Cotton & Company's Audit of NARA's Enterprise Wireless Access

OIG Audit Report No. 14-10

May 9, 2014

Cotton & Company LLP
635 Slaters Lane
4th Floor
Alexandria, VA 22314

P: 703.836.6701
F: 703.836.0941
www.cottoncpa.com

James Springs
Acting Inspector General
National Archives and Records Administration
8601 Adelphi Rd, Room 1300
College Park, MD 20740

Subject: Audit of the Policies, Implementation, and Security of the National Archives and Records Administration's Wireless Network

Cotton & Company LLP is pleased to submit this independent audit report on the effectiveness of the National Archives and Records Administration (NARA)'s enterprise wireless access. We conducted a review of NARA's information security policies, procedures, and technical controls over wireless access and information technology controls in accordance with the Government Accountability Office (GAO)'s *Government Auditing Standards.* Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We carried out testing during the period from October 1, 2013, through March 21, 2014. We discussed our observations and conclusions with management officials on March 18, 2014, and included their comments where appropriate. We did not audit NARA's responses, and accordingly, we express no opinion on them.

Sincerely,

COTTON & COMPANY LLP

George E. Bills, CPA, CISSP, CISA, CIPP
Partner, Information Assurance

May 9, 2014
Alexandria, Virginia

Table of Contents

Executive Summary

Cotton & Company LLP assisted the National Archives and Records Administration (NARA) Office of Inspector General (OIG) in assessing the extent to which NARA's policies, procedures, and technical controls provide adequate security over its employee and guest wireless networks. The purpose of this engagement was to evaluate NARA's:

1. Wireless network security policies and procedures against NIST guidelines and industry best practices.
2. Wireless network access controls, including the design and implementation of control procedures around centralized access management, authentication, and encryption.
3. Policies and procedures for monitoring wireless usage.
4. Policies and procedures for conducting security and vulnerability assessments of its wireless network environment.
5. Policies and procedures for encrypting and configuring employee and guest access points to its wireless network to deny unauthorized access.

Overall, we determined NARA is not effectively managing their wireless environment to ensure appropriate security controls over wireless are identified, documented, and periodically tested for effectiveness. As a result, we identified weaknesses in each of the areas tested during our review of NARA's information security policies, procedures, and technical controls over its wireless networks and believe management does not have a clear understanding of the current or potential risks related to their use of wireless technology.

We identified a number of wireless security weaknesses that, if exploited, could adversely impact the confidentiality, integrity, and availability of NARA's data and information systems and could ultimately have a negative impact on the agency's ability to protect the security of its information or information systems. These weaknesses include:

- Implementation of the NIST SP 800-37, Revision 1 Risk Management Framework (RMF)
- Implementation of the NIST SP 800-97 Robust Security Network
- Wireless access controls
- Wireless access policies and procedures
- Implementation of configuration settings for wireless information technology products
- Scanning and remediation of wireless network vulnerabilities

A key cause of the weaknesses identified in this report is NARA's lack of implementation of the security assessment and authorization (SA&A) process for their employee and guest wireless environments. Because changes regularly occur within organizations and new security risks are constantly being identified, implementation of the SA&A process (which is addressed at tier 3, *the information system level*, of the RMF) is essential to ensure that systems and data supporting NARA's mission are adequately protected. Diagram 1 shows the formal steps carried out within tier 3 of the RMF. This process helps ensure that important systems are identified and that appropriate security controls are selected, implemented, and regularly assessed to ensure they are working as intended.

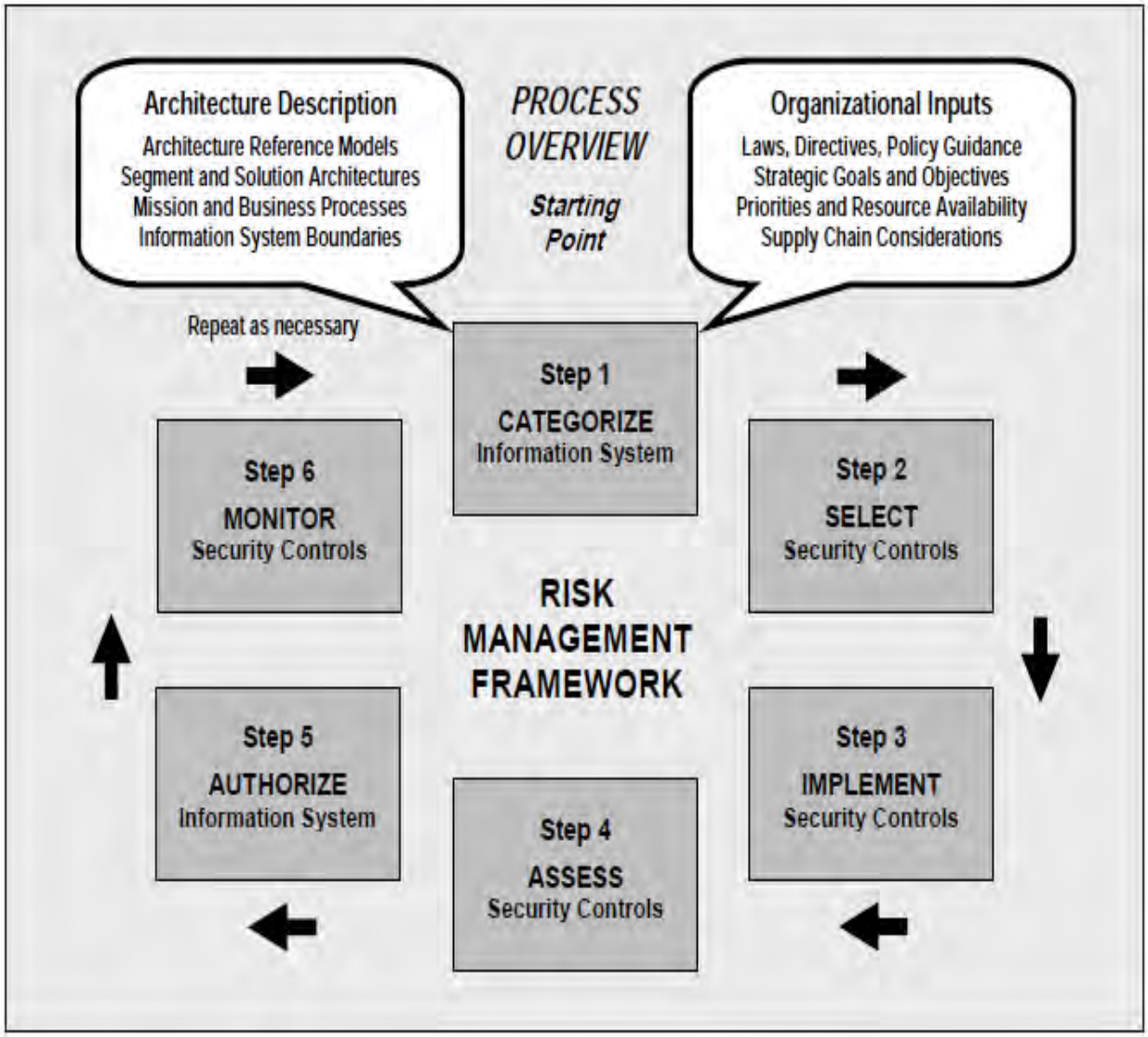

Diagram 1

When implemented, the SA&A helps ensure that management is aware of the risks to their environment, and that the limited resources available are used to protect the systems and data most important to the organization's goals. Further, because this process is intended to be carried out continuously, an SA&A helps ensure that management continues to understand the risks present within their environment and the effectiveness of the controls as changes occur.

We are making five recommendations that we believe, once implemented, will address the weaknesses cited in this review.

Background

NARA has implemented two wireless access networks that were deployed in separate phases: Guest wireless, implemented in FY 2009, and Employee wireless, implemented in FY 2011. The fundamental components of NARA's wireless network are client devices, such as laptops, and access points (APs), which logically connect client devices with NARA's wired network infrastructure.

The Guest wireless network was primarily implemented to offer the public, including guest researchers and those attending special events, internet access while visiting NARA archives and Presidential libraries.

The **Guest wireless network** is in operation at the following 22 sites:

1. Archives I
2. Archives II
3. Archives Boston
4. Archives Kansas City
5. Carter Library
6. Clinton Library
7. Archives New York City
8. GH Bush Library
9. GW Bush Library
10. Eisenhower Library
11. FD Roosevelt Library
12. Ford Library
13. Ford Museum
14. Hoover Library
15. Johnson Library
16. Kansas City Records Center
17. Kennedy Library
18. Archives Atlanta
19. Nixon Library
20. Reagan Library
21. Truman Library
22. Waltham

No encryption or authentication restrictions are in place as this network is considered public access but is also used by NARA Blackberry devices. The Guest wireless network

uses no layer 2 or layer 3 client encryption and is designated for open public access and for NARA Blackberry mail.

Security controls primarily protect the internal NARA network and resources from guest users. This network is open to any users with devices that are capable of connecting to Wi-Fi and that have a capable web browser to accept the NARA terms and conditions. There is no registration or authentication process necessary to connect to this class. To accomplish separation of the employee and guest networks, the following security controls are included in the design of the guest network:

a. The guest WLAN initially appears to be open and broadcasting, allowing guests to easily associate their systems with the network.

b. The guest traffic is sent to an "anchor" controller in a demilitarized zone (DMZ) at Archives II, where the traffic is placed natively into an isolated guest DMZ Virtual Local Access Network (VLAN).

c. The Guest DMZ VLAN is isolated from the internal NARA network by a firewall to prevent guest access to internal NARA resources.

The Employee wireless network was primarily implemented to aid in the process of record keeping and inventorying artifacts at Presidential libraries. Wireless enables records and archival artifacts to be handled less frequently because it is no longer necessary to transport them to and from the areas having directly wired computers. Wireless access also increases the number of staff members that can work with inventory, as access to business applications is not restricted by the number of computers currently installed in the artifact storage areas, or the specific locations of those computers.

The **Employee wireless network** is in operation at the following five sites:

1. GH Bush Library (College Station, TX)
2. Carter Library (Atlanta, GA)
3. Clinton Library (Little Rock, AR)
4. Nixon Library (Yorba Linda, CA)
5. Reagan Library (Simi Valley, CA)

This network is intended to be the more secure of the two wireless networks. Key security settings include:

a. The Employee WLAN does not advertise its Service Set Identifier (**SSID**). It must be known by the person configuring the client interface.

b. Encryption for this network is [redacted].

c. Once authenticated, a networking protocol transfers the connection from the associated access point to the local [redacted].

d. [redacted]

There are two distinct classes of wireless users: (1) NARA Employees, and (2) Guest Researchers.

Wireless User Classes	
User Class	**Class Description**
NARA Employee	This user class is expected to have wireless connectivity to NARANET, with access to NARANET resources that is comparable to a wired connection, as is currently provided for NARA employees and contractors.
Guest Researcher	This user class only provides access to the Internet.

Objectives, Scope, and Methodology

Cotton & Company's objective for this engagement was to assist the NARA Office of Inspector General (OIG) in assessing the extent to which NARA's policies, procedures, and technical controls provide adequate security over its Employee and Guest wireless networks. We conducted our review in accordance with the Government Accountability Office (GAO)'s *Government Auditing Standards.* To meet this objective, we evaluated NARA's:

1. Wireless network security policies and procedures against National Institute of Standards and Technology (NIST) guidelines and industry best practices.

2. Wireless network access controls, including the design and implementation of control procedures around centralized access management, authentication, and encryption.

3. Policies and procedures for monitoring wireless usage.

4. Policies and procedures for conducting security and vulnerability assessments of its wireless network environment.

5. Policies and procedures for encrypting and configuring employee and guest access points to its wireless network to deny unauthorized access.

We conducted our review in three distinct phases: planning, testing, and reporting. During the planning phase, we obtained a high-level understanding of NARA's information technology (IT) policies, procedures, and practices by reviewing available documentation and interviewing key individuals responsible for information security. Based on our understanding of NARA's IT and security controls environment, we designed specific test procedures to assess the effectiveness of wireless and information security controls.

Our test plans tied review objectives to security controls outlined in NIST Special Publication (SP) 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.* NIST SP 800-97, published in February 2007, seeks to assist organizations in understanding, selecting, and implementing technologies based on Institute of Electrical and Electronics Engineers (IEEE) 802.11i, part of the IEEE 802.11 family of wireless networking standards. The document explains at length the security features and capabilities associated with IEEE 802.11i through its framework for Robust Security

Networks (RSN), and provides extensive guidance on the planning and deployment of RSNs. The document also discusses previous IEEE 802.11 security measures and their shortcomings. Furthermore, NIST SP 800-97 establishes the following organization-level recommendations for implementing wireless networks:

- Organizations should ensure that all WLAN components use Federal Information Processing Standards (FIPS)-approved cryptographic algorithms to protect the confidentiality and integrity of WLAN communications.

- Organizations should select IEEE 802.11 RSN authentication methods for their environment carefully.

- Organizations should integrate their existing authentication technology with their IEEE 802.11 RSN WLAN to the extent feasible.

- Organizations should ensure that the confidentiality and integrity of communications between access points and authentication servers are protected sufficiently.

- Organizations establishing IEEE 802.11 RSNs should use technologies that have the appropriate security certification from NIST and interoperability certification from the Wi-Fi Alliance.

- Organizations should ensure that WLAN security considerations are incorporated into each phase of the WLAN life cycle when establishing and maintaining IEEE 802.11 RSNs.

Specifically, section 8 of NIST SP 800-97, *WLAN Security Best Practices*, documents recommendations provided in tables corresponding to the life cycle phases of the WLAN implementation. Each recommendation is accompanied by a brief explanation of the rationale for its inclusion, and is rated as “best practice” or “should consider.” Organizations are strongly encouraged to adopt the “best practice” recommendations. Failure to implement them significantly increases the risk of a WLAN security failure. Organizations should also examine each of the “should consider” recommendations to determine their applicability to the target environment. In general, “should consider” recommendations enhance security beyond what can be achieved through the “best practice” recommendations. A “should consider” recommendation should be rejected only if it is infeasible or if the reduction in risk from its implementation does not justify its cost. For the purposes of this audit, our test plans focused primarily on the “best practice” recommendations.

Our test plans also tied to the review of security controls outlined in NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, and the recommended security assessment procedures outlined in NIST SP 800-53A, Revision 1, *Guide for Assessing the Security Controls of Federal Information Systems and Organizations*. NIST's Computer Security Division (CSD) is charged with developing security standards and providing assistance to federal agencies and the private sector through Title III of the E-Government Act of 2002, entitled *Federal Information Security Management Act of 2002*. NIST carries out a number of efforts under this Act, including:

- Defining minimum information security requirements for information and information systems (SP 800-53)
- Identifying methods for assessing the effectiveness of security requirements (SP 800-53A)
- Providing assistance to agencies and the private sector
- Providing outreach, workshops, and briefings

During testing, we conducted a variety of detailed interviews with NARA personnel, reviewed available supporting documentation, and carried out technical testing on NARA's wireless network.

Audit Results

1. NARA has not applied the Security Assessment and Authorization process to NARA's Guest and Employee wireless networks.

Controls are not adequate to ensure that NARA has performed a Security Assessment and Authorization (SA&A) of the Employee and Guest wireless networks. Specifically, we found the following issues:

1) NARA did not consistently conduct WLAN risk assessments to identify and appropriately mitigate risks associated with implementing both the Guest and Employee wireless networks. Specifically, we noted the following:

   - The Employee wireless network has been operational since 2011; however, NARA has never conducted a risk assessment on this network.

   - NARA conducted wireless risk assessments over the Guest network in 2009 & 2010. These risk assessments were performed at one site (GH Bush and Archives II respectively) and did not consider security control effectiveness at the remaining 21 locations where Guest wireless was implemented. Additionally, NARA has not conducted a risk assessment for the Guest network since 2010.

   - The Guest network risk assessments that NARA conducted in 2009 & 2010 were not conducted in accordance with NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, as the following activities were not performed:

     i. System Characterization
     ii. Threat Identification
     iii. Control Analysis
     iv. Likelihood Determination
     v. Impact Analysis
     vi. Risk Determination
     vii. Control Recommendations

- Due to the lack of risk assessment over the wireless environment, controls are not adequate to ensure that NARA identifies vulnerabilities related to its wireless environment and tracks these vulnerabilities in a Plan of Action and Milestones (POA&M) document.

2) NARA has not maintained an up-to-date and accurate system security plan (SSP) for its Employee and Guest wireless environments that describes the operating environment and the security controls in place. Specifically, we found that the NARA Enterprise Wireless SSP (dated October 18, 2010) provides the planned security mechanisms for the wireless access implementations across NARA, but does not document the currently implemented wireless infrastructure. Through our review of this SSP, we noted that the documentation and network diagrams reflect that the Employee wireless segment was implemented using NIST SP 800-97 best practices, [redacted] This current implementation is not reflected anywhere in the NARA Enterprise Wireless SSP. Additionally, the SSP described a Multimedia Display (MMD) wireless network for multimedia devices to connect to, and we learned that this network was never implemented.

3) NARA's wireless network was not appropriately authorized to operate (ATO) in accordance with NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems.* Specifically, we learned that the wireless network was authorized to operate in November 2012 as part of the NARANET General Support System (GSS). However, in our review of the NARANET GSS SA&A package that was used to ATO NARANET, we noted that no wireless-related controls were documented or tested, and that the NARA Enterprise Wireless SSP contained inaccurate information regarding the design and implementation of wireless access.

The above conditions exist because NARA management did not incorporate the Employee and Guest wireless networks into its existing SA&A process; rather, it included the wireless networks within the NARANET SA&A boundary without considering additional controls specific to wireless. Additionally, due to a lack of funding, the wireless implementation was not carried out as it was initially designed, and

NARA implemented an alternative method without updating the respective wireless network documentation.

Without fully implementing the RMF for the wireless environment, NARA management may not have a clear understanding of risk related to its wireless environment, is increasingly vulnerable to a variety of risks that may not be foreseen or mitigated, and is not able to self-identify and appropriately manage significant weaknesses. Additionally, NARA is not able to take advantage of the benefits that come with the establishment of a well-developed and defined program, such as (1) improved decision-making, (2) risk identification, management, and mitigation, (3) opportunities for process improvement, (4) effective use of budgeted resources, and (5) strategic planning.

The following guidance is relevant to this control activity:

NIST SP 800-37, Revision 1, *Guide to Applying the Risk Management Framework to Federal Information Systems,* section 2.1, *Integrated Organization-Wide Risk Management,* states:

> *The RMF steps include:*
> - ***Categorize** the information system and the information processed, stored, and transmitted by that system based on an impact analysis.*
> - ***Select** an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions*
> - ***Implement** the security controls and describe how the controls are employed within the information system and its environment of operation.*
> - ***Assess** the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.*
> - ***Authorize** information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.*
> - ***Monitor** the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.*

NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i,* states:

> *Executive Summary*
> …
> *Phase 1: Initiation: This phase includes the tasks that an organization should perform before it starts to design its WLAN solution. These include developing a WLAN use*

policy, performing a WLAN risk assessment, and specifying business and functional requirements for the solution, such as mandating RSNAs for all WLAN connections.
…

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* states:

PL-2
Control: The organization:
a. Develops a security plan for the information system that:
- Is consistent with the organization's enterprise architecture;
- Explicitly defines the authorization boundary for the system;
- Describes the operational context of the information system in terms of missions and business processes;
- Provides the security category and impact level of the information system including supporting rationale;
- Describes the operational environment for the information system;
- Describes relationships with or connections to other information systems;
- Provides an overview of the security requirements for the system;
- Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
- Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
b. Reviews the security plan for the information system [Assignment: organization-defined frequency]; and
c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* states:

RA-3
Control: The organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]];
c. Reviews risk assessment results [Assignment: organization-defined frequency]; and
d. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Recommendation 1

We recommend that NARA incorporate the wireless network into its RMF process by performing the following SA&A tasks:

A. ***Categorize*** the network and the information processed, stored, and transmitted by that system based on an impact analysis.

B. ***Select*** an initial set of baseline security controls for the network based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.

C. ***Implement*** the security controls and describe how the controls are employed within the network and its environment of operation.

D. ***Assess*** the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the network.

E. ***Authorize*** network operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.

F. ***Monitor*** the security controls in the network on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

Management Response

Management concurred with the recommendation.

2. NARA has not implemented the Robust Security Network (RSN) for wireless.

Controls are not adequate to ensure that NARA has implemented wireless in accordance with best practices documented in NIST SP 800- 97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*. Specifically, we noted the following:

1) NARA's WLAN is not based on an IEEE 802.11i RSNA using IEEE 801.1A/EAP authentication. Instead, NARA is utilizing [redacted].

2) NARA has not procured products that support the planned EAP methods and has not implemented TLS-based EAP methods; therefore, it is unknown whether NARA's wireless machines can be configured to specify valid authentication servers (AS) by name.

3) [redacted]

4) NARA has not implemented best practices for its current wireless implementation in the most secure fashion. Specifically, the following issues represent present risks and flaws applicable to the current implementation of wireless:

   A. [redacted]

   B. [redacted]

   C. [redacted]

D. [redacted]

E. [redacted]

F. [redacted]

G. [redacted]

H. [redacted]

The above weaknesses exist because NARA did not implement wireless access in accordance with its planned procedures that had been designed to align with NIST SP 800-97 best practices. Additionally, management has not developed or documented an organization-wide wireless access program that documents and describes the wireless access policies, procedures, controls, and implementation methods.

Without implementing NIST SP 800-97 RSN best practices, there is a greater risk that NARA's employee wireless authentication process is susceptible to vulnerabilities [redacted]. Additionally, without documenting and implementing an agency-wide wireless access program, there is an increased risk that wireless controls are not implemented at remote locations in compliance with organization policy, which in turn increases the risk that internal wireless networks are less secure and therefore more susceptible to attack.

The following guidance is relevant to this control activity:

[1] [redacted]

NIST SP 800-97*, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i,* states:

> ***8. WLAN Security Best Practices***
> *To be effective, WLAN security should be incorporated throughout the entire life cycle of WLAN solutions, involving everything from policy to operations… The phases of the life cycle are as follows:*
>
> - ***Phase 1: Initiation**. This phase includes the tasks that an organization should perform before it starts to design its WLAN solution. These include providing an overall vision for how the WLAN would support the mission of the organization, creating a high-level strategy for the WLAN's implementation, developing a WLAN use policy, and specifying business and functional requirements for the solution.*
> - ***Phase 2: Acquisition/Development**. For the purposes of this guide, the Acquisition/Development phase is split into the following two phases:*
>
> ***– Phase 2a: Planning and Design**. In this phase, WLAN network architects specify the technical characteristics of the WLAN solution and related network components. These characteristics include the EAP method or methods used to support authentication; the protocols used to support communication between AP and AS; access control lists and firewall rules to segregate WLAN traffic; and the nature of the supporting PKI. The types of clients to be deployed also need to be considered, since they can affect the desired security policies. There is a wide variety of supplicants that may or may not support desired EAP methods; care must be taken to ensure that the security policy can be employed and enforced by all components (client, AP, and AS). A site survey is typically conducted to help determine the number and placement of access points, as well as how they integrate into the existing network.*
>
> ***– Phase 2b: Procurement**. This phase involves specifying the number and type of WLAN components that must be purchased, the feature sets they must support, and any certifications they must hold.*
>
> - ***Phase 3: Implementation**. In this phase, procured equipment is first configured to meet operational and security requirements, and then installed and activated on a production network. Implementation includes altering the configuration of other security controls and technologies, such as security event logging, network management, AAA server integration, and PKI.*
> - ***Phase 4: Operations/Maintenance**. This phase includes security-related tasks that an organization should perform on an ongoing basis once the WLAN is operational, including log review and rogue AP detection.*
> - ***Phase 5: Disposition**. This phase encompasses tasks that occur after a system or its components have been retired, including preserving information to meet legal requirements, sanitizing media, and disposing of equipment properly.*
>
> ***6.1.3.1 EAP-TLS***
> *EAP-TLS is defined in RFC 2716, which was published in October 1999. EAP-TLS is considered the most secure of the widely supported EAP methods, because it allows strong mutual cryptographic authentication of both STA and AS using public key certificates. It is also favored by high-security environments because it is not a compound method, unlike PEAP or EAP-TTLS, and therefore does not suffer from compound binding problems. To enable mutual authentication, each STA must obtain and host its*

own unique certificate. To provide each STA with its own certificate, organizations should maintain a public key infrastructure (PKI).
…

4.2.1 Pairwise Key Hierarchy
PSK may be generated and installed in any number of ways, including proprietary automated public-key cryptographic approaches, and manual means such as a USB device or a passphrase (which can be converted to a cryptographic key using one of a number of algorithms). If any of the PSKs are compromised, they must be re-distributed in the same way. The security of the WLAN is compromised if any of the PSKs does not possess sufficient cryptographic strength; the passphrase from which the PSK is generated must be a long and complex, possibly randomly generated. The IEEE 802.11 standard does not specify how PSKs are to be generated or distributed, so these decisions are left to implementers. As a result, organizations should review any PSK approach carefully for possible vulnerabilities and evaluate its performance implications. Distributing PSKs in a large network might be infeasible. Due to client software limitations, a common practice is to assign a single PSK per SSID to enable roaming. In such a case, all users can decrypt the traffic of other users, even if the network is protected from outsiders.
…

7.3.3 Modes of Operation
The use of an authentication server rather than pre-shared keys is recommended for most situations because of the impracticality of generating, deploying, and periodically replacing pre-shared keys. The lack of individual user/client authentication in most PSK APs is another reason to avoid the use of pre-shared keys.

NIST SP 800-153*, Guidelines for Securing Wireless Local Area Networks (WLANs),* states:

Executive Summary
Organizations should implement the following guidelines to improve the security of their WLANs:

- *Have standardized security configurations for common WLAN components, such as client devices and APs…*
- *When planning WLAN security, consider the security not only of the WLAN itself, but also how it may affect the security of other networks…*
- *Have policies that clearly state which forms of dual connections are permitted or prohibited for WLAN client devices, and enforce these policies through the appropriate security controls…*
- *Ensure that the organization's WLAN client devices and APs have configurations at all times that are compliant with the organization's WLAN policies…*
- *Perform both attack monitoring and vulnerability monitoring to support WLAN security…*
- *Conduct regular periodic technical security assessments for the organization's WLANs.*

Simple Network Management Protocol (SNMP) v3 Whitepaper (available at http://www.snmp.com/snmpv3/v3white.shtml) states:

> *1.2.3 The SNMPv3 Management Framework*
> …
> *As a result, SNMPv3 is SNMPv2 plus security and administration. The new features of SNMPv3 (in addition to those of SNMPv2 listed above) include:*
>
> - *Security*
> - *Authentication and privacy*
> - *Authorization and access control*
> - *Administrative Framework*
> - *Naming of entities*
> - *People and policies*
> - *Usernames and key management*
> - *Notification destinations*
> - *Proxy relationships*
> - *Remotely configurable via SNMP operations*

Recommendation 2

We recommend that, to the extent possible, NARA revisit the original design documentation of the Employee wireless network and implement RSN best practices for wireless authentication in accordance with NIST SP 800-97. At a minimum, NARA should take appropriate steps to remediate the following issues identified in condition statement #4, which represents the present risks and flaws applicable to the current implementation of wireless:

A. [redacted]

B. [redacted].

C. [redacted].

D. [redacted].

E. [redacted]

F. [redacted]

G. [redacted]

Management Response

Management concurred with the recommendation.

3. NARA did not develop or consistently update wireless policies and procedures.

Controls are not adequate to ensure that policies and procedures related to the use of wireless are reviewed and updated at least annually. Specifically, we found the following:

- During testing we requested documented procedures for gaining access to the wireless network; however, the *Procedures For Connecting Wireless Devices to NARANet* document provided was dated December 2013. The document was not created until after the audit team's request, indicating that the procedures were not previously documented. We also learned that organization-wide access control policies are documented in the *NARA IT Security Methodology for Access Control* document; however, we noted that this document is dated February 2011 and has not been reviewed or updated in nearly three years.
- NARA management has not documented wireless-specific audit logging and monitoring policies or procedures. Additionally, while it appears NARA has identified the events that are being monitored on the wireless network, they are not periodically reviewing and updating the listing of auditable events.

We noted that this weakness exists because NARA is not complying with internal policies that require at least an annual review/update of agency policies and procedures. Additionally, management was following an informal procedure for granting wireless access and had not documented a formal process.

Without formal documentation and continuous review of wireless policies and procedures, there is an increased risk that NARA's existing policies and procedures do not address wireless specific risks and processes, and that wireless processes in place will not be effectively implemented or followed on a consistent basis.

The following guidance is relevant to this control activity:

***NARA IT Security Requirements* states:**

> *AC-1. Access Control Policy and Procedures*
>
> *AC-1. For all data, the NARA Office of Information Services (NH) shall develop, disseminate, and review/update [at least annually]:*
> *AC-1a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among NARA entities, and compliance; and*
> *AC-1b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.*

AU-1. Audit and Accountability Policy and Procedures

AU-1. For all data, the NARA Office of Information Services (NH) shall develop, disseminate, and review/update [at least annually]:
AU-1a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among NARA entities, and compliance; and
AU-1b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* states:

AC-1
Control: The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]:
a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

AU-1
Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined-frequency]:
a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

Recommendation 3

We recommend that NARA develop, document, review, update, and implement wireless policies and procedures on at least an annual basis in accordance with internal NARA and NIST requirements.

Management Response

Management concurred with the recommendation.

4. NARA has not established and documented mandatory configuration settings for wireless information technology products.

Controls are not adequate to ensure that NARA has secured wireless information technology products with the most restrictive settings, in compliance with industry best practices. Specifically, we found that NARA has not developed baseline configurations for its WLC or Wireless Access Points (WAP), does not monitor the WLC or WAP configuration settings, and does not have a process to document and approve deviations from the WLC or WAP-approved configuration settings.

The above weakness exists because NARA has not implemented a secure baseline configuration for all wireless products in accordance with federal regulations and industry best practices.

Without implementing an adequate configuration for wireless IT products, there is an increased risk that the confidentiality, integrity, and availability of the data being processed over the wireless network may be compromised.

The following guidance is relevant to this control activity:

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* states:

> *CM-6 Configuration Settings*
>
> *Control: The organization:*
> *a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements;*
> *b. Implements the configuration settings;*
> *c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and*
> *d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures*
>
> *CM-2 Baseline Configuration*
>
> *Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.*
> *(1) The organization reviews and updates the baseline configuration of the information system:*
> *(a) [Assignment: organization-defined frequency];*

(b) When required due to [Assignment organization-defined circumstances]; and
(c) As an integral part of information system component installations and upgrades.
(3) The organization retains older versions of baseline configurations as deemed necessary to support rollback.

NIST SP 800-153*, Guidelines for Securing Wireless Local Area Networks (WLANs),* states:

Executive Summary
Organizations should implement the following guidelines to improve the security of their WLANs:

- *Have standardized security configurations for common WLAN components, such as client devices and APs…*
- *When planning WLAN security, consider the security not only of the WLAN itself, but also how it may affect the security of other networks…*
- *Have policies that clearly state which forms of dual connections are permitted or prohibited for WLAN client devices, and enforce these policies through the appropriate security controls…*
- *Ensure that the organization's WLAN client devices and APs have configurations at all times that are compliant with the organization's WLAN policies…*

Recommendation 4

We recommend that NARA:

- Utilize existing WLC and WAP baseline configurations or develop their own baseline configurations.

- Implement a process to monitor the WLC and WAP settings for compliance with the established baseline configurations.

- Document and approve any deviations from the WLC and WAP baseline configurations.

- Maintain older versions of the baseline configurations as necessary.

Management Response

Management concurred with the recommendation.

5. NARA is not scanning for vulnerabilities on the wireless network.

Controls are not adequate to ensure that wireless vulnerabilities are identified, evaluated, and remediated. Specifically, we noted the following:

- NARA is not including the WLC or WAPs in its current vulnerability scans.

- NARA has not implemented a formal process for identifying wireless vulnerabilities. Due to this lack of a formal process, we were unable to determine if NARA's process for remediating these identified vulnerabilities is operating effectively.

Without implementing a process to identify, evaluate, and remediate wireless vulnerabilities, there is an increased risk that NARA is susceptible to attack and exploitation of unknown vulnerabilities.

The following guidance is relevant to this control activity:

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* states:

> *RA-5 Vulnerability Scanning*
>
> *Control: The organization:*
> *a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported;*
> *b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:*
> *- Enumerating platforms, software flaws, and improper configurations;*
> *- Formatting and making transparent, checklists, and test procedures; and*
> *- Measuring vulnerability impact;*
> *c. Analyzes vulnerability scan reports and results from security control assessments;*

d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and
e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

NIST SP 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs),* states:

Executive Summary
Organizations should implement the following guidelines to improve the security of their WLANs:

- *Perform both attack monitoring and vulnerability monitoring to support WLAN security…*
- *Conduct regular periodic technical security assessments for the organization's WLANs.*

Recommendation 5

We recommend that NARA:

- Implement a process to conduct vulnerability scans that identify weaknesses related to NARA's wireless environment.

- Develop procedures to analyze and remediate the vulnerabilities identified.

Management Response

Management concurred with the recommendation.

Appendix A – Acronyms and Abbreviations

AES	Advanced Encryption Standard
CAPWAP	Control and Provisioning of Wireless Access Points
CCMP	Cipher Block Chaining Message Authentication Code Protocol
DMZ	Demilitarized Zone
EAP	Extensible Authentication Protocol
EoIP	Ethernet Over Internet Protocol
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GAO	Government Accountability Office
IEEE	Institute of Electrical and Electronics Engineers
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LWAPP	Lightweight Access Point Protocol
MAC	Media Access Control
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
PEAP	Protected Extensible Authentication Protocol
PKI	Public Key Infrastructure
PMK	Pair-wise Master Key
PSK	Pre-Shared Key
RADIUS	Remote Authentication Dial-In User Service
RMF	Risk Management Framework
RSN	Robust Security Network
SA&A	Security Assessment and Authorization
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
SSP	System Security Plan
STA	Station
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WAP	Wireless Access Point
WLAN	Wireless Local Access Network
WLC	Wireless LAN Controller
WPA2	Wi-Fi Protection Access Version 2

Appendix B - Management's Response to the Report

NATIONAL ARCHIVES

Date: APR 25 2014

To: James Springs, Acting Inspector General

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

Subject: OIG Draft Audit 14-10, Audit of NARA's Enterprise Wireless Access

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

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

DAVID S. FERRIERO
Archivist of the United States

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

Appendix C - Report Distribution List

Archivist of the United States
Deputy Archivist of the United States
Chief Operating Officer
Acting Chief Information Officer
Director, Performance and Accountability