as ensuring proper security configurations are set on the firewall. Proper logging can also provide vital information for responding to security incidents. In addition, real-time alerts should be set up to notify administrators when important events such as modifications or disabling of the firewall rules occur on the firewall. Part of managing the firewall involves continuously monitoring the logs and alerts to identify threats.

Previously, NH used a server to store the firewall logs. However, the server was removed from operation in June 2009 and has not been replaced. According to an NHT official, the server was removed due to security vulnerabilities and concerns. Instead of replacing the server, NH officials are in the process of implementing a Security Information Management (SIM)<sup>3</sup> tool which will collate information from multiple network services such as firewalls, network and host based intrusion detection services, web servers, and routers. NH has been in the process of installing the SIM tool for over three years now. While the SIM can accept and store logs, it has not been populated with rules to analyze the data.

We found that while firewall logs are currently being sent to the SIM, responsibility for reviewing these logs and acting on the information has not been assigned. Network administrators stated that they do not have access to the tool and that contractually their responsibility was only to send logs to the server. An NHI official stated that the security support contractor was using the SIM however, the support contractor stated that responsibility for monitoring and reporting information in the SIM has yet to be determined. According to the CISO, firewall logs are currently reviewed on an ad-hoc

---

<sup>3</sup> The SIM tool accepts alert data from devices throughout the network, correlates the data, and can then determine whether several indicators are related. By correlating the data such as system events, anti-virus events, and vulnerability data, the SIM can determine if an attacked system was vulnerable to the attack seen and determine whether the attack succeeded. However, NARA must first develop and implement rules that tell the SIM what to correlate.

basis while the concept of operations outlining roles and responsibilities for the new tool are being developed.

### **Recommendations**

8. The Assistant Archivist for Information Services/CIO should assign responsibility to the appropriate individuals to monitor the firewall log alerts to determine if attacks or inappropriate activity has occurred.
9. The Assistant Archivist for Information Services/CIO should expedite implementation of the SIM tool.

### **Management Comments**

The Assistant Archivist for Information Services concurred with the recommendations.

### **Access Controls**

Access controls provide reasonable assurance that access to computer resources (data, equipment, and facilities) is reasonable and restricted to authorized individuals. The Government Accountability Office (GAO) defines access controls as including both logical and physical controls. Logical access controls require users to authenticate themselves through the use of passwords or other identifiers and limit the files and other resources that authenticated users can access and the actions they can execute. Physical access controls involve restricting physical access to computer resources and protecting them from intentional or unintentional loss or impairment.

### **Logical Access Controls Need to be Strengthened**

We identified several weaknesses in the logical access controls for network infrastructure equipment and selected servers we reviewed. This occurred because adequate controls were not in place and additional oversight over contractor actions was needed. NIST SP 800-53 and NARA's IT Security Methodology require unique identification and authentication when accessing an IT system. Without appropriate controls in place, there is an increased risk of unauthorized access to network devices and servers.

Our review identified the following weaknesses:

- Multifactor authentication was not used for network access to administrator accounts;
- An administrator account belonging to a former contractor was shared by the new network administrators;
- Network device passwords were not changed immediately after a network administrator left; and
- Servers contained anonymous administrator accounts that may be unnecessary.

NIST SP 800-53 requires each individual to be uniquely identified and authenticated when accessing an information system. According to GAO, this occurs through the

implementation of adequate logical access controls. User authentication establishes the validity of a user's claimed identity using mechanisms such as requiring them to provide something they have (such as a smart card); something they alone know (such as a password or personal identification number); or something that physically identifies them uniquely (such as a biometric fingerprint or retina scan). Multifactor authentication is accomplished by using a combination of these mechanisms.

a.) We found that access to infrastructure devices by network administrators did not meet requirements established by NIST. Specifically, NIST SP 800-53, control IA-2 requires the use of multifactor authentication for network access to privileged accounts. NARA's network administrators used the network to manage the routers, switches, and firewalls from the computers at their desks instead of having to physically connect to each device. According to GAO, network access to devices can significantly increase the risk of unauthorized access. Therefore, to increase security, identification and authentication should be accomplished using multifactor authentication such as a smart card in conjunction with a password. NARA's network administrators were authenticated using only passwords, which does not meet the multifactor authentication requirement. In addition, network administrators had the ability to manage the network devices remotely using the Nortel VPN, which does not use multifactor authentication.

b.) We reviewed the TACACS server log for passed authentications and found a userID belonging to a former network administrator had been used to successfully log into NARA devices multiple times over a three month period. Terminated employees who continue to have access to critical or sensitive resources such as firewalls, routers, and switches pose a major threat to the network. We referred this to OIG Investigations as a potential violation of 18 U.S.C. 1030 "Unauthorized Access to Government Computer System." In a meeting with the CISO, the Lead Network Engineer explained that his network team had used this account on several occasions at the start of the new IT Services and Support contract in April 2009. According to the Lead Network Engineer, the previous contractor gave the new contractors the password to his account and the account was only enabled when needed. There were at least four individuals who knew the password to this account.

The use of this account by multiple network administrators was in violation of NARA's IT Security Requirements which does not allow accounts to be used by more than one user. The use of a shared account resulted in a lack of user accountability over the actions performed by the network administrators using this account because it would be impossible to determine the specific individual who performed the actions. The IT Operations Chief stated the account was only used the first week in April; however, we identified several logins that occurred after that time period including two successful logins in May and two in June. The Lead Network Engineer stated the administrator account has now been deleted.

c.) Network device passwords were not changed immediately after a network administrator left. According to the Lead Network Engineer, he was not directed to change the passwords until the week after the previous network administrator's departure

and it took several days to change the passwords on all devices. According to the Standard Operating Procedure, the passwords for system administrators must be changed when a systems administrator leaves the program. However, the procedure states NARA is responsible for submitting a request for administrator passwords to be changed. The IT Operations Chief was not aware of the previous network administrators exact departure date. As a result, there was an increased risk of unauthorized access during that time period.

d.) We reviewed the administrator accounts on selected servers at NARA field sites and found several servers had excessive administrator accounts. For example, a server supporting the VISTA system at a Presidential Library had 12 users in the "Administrators" group on the server. Of the 12 accounts, only three were assigned to specific individuals. Other accounts included a Novell backup account even though this was not a Novell server; two anonymous accounts, the purpose for which no documentation was available; and an anonymous account for the St. Louis Engineers.

The IT Security Methodology for Access Control requires that NARA specifically authorize and monitor the use of anonymous accounts and remove, disable, or otherwise secure unnecessary accounts. All of the Windows servers we reviewed, except for one, had an anonymous administrator account named ~~\_\_\_\_\_~~. According to the NHT Operations Chief, this account was the built-in administrator account that was renamed for security reasons. While this was true for some of the servers we reviewed, we found that the servers for the VISTA system had both the built-in administrator account and the ~~\_\_\_\_\_~~ account. No documentation was available regarding the creation and use of this account. Additional anonymous administrator accounts, which may be unnecessary, were found on the Windows servers. b(2)

NARA did not have adequate controls in place to prevent these weaknesses in logical access controls. NARA's IT Security Methodology for Identification and Authentication has not been updated to reflect the new controls for identification and authentication required by the latest revision to NIST SP 800-53. In addition, NARA's IT Operations staff needs to take a more proactive approach in monitoring actions by the contractor to ensure NARA access control policy is followed. b(2)

### Recommendations

10. The Assistant Archivist for Information Services/CIO should implement multifactor authentication for network access to infrastructure devices and update the IT Security Methodology for Identification and Authentication to reflect new requirements in NIST SP 800-53, Revision 3.

11. The Assistant Archivist for Information Services/CIO should periodically review  
 a) the access list for the central access control (TACACS) server to ensure accounts belonging to terminated staff are secured and b) logs for the central access control server to ensure successful logins belong to current employees or contractors.

12. The Assistant Archivist for Information Services/CIO should develop a process to ensure NHT is alerted to changes in IT contractor staff so that passwords can be changed.

13. The Assistant Archivist for Information Services/CIO should review the administrator accounts on field office servers and delete any unnecessary accounts.

### **Management Comments**

The Assistant Archivist for Information Services concurred with the recommendations.

### **Physical and Environmental Protections at Field Sites Need Improvement**

We visited 10 field sites and the ERA data center to observe the controls in place outside the main NARA data center at AII and found that additional physical security and environmental controls are needed to restrict physical access to computer resources and protect them from intentional or unintentional loss or impairment. According to NARA's IT Security Requirements, NARA must limit physical access to information systems and equipment and protect systems against environmental hazards.

Physical security controls restrict physical access or harm to computer resources and protect these resources from intentional or unintentional loss or impairment. These controls restrict physical access to computer resources, usually by limiting access to the buildings and rooms in which the resources are housed and by periodically reviewing the access granted, in order to ensure that access continues to be appropriate. Physical controls also include environmental controls which prevent or mitigate potential damage to facilities and interruptions in service. Examples of environmental controls include smoke and water detectors, fire alarms and extinguishers, and uninterruptible power supplies.

#### Physical Access Controls to Computer Rooms and Closets

Access to the areas where network equipment was located was not always limited to personnel responsible for equipment administration and maintenance. This occurred because key inventories and reviews of badge reader access had not been conducted annually, as required by the NARA IT Security Methodology for Physical and Environmental Protection. By not limiting access to areas where network equipment is stored, there is an increased risk of theft of network equipment or loss of network availability.

Badge readers were used at four of the facilities we visited to restrict entry of personnel to the computer rooms and closets. However we identified several instances where access was not limited to those personnel responsible for equipment administration and maintenance. For example, at one Presidential Library, over 124 NARA and Library Foundation employees had access to a closet where IT equipment was stored. As a result of our review, the facility manager at that location took immediate action to reduce the number of staff with access to the room. In another example, we reviewed the 273 badges issued at one of NARA's record centers and found the badge belonging to the

former security manager still had access to the server room. In addition, there were four badges not assigned to a specific individual that had access to the server room. As a result of our review, the facility manager took immediate action and deleted access for these five badges.

At six locations visited, key locks were used to restrict access to the computer room. Keys were generally given to the Field Office System Administrator, the facility manager, and top management. However, at one Presidential Library we identified six copies of the master key were unaccounted for. These master keys could be used to open exterior doors as well as the door to the computer room. At another location, one of the three keys to the computer room was unaccounted for.

According to NARA's IT Security Methodology for Physical and Environmental Protection, keys and other access devices controlling entry to facilities containing information systems must be inventoried annually. We found key inventories and reviews of badge reader access were not conducted annually as required. For example, at one site with badge reader access, the facility manager had not considered access to the computer room and closets as part of their review. The facility manager at one location could not provide any evidence that a key inventory had ever been completed. At a third location, the last evidence of a key inventory was from 1994.

### **Recommendation**

14. The Archivist should direct the Assistant Archivist for Information Services/CIO, the Assistant Archivist for Regional Record Services, and the Assistant Archivist for Presidential Libraries to coordinate with the Assistant Archivist for Administration to develop a mechanism to track access reviews and key inventories for computer rooms and other locations where IT network infrastructure equipment is stored at the field sites.

### **Management Comments**

The Assistant Archivist for Information Services concurred with the recommendation.

### Physical Access to Network Equipment and Cables outside the Computer Room

Network equipment and cabling stored outside the computer room was not always protected at the same level as equipment inside the computer room. This occurred because NH did not have the proper controls in place to restrict access to network equipment. NIST SP 800-53 controls require the organization to protect network equipment and cabling within the facility to minimize potential damage and to minimize the opportunity for unauthorized access. Without adequate protection there is a risk network equipment could be stolen or network cables could be tampered with resulting in a loss of network availability.

As part of the audit we reviewed the controls in place to protect network equipment located outside the computer room. We observed that equipment was not always secured to minimize the potential for theft, damage, or unauthorized access. For example, we

observed network equipment stored in a janitorial closet (Figure 1). The rack holding the equipment was not locked; therefore anyone with access to the closet had access to the network equipment.



Figure 1. Network equipment stored in Janitorial Closet

At another location we observed a network switch stored in a lockable rack with the fiber cable and power cord protected by conduit (Figure 2). However, when we first observed the rack, it was unlocked and the door was left open, exposing the network equipment to theft, damage, or tampering. Another switch in the same facility was also stored in an unlocked rack (Figure 3). The key to this rack was initially located on top of the rack and during the site visit the facility manager locked the rack and placed the key on his key ring. In addition to the rack being unlocked, the fiber cable and power cord were not protected and vulnerable to damage or tampering. Both of these examples occurred on a floor accessible to the public. Doors separating the public museum from the employee side where the equipment was located were closed but not locked.



Figure 2. Rack was unlocked



Figure 3. Rack was unlocked and key was located on top of the rack



According to NIST SP 800-53 control PE-4, physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. In addition, control PE-18 requires organizations to position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. Without proper controls in place the confidentiality and availability of NARANet could be impacted.

### **Recommendation**

15. The Assistant Archivist for Information Services/CIO in conjunction with the Assistant Archivist for Regional Record Services and the Assistant Archivist for Presidential Libraries should periodically monitor the network environments at the field sites to ensure network equipment and cables stored outside the computer rooms are protected.

### **Management Comments**

The Assistant Archivist for Information Services concurred with the recommendation.

### Physical and Environmental Hazards to Network Equipment

Network equipment was not always protected from physical and environmental hazards. This occurred because racks were not provided to store the equipment properly. In addition, facilities owned by other Federal agencies required approval before changes could be made. As a result, network equipment could be inadvertently or deliberately misused, damaged, or destroyed.

According to NARA's Physical and Environmental Protection Methodology control PE-18 "Location of Information System Components," NARA positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

In one example, installation of a wall mounted rack with network equipment was not strong enough to hold the rack and a jack stand was needed to support the weight of the cabinet (Figure 4). If the rack was to fall, the network equipment could be damaged or destroyed. In another example, we found some NARA facilities were lacking the proper racks to store the IT equipment. Specifically, we observed a NARANet switch which was placed on a temporary rack until the proper rack could be provided by NH (Figure 5). This places the equipment at an increased risk of damage because the equipment could be inadvertently knocked over.



Figure 4. Jack needed to hold rack in place



Figure 5. Switch on temporary rack

At two facilities a rack was not available to store the PBX telephone equipment (Figures 6 and 7). Without racks to secure the equipment in place there is an increased risk that the equipment could be damaged, resulting in a loss of telephone service.



Figure 6. PBX balanced on top of UPS



Figure 7. PBX not in a rack

We also observed that additional environmental controls were not usually implemented to mitigate the effects of fire, heat, or other natural disasters. None of the facilities we visited had heat or water alarms. For example, at one facility environmental controls had not been implemented to mitigate the affect of a flood even though the facility is located in an area subject to flash flooding. Specifically, network equipment was stored in a room in the basement which did not have a raised floor and water alarms were not used to alert officials to flooding in the room.

We observed at least two NARA facilities had water sprinkler systems in the computer rooms which could cause damage to the equipment if triggered. For example, a data center housing a critical NARA system had a wet pipe sprinkler system. According to NH officials, because the building is owned by another agency, they had to submit a request to replace the wet pipe sprinkler system with a gas system.

Additional environmental hazards we observed included:

- One computer room had exterior windows and was located on the first floor;
- Only two facilities had raised floors in the computer room; and
- Not all facilities had the capability to shut off power to equipment in the computer room during emergency situations.

Without proper environmental controls in place network equipment could be inadvertently damaged or destroyed.

### **Recommendations**

16. The Assistant Archivist for Information Services/CIO in conjunction with the Assistant Archivist for Regional Record Services and the Assistant Archivist for Presidential Libraries should conduct a review to determine which facilities require racks and provide the necessary racks.

17. The Assistant Archivist for Information Services/CIO in conjunction with the Assistant Archivist for Regional Record Services and the Assistant Archivist for Presidential Libraries should perform a risk assessment for each of the field offices to determine whether changes to the buildings are needed in order to properly protect network equipment.

### **Management Comments**

The Assistant Archivist for Information Services concurred with the recommendations.

### Wireless Networks

Three of the sites we visited had a wireless network as part of the local area network; however, NARA officials were not monitoring for unauthorized access to the network. This occurred because NARA had bought the hardware needed for a monitoring tool but had not yet implemented the tool. According to NIST SP 800-53 Control AC-18, the organization is to monitor for unauthorized wireless access. As a result, NARA does not know whether unauthorized users or devices were attempting to access, or had already accessed, the wireless network.

NARA is in the process of deploying wireless networks throughout the regions, including the Presidential Libraries. Three sites we visited had already deployed wireless networks. We found none of the three sites were using AirDefense. For example, at the Bush Library, the FOSA stated that the hardware for AirDefense had been purchased but it had not been installed.

According to NARA's Operations Architecture, AirDefense is a wireless network intrusion detection system that monitors wireless sensors for intrusion attempts coming in from wireless sources. NARA planned to start deploying sensors for the system in 2009, however, according to the CISO, the project team that was responsible for the wireless build-outs did not have the money to include sensor installation in FY 2009. The CISO

stated that a follow-on contract will be needed to install sensors at the existing sites in early FY 2010.

**Recommendations**

18. The Assistant Archivist for Information Services/CIO should monitor for unauthorized wireless access to NARANet.

**Management Comments**

The Assistant Archivist for Information Services concurred with the recommendations.

## Appendix A: Site Visit Results

	Record Centers			Regional Archives		Presidential Libraries					
<b>Physical and Environmental Controls Tested</b>											
Is there a separate computer room at the facility?	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Is a key or access badge needed for entry?	Badge	Key	Key	Key	N/A	Badge	Badge	Key	Key	Key	Badge
Is the room unmarked? (i.e. there should be no visible signs to indicate there is computer equipment in the room)	Y	N	N	N	Y	Y	N	Y	Y	N	Not Reviewed (NR)
Is computer equipment stored outside the main computer facility secured (i.e. stored in a locked rack)?	N	Y	Y	Y	N/A	Y	Y	N	N	N	NR
Are visitors signed in and escorted?	N	N	N	N	N	N	N	N	N	N	Y
Are physical access logs maintained?	N	N	N	N	N	N	N	N	N	N	N
Does the room contain air conditioning?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Is the room a reasonable temperature? (i.e. the room does not seem overly hot or cold, fans are not needed to cool the room)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Does the room contain smoke, heat, and water alarms?	N	N	N	N	N	N	N	N	N	N	N
Are fire extinguishers kept near the equipment?	Y	Y	Y	Y	Y	N	Y	Y	Y	N	NR
Is the equipment free from dust? (i.e. there is no visible dust on the equipment)	Y	Y	Y	Y	Y	Y	Y	Y	Y	NR	Y
Does the facility have an uninterruptible power supply or backup generator installed for the computer equipment?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Are surge protectors used?	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	NR
Does each piece of equipment contain a Blue NARA barcode and/or a Red NARA IT Hardware barcode?	Y	N	N	N	N	N	N	Y	N	N	Y
Is the room housing the PBX equipment locked?	Y	Y	Y	Y	N/A	Y	Y	Y	Y	N	Y

**Attachment 1. Management Comments  
on the Draft Report**



# *National Archives and Records Administration*

8601 Adelphi Road  
College Park, Maryland 20740-6001

Date : APR 21 2010

Reply to

Attn of : Office of Information Services (NH)

Subject : Comments on Draft OIG Audit Report 10-07, Audit of NARA'S Network Infrastructure

To : Office of Inspector General (OIG)

We offer the following comments on the subject draft report of our agency's infrastructure. It is clear from the draft that the auditor spent considerable time developing the findings and recommendations and we commend the draft's coherence, organization, and opportunities for improving our network infrastructure when we implement the recommendations.

## **EXECUTIVE SUMMARY**

In the middle of the first page, the statement is made that the weaknesses found in this audit "could jeopardize the availability of NARANet." Further, the first bulleted statement on the page states: "The Chief Information Officer and her staff were unable to effectively manage and assess the overall network security of NARA's infrastructure because a complete and accurate network diagram was not maintained."

We disagree with both statements. On the diagram issue, there is simply no "one" singular diagram or topology that represents a complete, contemporaneous, and accurate depiction of the entire network. Multiple documents that NH maintains serve this purpose. NH currently maintains, among others, a broad set of network diagrams, including: NARA Network Logical Design, Typical Wireless Pilot Logical Network A, Typical Wireless Pilot Physical Network A, NARA WAN Frame Relay, Novell Groupwise Fully Meshed Network, COOP Disaster Recovery Component Location, St. Louis COOP DR Network Infrastructure, Rocket Center COOP Network Logical Design, NARA Ethernet Tap Deployment, Austin Automation Center v5.5, ERA WAN Network Topology, DREN Connection at A-II, NARA Access to ERA, and ERA WAN RC Physical. Most of these engineering drawings are captured in NARA's Enterprise Architecture Operations Engineering Baseline document, which we are in the process of updating to reflect recent changes such as the recent MPLS network upgrade.

On the CIO managing the overall network security, this assessment is primarily done using monitoring tools that provide real-time and near-real time reporting on threats and vulnerabilities, not diagrams. Those tools are in place as is a POA&M process that provides strong management controls when weaknesses are found in the course of network operations. We assert that diagrams assist planning and change management processes, not day-to-day network security operations.

## **OBJECTIVE, SCOPE, METHODOLOGY**

We disagree with the statement near the end of page three that states “We originally planned to perform vulnerability scans of the network, however; NH was unable to provide us with a current listing of IP addresses.” Vulnerability scans do not rely on having IP addresses. NARA has a published range of IP addresses and the auditor could have effectively performed a scan of this range and made an effective evaluation on the security status of NARA based on the scan. The issue of effectively working with our NH-appointed point of contact for audits applies here; if there was any question of what IP address set the auditor was provided, the NH point of contact could have been contacted to rectify this situation.

## **FINDINGS AND RECOMMENDATIONS**

### **Review of Network Devices**

#### **Inaccurate and Incomplete Network Diagram**

We disagree with several findings in this section, most based on an over reliance on a flawed assumption about the proper use of network diagramming.

- “This occurred because a complete and accurate network diagram was not maintained.”

Updates to network diagrams are on-going, they are not static. While it is theoretically possible to develop drawings that are a “snapshot in time,” changes to networking and engineering diagrams are a dynamic and ongoing process. Further, as before, it is impossible to render on a single diagram the entirety of the NARANet infrastructure. A “full set” provides an accurate and complete picture.

- “Specifically, NH officials did not have a process in place to update and maintain an accurate network diagram and believed it was the contractor’s responsibility to do so.”

And that is the case; NITTSS contractors *do* have this responsibility under the contract. We have advised the contractor about schedule of their schedule of deliverables.

- “By not having a complete network diagram, NH officials are not aware of potential security vulnerabilities that may exist in the network.”

We believe the determination and reliance on a network diagram or topology to determine vulnerabilities is an assumption with limitations. First, any diagram has a potential latency in keeping the document up-to-date with changes. Second, the context of NARA’s “flat” network design, and the limited and centrally controlled external access points, reduces the importance of diagrams in evaluating the risks associated with network interfaces. And the flip side is true as well; simply having a “perfect” network diagram/s does not constitute the broad assumption that NARA does not have security vulnerabilities.



**Recommendations:**

**1. The Assistant Archivist for Information Services/CIO should develop a comprehensive topology of the current network environment and maintain the drawing by updating the drawing periodically (i.e. monthly or quarterly).**

Response: Concur, but these are sets of "diagrams/topologies," and not a single rendering.

**2. The Assistant Archivist for Information Services/CIO should develop network diagrams for each field office.**

Response: Concur.

**3. The Assistant Archivist for Information Services/CIO should assess and document the risks involved with: a) the use of one firewall; b) the direct connection by an external agency into NARA's internal network; and c) traffic that can pass between a web server and the internal network without first going through the firewall.**

Response: Concur.

**Boundary Protection: Firewall Rules and Policy Needs Improvement**

**Recommendations:**

**4. The Assistant Archivist for Information Services/CIO should perform a risk analysis to develop a list of the types of traffic needed by the organization.**

Response: Do not concur. We conduct risk assessments system-by-system in the C&A process and see no compelling business reason to change this strategy.

**5. The Assistant Archivist for Information Services/CIO should create a firewall policy to establish rules for inbound and outbound traffic and how the firewall will be managed and updated.**

Response: Concur.

**6. The Assistant Archivist for Information Services/CIO should periodically review the firewall configuration and conduct penetration testing at least annually.**

Response: Concur.

**7. The Assistant Archivist for Information Services/CIO should review the St. Louis firewall configuration and ensure necessary firewall rules are included.**

Response: Concur.

### **Firewall Logs Not Reviewed and Assessed**

At the bottom of page 8, the draft states in part: "...however, the CIO has not assigned responsibility for reviewing the logs." In the second paragraph on page 9, the draft reads in part: "We found that while firewall logs are currently being sent to the SIM, responsibility for reviewing these logs and acting on the information has not been assigned." These statements are not entirely accurate. Section 7.9 of the NITTSS Performance Work Statement clearly assigns responsibility for reviewing firewall logs to the NITTS contractor. And to facilitate this work the Government has put the NetForensics SIM system in place that consolidates and automates the log analysis function. Basic SIM functionality is now in place and we are working to get more systems reporting to the SIM and placing additional log reviews in place. While we accept the general spirit of the word "expedite," in the recommendation below, we are already using all due diligence to fully implement the SIM.

### **Recommendations:**

**8. The Assistant Archivist for Information Services/CIO should assign responsibility to the appropriate individuals to monitor the firewall log alerts to determine if attacks or inappropriate activity has occurred.**

Response: Concur.

**9. The Assistant Archivist for Information Services/CIO should expedite implementation of the SIM tool.**

Response: Concur.

### **Access Controls**

#### **Logical Access Controls Need to be Strengthened**

### **Recommendations:**

**10. The Assistant Archivist for Information Services/CIO should implement multifactor authentication for network access to infrastructure devices and update the IT Security Methodology for Identification and Authentication to reflect new requirements in NIST SP 800-53.**

Response: Concur to the extent that our actions reflect revision 3 to NIST 800-53.

**11. The Assistant Archivist for Information Services/CIO should periodically review**  
**a) the access list for the central access control server to ensure accounts belonging to terminated staff are secured and b) logs for the central access control server to ensure successful logins belong to current employees or contractors.**

Response: Concur.

**12. The Assistant Archivist for Information Services/CIO should develop a process to ensure NHT is alerted to changes in IT contractor staff so that passwords can be changed.**

Response: Concur.

**13. The Assistant Archivist for Information Services/CIO should review the administrator accounts on field office servers and delete any unnecessary accounts.**

Response: Concur.

### **Physical and Environmental Protections at Field Sites Need Improvement**

We need to point out that many of the issues in the following sections also are the responsibility of other Offices at NARA (particularly NA) to ensure that NARA critical infrastructure components are properly protected and facilities are properly maintained. NH is provided space to operate equipment at these sites and is relying on NA, NL, and NR to ensure adequate security protections based on legal requirements and best business practices. We are working with field offices to properly protect and maintain all our IT assets.

#### Physical Access Controls to Computer Rooms and Closets

##### **Recommendations:**

**14. The Archivist should direct the Assistant Archivist for Regional Record Services the Assistant Archivist for Presidential Libraries, and the Assistant Archivist for Information Services to work with the Space and Security Management Division to develop a mechanism to track access reviews and key inventories at the field sites.**

Response: Concur.

#### Physical Access to Network Equipment and Cables outside the Computer Room

##### **Recommendations:**

**15. The Assistant Archivist for Information Services/CIO in conjunction with the Assistant Archivist for Regional Record Services and the Assistant Archivist for Presidential Libraries should periodically monitor the network environments at the field sites to ensure network equipment and cables stored outside the computer rooms are protected.**

Response: Concur.

Physical and Environmental Hazards to Network Equipment

**Recommendations:**

**16. The Assistant Archivist for Information Services/CIO in conjunction with the Assistant Archivist for Regional Record Services and the Assistant Archivist for Presidential Libraries should conduct a review to determine which facilities require racks and provide the necessary racks.**

Response: Concur.

**17. The Assistant Archivist for Information Services/CIO in conjunction with the Assistant Archivist for Regional Record Services and the Assistant Archivist for Presidential Libraries should perform a risk assessment for each of the field offices to determine whether changes to the buildings are needed in order to properly protect network equipment.**

Response: Concur.

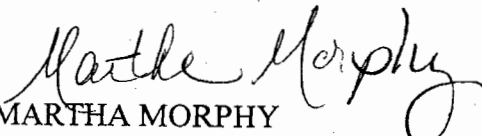
Wireless Networks

**Recommendations:**

**18. The Assistant Archivist for Information Services/CIO should monitor for unauthorized wireless access to NARANet.**

Response: Concur.

If you have any comments or questions, please contact Steve Heaps via email or on 301-837-3170.

  
MARTHA MORPHY  
Assistant Archivist for Information Services