OFFICE of INSPECTOR GENERAL
NATIONAL ARCHIVES and RECORDS ADMINISTRATION
8601 ADELPHI ROAD, ROOM COLLEGE PARK, MD 20740-6001
www.archives.gov

DATE: January 15, 2016

REPLY TO ATTN OF: Office of Inspector General (OIG)

SUBJECT: Audit Report No. 16-02, CliftonLarsonAllen, LLP Audit of NARA's Compliance with FISMA, As Amended

TO: David S. Ferriero, Archivist of the United States (N)

Enclosed for your information is the report prepared by CliftonLarsonAllen, LLP (CLA) for the subject audit. The report contains 20 recommendations. In response to the draft report, you concurred with each of the recommendations. Your comments can be found in full as Appendix II to this report.

In connection with the contract, we reviewed CLA's report and related documentation and inquired of its representatives. CLA is responsible for the attached auditor's report dated January 12, 2016, and the conclusions expressed in the report. However, our review disclosed no instances where CLA did not comply, in all material respects, with Generally Accepted Government Auditing Standards.

In accordance with NARA Directive 1201, Audits of NARA Programs and Operations, section S7.m, your written response, in the form of a management action plan, to the recommendations in this report should be forwarded to our office within 45 days.

As with all OIG products, we will determine what information is publically posted on our website from this audit report. Should you or management have any redactions suggestions based on FOIA exemptions, please submit them to my counsel within one week from the date of this letter. Should we receive no response from you or management by this timeframe, we will interpret that as confirmation NARA does not desire any redactions to the posted report.

We appreciate the cooperation and assistance NARA extended to CLA and my staff during the audit. Should you have any questions concerning the report and recommendations please contact me at 301-837-3000.

James Springs
Inspector General

Attach: Audit Report No. 16-02

Audit of the National Archives and Records Administration
Compliance with the
Federal Information Security Management Act of 2002, As Amended

Fiscal Year 2015

CliftonLarsonAllen LLP
www.claconnect.com

January 12, 2016

Mr. James Springs
Inspector General
National Archives and Records Administration
8601 Adelphi Rd., Suite 1300
College Park, MD. 20740

Dear Mr. Springs:

Enclosed is the final version of the *Audit of the National Archives and Records Administration Fiscal Year 2015 Compliance with the Federal Information Security Management Act of 2002, as Amended*. The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP to conduct the audit.

The audit objective was to determine whether the National Archives and Records Administration (NARA) implemented selected security and privacy controls for selected information systems in support of the Federal Information Security Management Act (FISMA) of 2002[1], as amended[2]. To answer the audit objective, we tested NARA's implementation of selected controls outlined in National Institute of Standards and Technology Special Publication (NIST SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

For this audit we reviewed the following systems: (1) NARA's Badge and Access System (B&A); (2) Expanding NARA Online Services/Holding Management System (ENOS/HMS); (3) NARANet[3] general support system; (4) Order Fulfillment Accounting System (OFAS); (5) Records Center Program Billing System (RCPBS); (6) Researcher Registration System (RRS); (7) NARA Google Apps/Email (GOOGLE); (8) Security Clearance and Tracking System (SCTS); and (9) Document Conversion Utility (DCU). Fieldwork was conducted at NARA's headquarters in College Park, MD, from August 06, 2015, to October 30, 2015.

Our audit was performed in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. 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.

---

[1] Enacted as Title III of the E-Government Act of 2002, Public Law 107-347 (2002). Section 301 of the Act added a new subchapter on information security to the United States Code at 44 U.S.C. 3541-3549.

[2] The Federal Information Security Modernization Act of 2014 – Amends the FISMA Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.

[3] NARA's unclassified computer network that provides access to NARA intranet, e-mail, and the Internet.

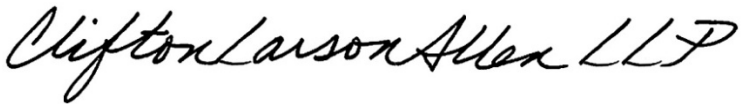
The audit concluded that NARA generally had policies for its information security program, however, its implementation of those policies was not fully effective to preserve the confidentiality, integrity, and availability of the Agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction.

We identified 20 recommendations to help NARA strengthen its information security program. These recommendations include but are not limited to development and updating of policies and procedures, security plans, configuration management and contingency plans, address critical and high risk security weaknesses related to patching and software upgrades, address weaknesses overdue for remediation within plans of actions and milestones, more tightly monitor system account usage, user account recertification reviews and system access approvals.

We very much appreciate the opportunity to serve you and will be pleased to discuss any questions you may have.

Very truly yours,

CLIFTONLARSONALLEN LLP



Calverton, MD
January 12, 2016

Table of Contents

Executive Summary 1
Results 2

Audit Findings 3
1. Risk Assessment Controls Need to be Strengthened 3
2. Security Configuration Baseline Implementation Controls Need to be Strengthened 3
3. Account Management Controls Need to be Strengthened 4
4. Plans of Actions and Milestones Process Needs to be Strengthened 7
5. Controls over System Security Plans Need to be Strengthened 8
6. Security Controls over Patch and Configuration Management Needs to be Strengthened. 9
7. Contracts with External Information System Service Providers Address Security and Privacy Control Requirements Need to be Strengthened 11
8. Controls Surrounding Role-Based Training Need to be Strengthened 12
9. Contingency Planning Controls Need to be Strengthened 13
10. Controls over System Inventory Need to be Strengthened 14
11. Audit Logging Controls Need to be Strengthened 15

Background 17
Federal Information Security Management Act 17
NIST Security Standards and Guidelines 18

Appendix I - Scope and Methodology 19
Appendix II - Management Comments 21
Appendix III - Evaluation of Management Comments 22
Appendix IV - Status of Prior Year Findings 23
Appendix V - Summary of Results of each Control Reviewed 24

Executive Summary

The Federal Information Security Management Act of 2002 (FISMA), as amended[4] requires agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor or source. Because the National Archives and Records Administration (NARA) is a federal agency, it is required to comply with federal information security requirements.

The Act also requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capability is established, and (3) information security management processes are integrated with the agency's strategic and operational planning processes. All agencies must also report annually to the Office of Management and Budget and Congressional committees on the effectiveness of their information security program. In addition, FISMA has established that the standards and guidelines issued by the National Institute of Standards and Technology (NIST) are mandatory for Federal agencies.

The NARA Office of Inspector General engaged us, CliftonLarsonAllen LLP (CLA), to conduct an audit in support of the FISMA requirement for an annual evaluation of NARA's information security program. The objective of this performance audit was to determine whether NARA implemented selected security and privacy controls for selected information systems in support of FISMA and related information security policies, procedures, standards and guidelines.

These objectives included evaluating and reporting on whether a) security programs, plans, policies, and procedures in place were in compliance with applicable federal laws and regulations, b) controls provide reasonable assurance to adequately safeguard and protect sensitive data and ensure that financial data are reliable and complete and provided timely, and c) controls were adequate to prevent or detect unauthorized activities, including external intrusion, theft, or misuse of NARA data, and destruction of NARA hardware, software and data.

Our audit was performed in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. 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.

For this audit, we reviewed the following systems: (1) NARA's Badging and Access System (B&A); (2) Expanding NARA Online Services/Holdings Management System (ENOS/HMS); (3) NARANet General Support System (GSS); (4) Order Fulfillment and Accounting System (OFAS); (5) Records Center Program Billing System (RCPBS); (6) Researcher Registration System (RRS); (7) NARA Google Apps/Email (GOOGLE); (8) Security Clearance and Tracking System (SCTS); and (9) Document Conversion Utility [DCU].

[4] The Federal Information Security Modernization Act of 2014 – Amends the FISMA Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.

Results

The audit concluded that NARA implemented 185 of 282 selected security controls[5] for selected information systems in support of the Federal Information Security Management Act, as amended.

Although NARA generally had policies for its information security program, its implementation of those policies was not fully effective to preserve the confidentiality, integrity, and availability of the Agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, the audit identified the following areas in NARA's information security program where improvements can be made.

- Risk assessment controls (1 control weakness)
- Security configuration baseline implementation controls (1 control weakness)
- Account management controls (6 control weaknesses)
- Plans of action and milestones process (1 control weakness)
- Update of system security plans (3 control weaknesses)
- Security controls surrounding patch and configuration management (2 control weakness).
- Contractual clauses with external information system service providers (1 control weakness)
- Controls over role-based training (1 control weakness)
- Contingency planning controls (4 control weaknesses)
- Controls over system inventory (1 control weakness)
- Controls over audit logging (3 control weaknesses)

Consequently, NARA's operations and assets may be at risk of unauthorized access, misuse and disruption. Comments subsequently provided by NARA's Chief Information Officer (CIO) indicated that although several plans of actions were in place to remediate these weaknesses, which, over time, would allow NARA to better address the reported issues, none of the existing issues could be fixed over night. Additionally, the CIO indicated that these weaknesses represent long-standing issues in NARA's security environment, specifically due to the following:

- inadequate management resources and budget for many years
- lack of effectively implemented processes and procedures
- corrective actions which require long term solutions

We made twenty recommendations to assist NARA in strengthening its information security program. (See pages 3 – 16.)

[5] See Appendix V – Summary of Results of Each Control Reviewed.

Audit Findings

1. Risk Assessment Controls Need to be Strengthened

NARA IT Security Requirements, control RA-3 Risk Assessment, states the following regarding risk assessments:

RA-3. For all data, the NARA IT Security Staff (IT) shall:
RA-3a. Conduct 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;
RA-3b. Document risk assessment results in [a risk assessment report];
RA-3c. Review risk assessment results [SSP-defined frequency for unclassified information systems or at least every 3 years for classified information systems];
RA-3d. Disseminate risk assessment results to [SSP-defined personnel];
RA-3e. Update the risk assessment [SSP-defined frequency for unclassified information systems or at least every 3 years for classified information systems] 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.

NARA had not reviewed the updated Federal Risk and Authorization Management Program (FedRAMP) documentation for Google Apps and SCTS within the past year. This documentation review would include reviewing the updated risk assessment as part of those packages. As these systems are Software as a Service (SaaS) cloud solutions, the majority of security controls are provided by the Cloud Service Provider (CSP). This was due to NARA's lack of formalized procedures. By not properly updating and ensuring the completeness of risk documentation, NARA may have difficulty ensuring that all system risks and great risks to business operations have been identified, addressed, and minimized using adequate and sufficient security controls.

Recommendation #1: We recommend that NARA develop and implement formalized procedures to ensure for those systems utilized by NARA and managed by Cloud Service Providers, controls for which NARA has a shared responsibility should be reviewed on an annual basis, documented and assessed as to the impact to NARA of any risks that may be present.

Management Response: Management concurred with the recommendation.

2. Security Configuration Baseline Implementation Controls Need to be Strengthened

NARA IT Security Requirements, control CM-2 Baseline Configuration, states the following regarding baseline configurations:

CM-2. For all data, the NARA System Owner shall develop, document, and maintain under configuration control, a current baseline configuration of the information system.
CM-2(1) For data requiring moderate or high integrity, the NARA System Owner shall review and update the baseline configuration of the information system:

- [At least annually];

- When required due to [changes to baseline configuration requiring change control approval and at weekly CCB meetings]; and
- As an integral part of information system component installations and upgrades.

System baseline configurations were not formally developed, approved, deployed, and implemented for various operating systems and devices (Solaris 11 platforms and networked printers) to ensure, among other things, vendor default accounts are renamed and vendor default passwords are not used prior to rollout. This occurred because NARA had not followed its CM-2 Baseline Configuration security requirements. The exploitation of inconsistent system security configurations by an attacker could cause a denial of service attack or provide a mechanism to gain unauthorized access to files and data.

Recommendation #2: We recommend that NARA complete the development, approval and deployment of baseline configurations which are currently in progress and ensure that systems are configured in accordance with best practices (including NIST-approved baselines), to include, but not limited to, always changing default credentials at the time of implementation.

Management Response: Management concurred with the recommendation.

3. Account Management Controls Need to be Strengthened

NARA IT Security Requirements, control IA-5 Authenticator Management, states the following regarding user authentication:

IA-5(1) For all data, the information system, shall, for password-based authentication:
(a) Enforces minimum password complexity of [a case sensitive, 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each];

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, states the following regarding account management:

AC-2 ACCOUNT MANAGEMENT
Control: The organization:

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];
b. Assigns account managers for information system accounts;
c. Establishes conditions for group and role membership;
d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;
f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];
g. Monitors the use of information system accounts;

h. Notifies account managers:
    1. When accounts are no longer required;
    2. When users are terminated or transferred; and
    3. When individual information system usage or need-to-know changes;
i. Authorizes access to the information system based on:
    1. A valid access authorization;
    2. Intended system usage; and
    3. Other attributes as required by the organization or associated missions/business functions;
j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

NARA IT Security Requirements, control AC-17 Remote Access, states the following regarding remote access:

> AC-17. For all data, the NARA Office of Information Services (I) shall:
> AC-17a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
> AC-17b. Authorize remote access to the information system prior to allowing such connections.

NARA did not effectively configure password settings, or develop and implement user access administration policies and procedures as follows:

1. NARA did not configure RRS application password settings. Specifically, the maximum password length for RRS application user authentication was limited to 6 characters; however, NARA policy required a minimum length of 8 characters. This occurred because RRS application configuration limitations precluded extending the password length past 6 characters. If password settings are not configured in accordance with NARA policy, there is an increased risk that passwords could be more easily guessed by an attacker to access, modify, add or delete sensitive data.

2. NARA did not develop, effectively update, or implement system-specific user access administration and recertification policies and procedures. This occurred since NARA's overarching IT security requirements for account management were not being consistently followed at the system level. Without formalized access control procedures, there is the risk that detailed processes and procedures related to granting, approving and removing system access could be misinterpreted, misapplied, or not implemented.

   Specifically, we noted the following:
   - Procedures or documentation (access request forms) for establishing, modifying, and approving user accounts to the B&A, RRS, SCTS, DCU, and ENOS/HMS systems were not developed.
   - Users were not recertified on an annual basis for the B&A, ENOS/HMS, RRS, SCTS and DCU systems.
   - There was no process for reissuing shared/group account credentials for B&A and RRS when individuals are removed from the group.

- Policies and procedures titled “NARA IT Security Methodology for Access Control and Identification and Authentication” were not reviewed or updated in FY2015, and last updated in 2011.

3. NARA did not disable or delete inactive NARANet accounts in a timely manner. Specifically, we identified 36 accounts which remained inactive for over 90 days, 11 domain admin accounts were created over a year ago but never used, and 9 accounts were created over 90 days ago but never logged in. Upon notification to management, these accounts were subsequently disabled or deleted. This occurred because NARA did not have an effective process in place to ensure inactive accounts are flagged and investigated for reasonableness during the quarterly account reviews. Without an effective account review process inactive accounts could be accessed by unauthorized users and cause harm to agency resources, including financial data and systems.

4. NARA did not develop policies and procedures for remote access (Virtual Private Network – VPN) or provide evidence of supervisory approval for VPN access for all 22 individuals tested, of 223 total VPN user accounts. This occurred because NARA did not have an effective process in place to ensure documentation of VPN access approvals is maintained. Without formalized remote (VPN) access policies and procedures, there is a risk that unauthorized access may lead to intentional or unintentional harm to system resources.

Recommendation #3: We recommend that NARA configure RRS application password settings in accordance with NARA policy.

Management Response: Management concurred with the recommendation.

Recommendation #4: We recommend that NARA develop, update and implement formalized access control policies and procedures for the B&A, RRS, SCTS and DCU systems.

Management Response: Management concurred with the recommendation.

Recommendation #5: We recommend that NARA implement and document user access reviews for B&A, ENOS/HMS, RRS, SCTS, and DCU.

Management Response: Management concurred with the recommendation.

Recommendation #6: We recommend that NARA develop and implement procedures to reissue shared/group account credentials when individuals are removed from B&A and RRS user groups.

Management Response: Management concurred with the recommendation.

Recommendation #7: We recommend that NARA establish and implement a formalized process for identifying NARANet accounts that are inactive after 90 days and disable if no longer needed.

Management Response: Management concurred with the recommendation.

Recommendation #8: We recommend that NARA develop, update and implement formalized VPN access policies and procedures to ensure individuals are granted appropriated access.

Management Response: Management concurred with the recommendation.

4. The Plans of Actions and Milestones Process Needs to be Strengthened

NARA IT Security Requirements, control CA-5 Plan of Action and Milestones (POA&Ms), states the following regarding Plans of actions and Milestones:

> CA-5. For all data, the NARA System Owner shall:
> CA-5a. Develop a plan of action and milestones for the information system to document the NARA System Owner's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
> CA-5b. The System Owner is responsible for managing the system POA&M which includes ensuring that milestone completion dates are met and any delays or changes in milestones are documented in the system POA&M and communicated to IT.
> CA-5(1) For data deemed by the NARA System Owner to require this additional integrity protection, the NARA System Owner shall employ automated mechanisms to help ensure that the plan of action and milestones for the information system is accurate, up to date, and readily available.

NARA had not closed out POA&Ms in a timely manner for the B&A, ENOH/HMS, RRS, SCTS, NARANet, RCPBS, OFAS and DCU systems. Specifically, multiple high and medium level POA&Ms were identified as still open and overdue one or more years past scheduled completion dates for the following systems:

- *B&A*
  - 17 POA&Ms were still listed as ongoing and overdue.
  - The POAM report was last updated March 30, 2011.
  - POA&Ms were not prioritized and/or did not have information on the point of contact, resources required, and scheduled completion date.
  - B&A was not listed on the NARANet Enterprise POA&M Quarterly Status Report.

- *ENOS/HMS*
  - 8 POA&Ms are ongoing and overdue (1 Medium and 7 High).

- *NARANET*
  - 5 high risk weaknesses were still open more than one year after their due date.
  - 26 POA&Ms were not completed by their scheduled completion date.

- *OFAS*
  - OFAS did not have a POA&M item related to updating its system security plan.

- *RCPBS*
  - 1 POA&M was not completed by its scheduled completion date.

- *RRS*

- 5 POA&Ms were ongoing and overdue (2 Medium and 2 High).
- POA&Ms were not prioritized, and/or did not have information on the point of contact, resources required, and scheduled completion date.

- *SCTS*
  - 5 POA&Ms were ongoing and overdue (4 Medium and 1 High).

- *DCU*
  - 28 POA&Ms were listed as ongoing and overdue (14 Medium and 14 High).
  - POA&Ms did not state resources required and scheduled completion date.

This occurred because NARA had not performed regular reviews and updates of POA&Ms in accordance with IT Security Requirements, to ensure milestone dates are updated as needed, milestone tasks were updated to reflect delays, and completion of milestone items. By not appropriately documenting and tracking IT security weaknesses, NARA may not have a sufficient awareness of potential risks associated with the operation of key financial applications and supporting infrastructure. Incomplete documentation and tracking of IT security weaknesses increases the risk that critical vulnerabilities will not have the appropriate management level exposure and may persist beyond agreed-upon timeframes. Unaddressed IT security weaknesses could also result in compromise of sensitive data and systems.

Recommendation #9: We recommend that NARA establish and implement a formal process to create, assign, track, and remediate identified weaknesses in accordance with NARA-established requirements to:

- Ensure milestone dates are updated as needed if targeted dates are expected to be missed or are overdue, while still documenting original targeted completion dates.
- Investigate and complete actions and milestones to close out overdue POA&M items, specifically items with a medium risk level or higher

Management Response: Management concurred with the recommendations.

5. Controls over System Security Plans Need to be Strengthened

Office of Management and Budget (OMB) Memorandum A-130, 2) System security plans states that “the security plan shall be consistent with guidance issued by the National Institute of Standards and Technology (NIST)."

NARA IT Security Requirements, control CA-3 Information System Connections, states the following regarding system interconnections:

> CA-3. For all data, the NARA Office of Information Services (I) shall:
> CA-3a. Authorize connections from the information system to other information systems through the use of Interconnection Security Agreements; and
> CA-3b. Document, for each connection, the interface characteristics, security requirements, and the nature of the information communicated.

NARA did not finalize system security plans, update in accordance with NIST, or incorporate system interconnections. We noted the following discrepancies with NARA system security plans:

- System security plans were either not finalized (e.g. B&A, SCTS, RCPBS and Google) or lacking current information (e.g. RRS, DCU, ENOS/HMS)
- System security plans included outdated references to NIST 800-53, Revision 3 and were not updated to reflect Revision 4 updates.
- System interconnections were not effectively managed or documented as follows:
  i. System interconnections between NARANet and IBC were not described within the NARANet GSS Infrastructure System Security Plan (SSP).
  ii. Although the DCU SSP listed an interconnection with Veterans Benefit Administration (VBA) this connection is no longer maintained.

This occurred because NARA's process to update security plans was not effective. Without the timely updating of system security plans in accordance with NIST standards and guidelines, NARA systems could be susceptible to new security risks resulting from changes to the environment. Also, if 800-53 Revision 4 controls are implemented without NARA's documentation of these controls, this could potentially create confusion and misapplication of controls.

Recommendation #10: We recommend that NARA implement OMB A-130 and NARA IT Security Requirement which require regular reviews and updates of system security plans and policies and procedures to address NIST 800-53, Revision 4 requirements and address related POA&M milestones.

Management Response: Management concurred with the recommendation.

6. Security Controls over Patch and Configuration Management Needs to be Strengthened

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, states the following regarding flaw remediation and unsupported systems:

SI-2 Flaw Remediation

- that the organization identifies information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures.

SA-22 Unsupported System Components

- that the organization replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.
- Support for information system components includes, for example, software patches, firmware updates, replacement parts, and maintenance contracts. Unsupported components (e.g., when vendors are no longer providing critical software patches), provide a substantial opportunity for adversaries to exploit new weaknesses

discovered in the currently installed components. Exceptions to replacing unsupported system components may include, for example, systems that provide critical mission/business capability where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option.

NIST Special Publication 800-40, Revision 3, *Guide to Enterprise Patch Management Technologies* states the following regarding patch management, "patches are usually the most effective way to mitigate software flaw vulnerabilities, and are often the only fully effective solution. Sometimes there are alternatives to patches, such as temporary workarounds involving software or security control reconfiguration, but these workarounds often negatively impact functionality."

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, states the following regarding configuration management plans:

CM-9 CONFIGURATION MANAGEMENT PLAN

Control: The organization develops, documents, and implements a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;
b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
c. Defines the configuration items for the information system and places the configuration items under configuration management; and
d. Protects the configuration management plan from unauthorized disclosure and modification

NARA did not have an effective process for monitoring, detecting, and remediating known vulnerabilities. Specifically, we found critical and high severity vulnerabilities regarding patches and software updates representing 950 (combined) high and critical risk level vulnerability instances as a result of our scans.

- Of this total, 813 (86%) represented either missing patches [750 (92%)] or unsupported software [63 (8%)].
    - The instances of unsupported software represented installations of the following versions of software which were no longer supported by their vendors (McAfee Agent, Windows Server 2003, Windows XP, Oracle Database, Hypertext PreProcessor (PHP), Unix, and Oracle Application Web Server).

Based upon discussions with NARA management, we determined that for those servers running Windows Server 2003, the migrations to Windows 2008 was ongoing. Extended vendor support for the Microsoft Windows Server 2003 ended on July 14, 2015. Based upon discussions with NARA management and review of configuration documentation, 73 servers were identified as running on Windows Server 2003. A schedule was developed by NARA to track Windows Server 2003 remediation efforts. This schedule also establishes due dates for remediation efforts and provided remediation status for each server. Servers were identified as planned for decommissioning and either to be upgraded or retired. However, the migration and upgrade process has continued beyond the July 14, 2015 end of life support date indicated by Microsoft.

Although management had a patch and vulnerability management program in place, it was not effective to result in the identification and implementation of all needed software patches and upgrades. Although software vendors announce upcoming end of service dates for their products months and sometimes years in advance, NARA was not proactive enough in its efforts to ensure software did not fall out of support. Although NARA planned for the Windows Server operating system migration, these actions did not adequately prepare for the challenges and potential delays associated with the migration of a major operating system on its servers, to ensure the migration was completed prior to the conclusion of vendor support.

Also, NARA did not (1) develop configuration management plans for the B&A, RRS, RCPBS and DCU systems; or (2) review these plans during FY2015 for OFAS and SCTS, ENOH/HMS and NARANet. Additionally, we determined that the policies and procedures titled "NARA IT Security Methodology for Change Management" was not reviewed or updated in FY2015, and last updated in 2011. This occurred because NARA did not have an effective process in place to ensure: (a) policies and procedures are reviewed and updated annually; and (b) configuration management plans are developed and updated on a regular basis. Without formalized change management procedures or system-specific configuration management plans, there is the risk that detailed processes and procedures related to change management could be misinterpreted, misapplied, or not implemented.

Recommendation #11: We recommend that NARA implement improved processes to continuously identify and remediate security deficiencies on NARA's network infrastructure to include enhancing its patch and vulnerability management program to address security deficiencies identified during our assessments of NARA's applications and network infrastructure.

Management Response: Management concurred with the recommendation.

Recommendation #12: We recommend that NARA develop, update and implement configuration management policies and system-specific configuration management plans which were either not developed or out of date.

Management Response: Management concurred with the recommendation.

7. Contracts with External Information System Service Providers Address Security and Privacy Control Requirements Need to be Strengthened

NARA IT Security Requirements, control SA-9 External Information System Services, states the following regarding security requirements for external information system services:

> SA-9. For all data, the NARA System Owner shall:
> SA-9a. Require that providers of external information system services comply with NARA information security requirements and employ [SSP-defined security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
> SA-9b. Define and document government oversight and user roles and responsibilities with regard to external information system services; and
> SA-9c. Employ (SSP-defined processes, methods, and techniques] to monitor security control compliance by external service providers on an ongoing basis.

NARA had not incorporated clauses in agreements between NARA and vendors of contractor hosted systems (e.g. Google and SCTS) requiring these providers to comply with NARA security requirements and employ appropriate security controls which are effectively implemented and compliant with FISMA requirements, OMB policy, and applicable NIST guidelines. This occurred because the agreements were signed prior to the requirement of the clause. Without a clause requiring vendors to adhere to NARA IT Security Requirements, NARA's data and systems are potentially at risk for unauthorized access, deletion, or modification.

Recommendation #13: We recommend that for future agreements, NARA should:

- require that providers of external information system services comply with NARA information security requirements.
- define and document government oversight and user roles and responsibilities with regard to external information systems, and.
- establish a process to monitor security control compliance by external service providers on an ongoing basis.

Management Response: Management concurred with the recommendations.

Recommendation #14: We recommend that NARA add an addendum to current agreements which requires compliance with NARA's information security requirements.

Management Response: Management concurred with the recommendation.

8. Controls Surrounding Role-Based Training Need to be Strengthened

NIST Special Publication 800-53, Revision 4– *Security and Privacy Controls for Federal Information Systems and Organizations*, states the following regarding role-based training:

> AT-3 ROLE-BASED SECURITY TRAINING
> Control: The organization provides role-based security training to personnel with assigned security roles and responsibilities:
> a. Before authorizing access to the information system or performing assigned duties;
> b. When required by information system changes; and
> c. [Assignment: organization-defined frequency] thereafter.

NARA did not provide evidence of role-based training (Tier-II) provided for all 12 individuals sampled with significant security responsibilities (e.g. domain administrators, Novell site administrators, information system owner, etc.) during FY2015. Although NARA had planned in 2014 to implement role-based training in 2015, this did not occur due to other priorities and resource limitations. Without regular role-based training, individuals with security roles and responsibilities may not stay current with threats and vulnerabilities, or be fully cognizant of their security responsibilities.

Recommendation #15: We recommend that NARA develop and implement procedures to ensure all individuals with security roles and responsibilities are provided with adequate security-related technical training specifically tailored for their assigned duties on an annual basis.

Management Response: Management concurred with the recommendation.

9. Contingency Planning Controls Need to be Strengthened

The *NARA IT Security Methodology for Contingency Planning* states the following regarding contingency plan updates:

> The "NARA IT Security Requirements" document contains the requirements for security control [CP-5] for Contingency Plan Update.
> Factors requiring revision of the contingency plan include major changes in locations, key personnel, organization structure, vendor policies, hardware, and software or a reassessment of the BIA. Any resulting updates to the contingency plan should be noted during annual CP reviews or when the system is re-accredited.

The NIST Special Publication 800-53, Revision 4 – *Security and Privacy Controls for Federal Information Systems and Organizations*, states the following regarding contingency plans:

> CP-2 CONTINGENCY PLAN
> Control: The organization:
> a. Develops a contingency plan for the information system that:
> 1. Identifies essential missions and business functions and associated contingency requirements;
> 2. Provides recovery objectives, restoration priorities, and metrics;
> 3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
> 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
> 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
> 6. Is reviewed and approved by [Assignment: organization-defined personnel or roles];
> b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];
> c. Coordinates contingency planning activities with incident handling activities;
> d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency].

NARA had not developed, reviewed on an annual basis, or tested system contingency plans in FY2015, as required by NARA's IT contingency planning policy. Specifically, we noted the following:

- The SCTS contingency plan was not developed.
- The RRS and DCU contingency plans were not updated during FY2015.
- NARA Continuity of Operations Plan (COOP)/Disaster Recovery Infrastructure Specification and Rocket Center Network Design document was last updated in January 2011.
- The Business Impact Analysis (BIA) for OFAS and RCPBS was last updated in 2008.
- The contingency plan for B&A was not completed and still in draft status.

- Testing of contingency plans was not performed during FY2015 for the B&A, (ENOH/HMS), RCPBS, RRS, DCU and SCTS systems.
- Testing of the recovery of tape backups did not occur in FY15 for the B&A, RRS, DCU and SCTS systems.

This occurred because NARA's policies related to reviewing, updating, and testing business continuity and disaster recovery plans on an annual basis was not effectively implemented. Without the regular review and update of contingency plans, there is an increased likelihood that contact information, software and hardware details and restoration procedures may become outdated and not relevant in the event of a disaster. This could create a delay in the timely restoration of critical business functions, systems or processes subsequent to a disaster. Additionally, without regular testing of these plans, there is an increased risk that in the event of a disaster, the execution of defined recovery procedures and steps could fail, resulting in the delay or partial restoration of critical systems and data.

Recommendation #16: We recommend that NARA develop contingency plans and disaster recovery plans for SCTS and B&A, and any other systems identified as critical.

Management Response: Management concurred with the recommendation.

Recommendation #17: We recommend that NARA review and update the RRS, NARA COOP/Disaster Recovery Infrastructure Specification and Rocket Center Network Design document, and DCU contingency plans and disaster recovery plans as necessary, and institute procedures to ensure annual reviews and updates of these documents for these systems and any other systems identified as critical.

Management Response: Management concurred with the recommendation.

Recommendation #18: We recommend that NARA test the B&A, ENOS/HMS, RRS, DCU and SCTS system contingency plans for these and any other systems identified as critical once these documents have been developed and updated; and test tape backup information to verify media reliability and information integrity on a regular basis.

Management Response: Management concurred with the recommendation.

10. Controls over System Inventory Need to be Strengthened

NARA IT Security Requirements, control CM-8 Information System Component Inventory, states the following regarding system inventories:

CM-8. For all data, the NARA System Owner shall:
CM-8a. Develop and document an inventory of information system components that:
1. Accurately reflects the current information system;
2. Includes all components within the authorization boundary of the information system;
3. Is at the level of granularity deemed necessary for tracking and reporting; and
4. Includes [SSP-defined ports, protocols, and services, IP address, FIPS-rating, etc. (including other columns being added to the Master System List]; and

CM-8b. Review and update information system component inventory [at least annually].

NARA's FY2015 information system component inventory indicated that the existence of 170 assets were confirmed during inventory counts more than one year ago and 79 assets had an unverifiable status with no last inventory count date. Thus, the current inventory may not be accurate or complete. This occurred because NARA did not have an effective process in place for conducting the inventory count, which could result in the misuse (e.g. misappropriation of misallocation) of assets.

Recommendation #19: We recommend that NARA establish and document a detailed process to perform a comprehensive annual information system component inventory count.

Management Response: Management concurred with the recommendation.

11. Audit Logging Controls Need to be Strengthened

NARA IT Security Requirements, control AU-2 Auditable Events, states the following regarding auditing:

> AU-2. For all data, the NARA System Owner shall:
> AU-2a. Determine that the information system is capable of auditing the following events:
> 1. Successful and unsuccessful attempts to access, modify, or delete security objects,
> 2. Successful and unsuccessful logon attempts,
> 3. Privileged activities or other system level access,
> 4. Starting and ending time for user access to the system,
> 5. Concurrent logons from different workstations,
> 6. Successful and unsuccessful accesses to objects.
>
> NARA IT Security Requirements, control AU-6 Auditable Events, states the following regarding audit logging:
> AU-6. For all data, the NARA Office of Information Services (I) shall:
> AU-6a. Review and analyze information system audit records [at least on a weekly basis] for indications of [SSP-defined inappropriate or unusual activity];

NARA did not have effective controls over audit logging. Specifically,

- E-Directory user activity on the network (E-Directory is the primary directory service for authentication to NARANet) was not being reviewed for potential security violations. This occurred because although NARA was awaiting the deployment of the IQ Sentinel product to consolidate and integrate all E-Directory logging efforts of user actions on the network, it did not have compensating controls in place.
- NARA did not enable audit logging on the RRS system to capture user activity. This occurred due to limited auditing functionality within RRS.
- NARA did not routinely monitor, review or analyze on a weekly basis, user audit records for the B&A, ENOS-HMS, and DCU systems for indication of inappropriate or unusual activity. This occurred because NARA does not have a process in place to require audit log reviews of these systems.

As a result, NARA may not detect events that could be indicative of security violations in a timely manner, leaving systems open to risks of unauthorized access and alteration of data. Without review of logs, such unauthorized access may go undetected.

Recommendation #20: We recommend that NARA implement the following corrective actions:

- complete efforts to implement the Net IQ Sentinel product
- develop and implement processes and procedures to monitor and at least weekly review user activity and audit logs (in accordance with NARA IT Security Requirements), on the network, RRS, B&A, ENOS-HMS and DCU systems that may indicate potential security violations
- Ensure the procurement of new IT system hardware and software, which provides user authentication, includes a minimum set of audit logging controls and functionality in accordance with NARA's IT Security Requirements, AU-2.

Management Response: Management concurred with the recommendations.

Background

Federal Information Security Management Act

The Federal Information Security Management Act of 2002 (FISMA), as amended, was enacted into law as Title III of the E-Government Act of 2002, Public Law No. 107-347. Key requirements of FISMA include:

- The establishment of an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source;
- An annual independent evaluation of the agency's information security programs and practices; and
- An assessment of compliance with the requirements of the Act.

In addition, FISMA requires Federal agencies to implement the following:

- Periodic risk assessments;
- Information security policies, procedures, standards, and guidelines;
- Delegation of authority to the Chief Information Officer to ensure compliance with policy;
- Security awareness training programs;
- Periodic (annual and more frequent) testing and evaluation of the effectiveness of security policies, procedures, and practices.
- Processes to manage remedial actions for addressing deficiencies;
- Procedures for detecting, reporting, and responding to security incidents;
- Plans to ensure continuity of operations; and
- Annual reporting on the adequacy and effectiveness of the information security program.

The Office of Management and Budget (OMB) has issued executive branch policy for implementing FISMA: Circular No. A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources* (OMB Circular A-130, Appendix III), dated November 28, 2000. This circular establishes a minimum set of controls to be included in Federal agency automated information security programs. In particular Appendix III of OMB Circular A-130 defines adequate security as security commensurate with the risk and magnitude of the harm resulting from loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability through the use of cost-effective management, personnel, operational, and technical controls.

Additionally, OMB has issued guidance related to information security with regard to plans of action and milestones (POA&Ms) for addressing findings from security control assessments, security impact analyses, and continuous monitoring activities. Per OMB Memoranda M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, POA&Ms provide a roadmap for continuous agency security improvement and assisting agency officials with prioritizing corrective action and resource allocation.

Further, OMB is responsible for reporting to Congress a summary of the results of Federal agencies' compliance with FISMA requirements.

NIST Security Standards and Guidelines

FISMA requires the National Institute of Standards and Technology (NIST) to provide standards and guidelines pertaining to federal information systems. Standards prescribed are to include information security standards that provide minimum information security requirements and are otherwise necessary to improve the security of federal information and information systems. FISMA also requires that federal agencies comply with Federal Information Processing Standards (FIPS) issued by NIST. In addition, NIST develops and issues Special Publications (SPs) as recommendations and guidance documents.

FIPS Publication (PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems* (FIPS PUB 200), mandates the use of NIST Special Publication (SP) 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

The purpose of NIST SP 800-53 is to provide guidelines for selecting and specifying security controls for information systems supporting an agency to meet the requirements of FIPS PUB 200. The security controls described in NIST SP 800-53 are organized into 18 families. Each security control family includes security controls associated with the security functionality of the family. In addition, there are three general classes of security controls: management, operational, and technical.

The NIST SP 800-53 security control families are as follows:

Table 1: Security Control Families

Control Class	Security Control Family
Management Controls	Risk Assessment
	Planning
	System and Services Acquisition
	Security Assessment and Authorization
Operational Controls	Personnel Security
	Physical and Environmental Protection
	Contingency Planning
	Configuration Management
	Maintenance
	System and Information Integrity
	Media Protection
	Incident Response
	Awareness and Training
Technical Controls	Identification and Authentication
	Access Control
	Audit and Accountability
	System and Communications Protection

Appendix I - Scope and Methodology

Scope

We conducted this audit in accordance with general accepted government auditing standards, issued as specified in the Government Accountability Office's 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. The audit was designed to determine whether NARA implemented selected security controls for selected information systems in support of the Federal Information security Management Act of 2002, as amended.

The audit included the testing of selected management, technical, and operational controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.* We assessed NARA's performance and compliance with FISMA in the following areas:

- Access Controls
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Program Management
- Risk Assessment
- Planning
- System and Information Integrity
- System and Communication Protection
- System and Services Acquisition

For this audit, we reviewed the NARA's Badging and Access System [B&A], Expanding NARA Online Services/Holding Management System [ENOS/HMS], NARANet general support system, Order Fulfillment Accounting System [OFAS], Records Center Program Billing System [RCPBS], Researcher Registration System (RRS), NARA Google Apps/Email [GOOGLE], Security Clearance and Tracking System [SCTS], and Document Conversion Utility [DCU]. See Appendix V for a listing of selected controls. In addition, the audit included a follow-up on prior year open audit recommendations[6] (to the extent related control areas were tested during the FY2015 FISMA audit) to determine if NARA had made progress in implementing any recommended improvements.

The audit was conducted at NARA's headquarters in College Park, MD, from August 06, 2015 to October 30, 2015.

[6] OIG Report No. 15-01, FY13 *NARA's Information Security Program,* October 27, 2014, and OIG Report No. 08-05, *Audit of NARA's Compliance with the Federal Information Security Management Act for 2007*.

Methodology

Following the framework for minimum security controls in National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, certain controls (listed in Appendix V) were selected from NIST security control families. We reviewed the selected controls over NARA's B&A, ENOS/HMS, NARANet general support system, OFAS, RCPBS, RRS, GOOGLE, SCTS, and DCU.

To accomplish our audit objective we:

- Interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA;
- Reviewed documentation related to NARA's information security program, such as security policies and procedures, system security plans, and security control assessments;
- Tested system processes to determine the adequacy and effectiveness of selected controls (listed in Appendix V);
- Completed a vulnerability assessment of NARA's general support system and evaluated NARAs process for identifying and correcting/mitigating technical vulnerabilities; and
- Reviewed the status of recommendations in the fiscal year 2013 Information Security Program audit report.

In testing for the adequacy and effectiveness of the security controls, we exercised professional judgment in determining the number of items selected for testing and the method used to select them. We considered relative risk, and the significance or criticality of the specific items in achieving the related control objectives. In addition, we considered the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review.

In some cases, this resulted in selecting the entire population. However, in cases that we did not select the entire audit population, the results cannot be projected and if projected may be misleading.

Appendix II - Management Comments

NATIONAL ARCHIVES

Date: JAN 06 2016

To: James Springs, Inspector General

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

Subject: OIG Draft Audit Report 16-02, Audit of NARA's Compliance with the Federal Information Security Management Act of 2002 (FISMA), As Amended

Thank you for the opportunity to provide comments on this draft report. We concur with the 20 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 III - Evaluation of Management Comments

NARA management concurred with all recommendations.

Appendix IV - Status of Prior Year Findings

The following table provides the status of prior FISMA audit recommendations.[7]

No.	OIG Audit Report No.	Audit Recommendation	NARA Status	Auditor's Position on Status
1	15-01	The CIO should develop new policies and procedures or updated existing policies and procedures for at least the 11 program areas included in the annual FISMA review.	Open	Agree, recommendation is still open
2	15-01	The CIO should coordinate with the Office of Performance and Accountability and the Chief Operating Officer (NARA's Risk Officer) to identify, assess, capture, and report IT Security controls within NARA's Internal Control Program Tool in order to adequately ensure safeguarding of assets; efficient and effective operations; reliable and accurate financial data and reporting; and compliance with applicable laws and regulations.	Open	Agree, recommendation is still open

[7] OIG Report No. 15-01, FY13 *NARA's Information Security Program,* October 27, 2014, and OIG Report No. 08-05, *Audit of NARA's Compliance with the Federal Information Security Management Act for 2007*. OIG Report No. 08-05 Recommendations 12, 15b, 16b, 16c, 17, and 20 were incorporated into the recommendations included in this audit report, since related control areas were tested during the FY 2015 FISMA audit.

Appendix V - Summary of Results of each Control Reviewed

Control	Control Name	Is Control Effective?
NARANet		
AC-2	Account Management	No, refer to Finding 3
AC-3	Access Enforcement	Yes
AC-17	Remote Access	No, refer to Finding 3
AT-1	Security Awareness & Training Policy and Procedures	Yes
AT-2	Security Awareness	Yes
AT-3	Security Training	No, refer to Finding 8
AT-4	Security Training Records	No, refer to Finding 8
AU-6	Audit Review, Analysis, and Reporting	No, refer to Finding 11
CA-1	Security Assessment and Authorization Policy & Procedures	Yes
CA-2	Security Assessments	Yes
CA-3	Information System Connections	No, refer to Finding 5
CA-5	Plan of Action and Milestones	No, refer to Finding 4
CA-6	Security Authorization	Yes
CA-7	Continuous Monitoring	Yes
CM-1	Configuration Management Policy and Procedures	No, refer to Finding 6
CM-2	Baseline Configuration	No, refer to Finding 2
CM-3	Configuration Change Control	Yes
CM-6	Configuration Settings	Yes
CM-8	Information System Component Inventory	No, refer to Finding 10
CP-1	Contingency Planning Policy & Procedures	Yes
CP-2	Contingency Plan	No, refer to Finding 9
CP-4	Contingency Plan Testing and Exercises	Yes
CP-6	Alternate Storage Sites	Yes
CP-7	Alternate Processing Sites	Yes
CP-9	Information System Backup	Yes
CP-10	Information System Recovery & Reconstitution	Yes
IA-1	Identification and Authentication Policy and Procedures	Yes
IA-2	Identification and Authentication (Organizational Users)	Yes
IA-3	Device Identification and Authentication	Yes
IA-4	Identifier Management	Yes
IA-5	Authenticator Management	Yes
IR-1	Incident Response Policy and Procedures	Yes
IR-4	Incident Handling	Yes
IR-5	Incident Monitoring	Yes
IR-6	Incident Reporting	Yes
IR-8	Incident Response Plan	Yes
RA-1	Risk Assessment Policy and Procedures	Yes
RA-2	Security Categorization	Yes
RA-3	Risk Assessment	Yes
RA-5	Vulnerability Scanning	No, refer to Finding 6
SA-1	System and Services Acquisition Policy and Procedures	Yes
SA-5	Information System Documentation	Yes
SA-9	External Information Systems	No, refer to Finding 7

Control	Control Name	Is Control Effective?
SC-7	Boundary Protection	Yes
SC-8	Transmission Integrity	Yes
SI-2	Flaw Remediation	No, refer to Finding 6
PL-2	System Security Plan	No, refer to Finding 5
PL-4	Rules of Behavior	Yes
PM-1	Information Security Program Plan	Yes
PM-3	Information Security Resources	Yes
PM-4	Plan of Action and Milestones Process	No, refer to Finding 4
PM-5	Information System Inventory	No, refer to Finding 10
PM-6	Information Security Measures of Performance	Yes
PM-9	Risk Management Strategy	Yes
PM-10	Security Authorization Process	Yes

Control	Control Name	Is Control Effective?
OFAS		
AC-2	Account Management	Yes
AC-3	Access Enforcement	Yes
AU-6	Audit Review, Analysis, and Reporting	Yes
CA-1	Security Assessment and Authorization Policy & Procedures	Yes
CA-2	Security Assessments	Yes
CA-3	Information System Connections	Yes
CA-5	Plan of Action and Milestones	No, refer to Finding 4
CA-6	Security Authorization	Yes
CA-7	Continuous Monitoring	Yes
CM-1	Configuration Management Policy and Procedures	No, refer to Finding 6
CM-2	Baseline Configuration	No, refer to Finding 2
CM-3	Configuration Change Control	Yes
CM-6	Configuration Settings	Yes
CM-8	Information System Component Inventory	No, refer to Finding 10
CP-1	Contingency Planning Policy & Procedures	Yes
CP-2	Contingency Plan	No, refer to Finding 9
CP-4	Contingency Plan Testing and Exercises	Yes
CP-6	Alternate Storage Sites	Yes
CP-9	Information System Backup	Yes
CP-10	Information System Recovery & Reconstitution	Yes
IA-1	Identification and Authentication Policy and Procedures	Yes
IA-2	Identification and Authentication (Organizational Users)	Yes
IA-3	Device Identification and Authentication	Yes
IA-4	Identifier Management	Yes
IA-5	Authenticator Management	Yes
RA-1	Risk Assessment Policy and Procedures	Yes
RA-2	Security Categorization	Yes
RA-3	Risk Assessment	Yes
RA-5	Vulnerability Scanning	No, refer to Finding 6

Control	Control Name	Is Control Effective?
SI-2	Flaw Remediation	No, refer to Finding 6
PL-2	System Security Plan	No, refer to Finding 5
PL-4	Rules of Behavior	Yes

Control	Control Name	Is Control Effective?
RCPBS		
AC-2	Account Management	Yes
AC-3	Access Enforcement	Yes
AU-6	Audit Review, Analysis, and Reporting	Yes
CA-1	Security Assessment and Authorization Policy & Procedures	Yes
CA-2	Security Assessments	Yes
CA-3	Information System Connections	Yes
CA-5	Plan of Action and Milestones	No, refer to Finding 4
CA-6	Security Authorization	Yes
CA-7	Continuous Monitoring	Yes
CM-1	Configuration Management Policy and Procedures	No, refer to Finding 6
CM-2	Baseline Configuration	No, refer to Finding 2
CM-3	Configuration Change Control	Yes
CM-6	Configuration Settings	Yes
CM-8	Information System Component Inventory	No, refer to Finding 10
CP-1	Contingency Planning Policy & Procedures	Yes
CP-2	Contingency Plan	No, refer to Finding 9
CP-4	Contingency Plan Testing and Exercises	No, refer to Finding 9
CP-6	Alternate Storage Sites	Yes
CP-9	Information System Backup	Yes
CP-10	Information System Recovery & Reconstitution	Yes
IA-1	Identification and Authentication Policy and Procedures	Yes
IA-2	Identification and Authentication (Organizational Users)	Yes
IA-3	Device Identification and Authentication	Yes
IA-4	Identifier Management	Yes
IA-5	Authenticator Management	Yes
RA-1	Risk Assessment Policy and Procedures	Yes
RA-2	Security Categorization	Yes
RA-3	Risk Assessment	Yes
RA-5	Vulnerability Scanning	No, refer to Finding 6
SI-2	Flaw Remediation	No, refer to Finding 6
PL-2	System Security Plan	No, refer to Finding 5
PL-4	Rules of Behavior	Yes

Control	Control Name	Is Control Effective?
B&A		
AC-2	Account Management	No, refer to Finding 3
AC-3	Access Enforcement	Yes
AU-6	Audit Review, Analysis, and Reporting	No, refer to Finding 11
CA-1	Security Assessment and Authorization Policy & Procedures	Yes
CA-2	Security Assessments	Yes
CA-3	Information System Connections	Yes

Control	Control Name	Is Control Effective?
CA-5	Plan of Action and Milestones	No, refer to Finding 4
CA-6	Security Authorization	Yes
CA-7	Continuous Monitoring	Yes
CM-1	Configuration Management Policy and Procedures	No, refer to Finding 6
CM-2	Baseline Configuration	No, refer to Finding 2
CM-3	Configuration Change Control	Yes
CM-6	Configuration Settings	Yes
CM-8	Information System Component Inventory	No, refer to Finding 10
CP-1	Contingency Planning Policy & Procedures	Yes
CP-2	Contingency Plan	No, refer to Finding 9
CP-4	Contingency Plan Testing and Exercises	No, refer to Finding 9
CP-6	Alternate Storage Sites	Yes
CP-9	Information System Backup	No, refer to Finding 9
CP-10	Information System Recovery & Reconstitution	Yes
IA-1	Identification and Authentication Policy and Procedures	Yes
IA-2	Identification and Authentication (Organizational Users)	Yes
IA-3	Device Identification and Authentication	Yes
IA-4	Identifier Management	Yes
IA-5	Authenticator Management	Yes
RA-1	Risk Assessment Policy and Procedures	Yes
RA-2	Security Categorization	Yes
RA-3	Risk Assessment	Yes
RA-5	Vulnerability Scanning	No, refer to Finding 6
SI-2	Flaw Remediation	No, refer to Finding 6
PL-2	System Security Plan	No, refer to Finding 5
PL-4	Rules of Behavior	Yes

Control	Control Name	Is Control Effective?
ENOS/HMS		
AC-2	Account Management	No, refer to Finding 3
AC-3	Access Enforcement	Yes
AU-6	Audit Review, Analysis, and Reporting	No, refer to Finding 11
CA-1	Security Assessment and Authorization Policy & Procedures	Yes
CA-2	Security Assessments	Yes
CA-3	Information System Connections	Yes
CA-5	Plan of Action and Milestones	No, refer to Finding 4
CA-6	Security Authorization	Yes
CA-7	Continuous Monitoring	Yes
CM-1	Configuration Management Policy and Procedures	No, refer to Finding 6
CM-2	Baseline Configuration	No, refer to Finding 2
CM-3	Configuration Change Control	Yes
CM-6	Configuration Settings	Yes
CM-8	Information System Component Inventory	No, refer to Finding 10
CP-1	Contingency Planning Policy & Procedures	Yes

Control	Control Name	Is Control Effective?
CP-2	Contingency Plan	No, refer to Finding 9
CP-4	Contingency Plan Testing and Exercises	No, refer to Finding 9
CP-6	Alternate Storage Sites	Yes
CP-9	Information System Backup	No, refer to Finding 9
CP-10	Information System Recovery & Reconstitution	Yes
IA-1	Identification and Authentication Policy and Procedures	Yes
IA-2	Identification and Authentication (Organizational Users)	Yes
IA-3	Device Identification and Authentication	Yes
IA-4	Identifier Management	Yes
IA-5	Authenticator Management	Yes
RA-1	Risk Assessment Policy and Procedures	Yes
RA-2	Security Categorization	Yes
RA-3	Risk Assessment	Yes
RA-5	Vulnerability Scanning	No, refer to Finding 6
SI-2	Flaw Remediation	No, refer to Finding 6
PL-2	System Security Plan	No, refer to Finding 5
PL-4	Rules of Behavior	Yes
RRS		
AC-2	Account Management	No, refer to Finding 3
AC-3	Access Enforcement	Yes
AU-6	Audit Review, Analysis, and Reporting	No, refer to Finding 11
CA-1	Security Assessment and Authorization Policy & Procedures	Yes
CA-2	Security Assessments	Yes
CA-3	Information System Connections	Yes
CA-5	Plan of Action and Milestones	No, refer to Finding 4
CA-6	Security Authorization	Yes
CA-7	Continuous Monitoring	Yes
CM-1	Configuration Management Policy and Procedures	No, refer to Finding 6
CM-2	Baseline Configuration	No, refer to Finding 2
CM-3	Configuration Change Control	Yes
CM-6	Configuration Settings	Yes
CM-8	Information System Component Inventory	No, refer to Finding 10
CP-1	Contingency Planning Policy & Procedures	Yes
CP-2	Contingency Plan	No, refer to Finding 9
CP-4	Contingency Plan Testing and Exercises	No, refer to Finding 9
CP-6	Alternate Storage Sites	Yes
CP-9	Information System Backup	No, refer to Finding 9
CP-10	Information System Recovery & Reconstitution	Yes
IA-1	Identification and Authentication Policy and Procedures	Yes
IA-2	Identification and Authentication (Organizational Users)	Yes
IA-3	Device Identification and Authentication	Yes
IA-4	Identifier Management	Yes
IA-5	Authenticator Management	No, refer to Finding 3
RA-1	Risk Assessment Policy and Procedures	Yes

Control	Control Name	Is Control Effective?
RA-2	Security Categorization	Yes
RA-3	Risk Assessment	Yes
RA-5	Vulnerability Scanning	No, refer to Finding 6
SI-2	Flaw Remediation	No, refer to Finding 6
PL-2	System Security Plan	No, refer to Finding 5
PL-4	Rules of Behavior	Yes

Control	Control Name	Is Control Effective?
DCU		
AC-2	Account Management	No, refer to Finding 3
AC-3	Access Enforcement	Yes
AU-6	Audit Review, Analysis, and Reporting	No, refer to Finding 11
CA-1	Security Assessment and Authorization Policy & Procedures	Yes
CA-2	Security Assessments	Yes
CA-3	Information System Connections	Yes
CA-5	Plan of Action and Milestones	No, refer to Finding 4
CA-6	Security Authorization	Yes
CA-7	Continuous Monitoring	Yes
CM-1	Configuration Management Policy and Procedures	No, refer to Finding 6
CM-2	Baseline Configuration	No, refer to Finding 2
CM-3	Configuration Change Control	Yes
CM-6	Configuration Settings	Yes
CM-8	Information System Component Inventory	No, refer to Finding 10
CP-1	Contingency Planning Policy & Procedures	Yes
CP-2	Contingency Plan	No, refer to Finding 9
CP-4	Contingency Plan Testing and Exercises	No, refer to Finding 9
CP-6	Alternate Storage Sites	Yes
CP-9	Information System Backup	No, refer to Finding 9
CP-10	Information System Recovery & Reconstitution	Yes
IA-1	Identification and Authentication Policy and Procedures	Yes
IA-2	Identification and Authentication (Organizational Users)	Yes
IA-3	Device Identification and Authentication	Yes
IA-4	Identifier Management	Yes
IA-5	Authenticator Management	Yes
RA-1	Risk Assessment Policy and Procedures	Yes
RA-2	Security Categorization	Yes
RA-3	Risk Assessment	Yes
RA-5	Vulnerability Scanning	No, refer to Finding 6
SI-2	Flaw Remediation	No, refer to Finding 6
PL-2	System Security Plan	No, refer to Finding 5
PL-4	Rules of Behavior	Yes

Control	Control Name	Is Control Effective?
SCTS		
AC-2	Account Management	No, refer to Finding 3
AC-3	Access Enforcement	Yes
AU-6	Audit Review, Analysis, and Reporting	Yes
CA-1	Security Assessment and Authorization Policy & Procedures	Yes
CA-2	Security Assessments	No, refer to Finding 1
CA-3	Information System Connections	Yes
CA-5	Plan of Action and Milestones	No, refer to Finding 4
CA-6	Security Authorization	Yes
CA-7	Continuous Monitoring	Yes
CP-1	Contingency Planning Policy & Procedures	Yes
CP-2	Contingency Plan	No, refer to Finding 9
CP-4	Contingency Plan Testing and Exercises	No, refer to Finding 9
CP-6	Alternate Storage Sites	Yes
CP-9	Information System Backup	No, refer to Finding 9
CP-10	Information System Recovery & Reconstitution	Yes
IA-1	Identification and Authentication Policy and Procedures	Yes
IA-2	Identification and Authentication (Organizational Users)	Yes
IA-3	Device Identification and Authentication	Yes
IA-4	Identifier Management	Yes
IA-5	Authenticator Management	Yes
RA-1	Risk Assessment Policy and Procedures	Yes
RA-2	Security Categorization	Yes
RA-3	Risk Assessment	No, refer to Finding 1
RA-5	Vulnerability Scanning	No, refer to Finding 6
SA-1	System and Services Acquisition Policy and Procedures	Yes
SA-5	Information System Documentation	Yes
SA-9	External Information Systems	No, refer to Finding 7
SC-8	Transmission Integrity	Yes
SI-2	Flaw Remediation	No, refer to Finding 6
PL-2	System Security Plan	No, refer to Finding 5
PL-4	Rules of Behavior	Yes

Control	Control Name	Is Control Effective?
Google		
RA-2	Security Categorization	Yes
RA-3	Risk Assessment	No, refer to Finding 1
SA-9	External Information Systems	No, refer to Finding 7
PL-2	System Security Plan	No, refer to Finding 5