Cotton&
Company

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

P: 703.836.6701
F: 703.836.0941
www.cottoncpa.com

The Inspector General
National Archives and Records Administration

INDEPENDENT AUDITOR'S REPORT

We have audited the accompanying consolidated balance sheet of the National Archives and Records Administration (NARA) as of September 30, 2010 and 2009, and the related Statements of Net Cost, Changes in Net Position, and Budgetary Resources for the years then ended. These financial statements are the responsibility of NARA management. Our responsibility is to express an opinion on the financial statements based on our audits.

We conducted our audits in accordance with auditing standards generally accepted in the United States of America; standards applicable to financial statement audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) audit guidance. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statements' presentation. We believe that our audits provide a reasonable basis for our opinion.

In our opinion, the financial statements referred to above, present fairly, in all material respects, the financial position of NARA as of September 30, 2010 and 2009, and its net cost, changes in net position, and budgetary resources for the year then ended, in conformity with accounting principles generally accepted in the United States of America.

In accordance with *Government Auditing Standards,* we have also issued our reports dated November 12, 2010, on our consideration of NARA's internal control over financial reporting, and on our tests of NARA's compliance with certain provisions of laws and regulations and other matters. The purpose of those reports is to describe the scope of our testing on internal control over financial reporting and compliance, and the results of that testing, and not to provide an opinion on the internal control over financial reporting or on compliance. Those reports are an integral part of an audit performed in accordance with *Government Auditing Standards* and should be read in conjunction with this report, in considering the results of our audits.

The information in the Management Discussion and Analysis and Required Supplementary Information sections is not a required part of the consolidated financial statements, but is supplementary information required by accounting principles generally accepted in the United States of America. We have applied certain limited procedures, which consisted principally of inquiries of management regarding methods of measurement and presentation of this information. We did not, however, audit this information and, accordingly, we express no opinion on it.

Our audits were conducted for the purpose of forming an opinion on the consolidated financial statements taken as a whole. The information in the Message from the Archivist, Performance Section, and Other Accompanying Information is presented for purposes of additional analysis and is not required as part of the consolidated financial statements. This information has not been subjected to auditing procedures and, accordingly, we express no opinion on it.

COTTON & COMPANY LLP

Colette Y. Wilson
Partner

Colette Y Wilson

Alexandria, Virginia
November 12, 2010

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

P: 703.836.6701
F: 703.836.0941
www.cottoncpa.com

The Inspector General
National Archives and Records Administration

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL

We have audited the financial statements of the National Archives and Records Administration (NARA) as of September 30, 2010 and 2009, and have issued our report thereon dated November 12, 2010. We conducted our audits in accordance with auditing standards generally accepted in the United States of America; standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) audit guidance.

In planning and performing our audits of NARA's financial statements as of and for the year ended September 30, 2010 and 2009, in accordance with auditing standards generally accepted in the United States of America, we considered NARA's internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of NARA's internal control. Accordingly, we do not express an opinion on the effectiveness of NARA's internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of an entity's financial statements will not be prevented, or detected and corrected on a timely basis.

Our consideration of internal control was for the limited purpose described in the second paragraph and was not designed to identify all deficiencies in internal control that might be deficiencies, significant deficiencies, or material weaknesses. We did not identify any deficiencies in internal control that we consider to be material weaknesses, as defined above. However, we identified certain deficiencies in internal control that we consider to be a significant deficiency. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

INFORMATION TECHNOLOGY

During Fiscal Year (FY) 2010, NARA continued to make improvements in its information technology (IT) control environment by addressing recommendations made in previous audits. Improvements are still needed in the IT control areas of access controls and configuration management, as noted below and in Appendix A to this report.

In addition, contingency planning and security management issues identified in prior years also remain open. Deficiencies identified during the FY 2010 financial statement audit are discussed below. These issues, combined with open recommendations from the prior-year financial statement audit (see Appendix A), collectively represent a significant deficiency in internal control over financial reporting.

Access Controls

Access controls provide reasonable assurance that access to computer resources is reasonable and restricted to authorized individuals. NARA's procedures for creating, identifying and authenticating, and providing accountability over NARANet accounts did not ensure that all accounts were properly authorized. Specific issues identified during testing are discussed below.

Account Creation. NARA has not implemented sufficient account creation controls to ensure that all new NARANet accounts are requested and authorized by a user's supervisor, or that the help desk ticket/access form process is properly followed. In our tested sample of new accounts, we noted the following issues:

- Proper documentation did not exist to support the creation of the account
- Accounts were created without first obtaining adequate supervisory approval
- Accounts were initiated by the end-user

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3: *Recommended Security Controls for Federal Information Systems and Organizations*, requires the following:

> *AC-2 ACCOUNT MANAGEMENT*
>
> *The organization manages information system accounts, including:*
>
> a. *Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);*
> b. *Establishing conditions for group membership;*
> c. *Identifying authorized users of the information system and specifying access privileges;*
> d. *Requiring appropriate approvals for requests to establish accounts;…*
> i. *Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and*
> j. *Reviewing accounts [Assignment: organization-defined frequency].*

Without effective account creation/authorization controls in place, NARA cannot ensure that current employees are not requesting unapproved and unauthorized access, potentially making them unauthorized members of groups that can access files and spreadsheets stored on financial share drives. NARA does require a badge to obtain a network account, which serves as a compensating control to ensure this weakness cannot be exploited by an individual who does not already have access to NARA facilities.

Recommendation 1. We recommend that the NARA Chief Information Officer (CIO) require a record of logged-in users creating account requests to show that request are being generated by a supervisor, not the user.

Identification and Authentication. Identification and Authentication controls provide reasonable assurance that individual users are uniquely identified and authenticated for all accesses other than those explicitly identified and documented by an organization. To properly address this requirement, the unique identification of individuals with access to group accounts (e.g., shared privilege accounts) must be considered for detailed accountability of activity.

NARA has not implemented sufficient Identification and Authentication controls to ensure that the Order Fulfillment and Accounting System (OFAS) application uniquely identifies all application users. We identified a shared domain administrator account within OFAS that is used as an OFAS support team group account with a shared password to perform activities in the OFAS application.

NIST SP 800-53, Revision 3, requires the following:

> *IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)*
>
> *The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).*
>
> *Supplemental Guidance: Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations). Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in AC-14. Unique identification of individuals in group accounts (e.g., shared privilege accounts) may need to be considered for detailed accountability of activity.*

Without the ability to uniquely identify and authenticate individual users of the shared Domain Admin account, accountability for activities and events performed by the account cannot be established.

Recommendation 2. We recommend that the NARA CIO assign one individual to the shared account, or split responsibilities of the shared account to additional administrator accounts, to allow accountability of administrator activities to be established.

Audit and Accountability. Audit and Accountability controls provide reasonable assurance that an organization is complying with required industry standards, as well as its own policies and procedures. NARA has not implemented sufficient audit and accountability controls over audit settings and logging and monitoring, as described below.

- **Audit Settings.** Audit Settings within an information system define what events or activities generate an audit log and what information about the event is recorded is included in the log. During the audit, we noted that NARANet's audit settings were not configured to log group membership add and delete activities.

- **Logging and Monitoring.** Logging and Monitoring is the process an organization follows to track, review, and escalate (if necessary) the events captured in audit logs generated by the system/OS/network/application. During the audit, we noted that NARA's Audit and Accountability Methodology is not being enforced or followed. General Support System (GSS) and application-specific issues noted during testing are discussed below:

  - **OFAS**. Controls were not adequate to ensure that the OFAS application was configured to log all required auditable events (per NARA IT Security Methodology for Audit and Accountability) and that procedures were implemented to appropriately review these logs on a regular basis. OFAS was reconfigured on September 29, 2010, to begin to log account creations, deletions, and modifications. Before this, settings were not in place, and there is still no formal process for reviewing the logs periodically.

  - **NARANet**. NARA personnel reviewed network activity logs on an as-needed basis, but not routinely and periodically. Management is currently working to address this by implementing a log consolidation and monitoring tool, Netforensics.

  - **RCPBS.** Controls were not adequate to ensure that the Records Center Program Billing System (RCPBS) application was configured to log all required auditable events (per NARA IT Security Methodology for Audit and Accountability) and that procedures were implemented to appropriately review these logs on a regular basis. We found no evidence to show that RCPBS is configured to log all required events, or that standard log monitoring procedures were established and are being performed.

NIST SP 800-53, Revision 3, requires the following:

> *AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING*
>
> *The organization:*
>
> *a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and*
>
> *b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.*

Additionally, NARA IT Security Methodology for Audit and Accountability, dated July 15, 2009, requires the following:

> *2 AUDITABLE EVENTS [AU-2]*
>
> *This section describes how NARA meets the NARA IT Security Architecture control [AU-2] for Auditable Events.*
>
> *NARA's security policy for Auditable Events is as follows:*
>
> *NARA Office of IT Services (NH) develops, disseminates, and at least annually reviews and updates a formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among NARA entities, and compliance; and formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.*
>
> *NARA's security requirements for Auditable Events are as follows:*
>
> *[AU-2.1] Each information system generates audit records for the following events:*
>
> - *Startup and shutdown*
> - *Account Creation*
> - *Authentication*
> - *Authorization and Permission granting/changing*
> - *Actions by trusted users*
> - *Password changes for privileged users*
> - *Unsuccessful login attempts*
>
> *[AU-2.2] NH shall identify important events which need to be audited as significant and relevant to the security of each information system. System Owner shall identify any additional specific events relevant to the system's sensitivity level. Audit records shall be generated at various levels of abstraction, including at the packet level as information traverse the network. System Owner shall specify in the SSP which information system components carry out auditing activities. The security audit function shall coordinate with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function.*

Without appropriately configured audit settings and an effective logging and monitoring process, management cannot ensure that only appropriate accesses and activities are taking place.

Recommendation 3. We recommend that the NARA CIO:

- Reconfigure audit settings within the NARANet Novell environment to log group membership add and delete activities.

- Continue with the implementation of Netforensic and, once in place, ensure that procedures exist for identifying key events that will be alerted to and reviewed by management on a periodic basis.

- Continue with efforts to audit account creations, deletions, and modifications within OFAS and develop standard procedures for regularly reviewing and monitoring application audit logs.

- Enable logging of all events within RCPBS, required by NARA IT Security Methodology for Audit and Accountability, and develop standard procedures for regularly reviewing and monitoring application activity logs.

Configuration Management

Configuration Management controls provide reasonable assurance that changes to an organization's IT infrastructure, hardware, or software are properly managed and tracked, and that baseline configurations are defined and configured within the production environment. During testing, we identified issues with NARA's baseline configuration practices. They are discussed below.

Configuration baselines provide current specifications for how an information system/network device, application, hardware, and software are built. Additionally, baselines provide individuals with configuration management responsibilities within the organization, a benchmark to compare against actual configurations.

NARA has developed configuration instructions and has a beginning baseline for configuration for switches. Configuration instructions or baselines are not, however, in place for NARA's routers and firewalls. The current baseline is not based on and does not address all areas in approved checklists for router and firewall platforms and devices in use contained in NIST SP 800-70, *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers*.

NIST SP 800-53, Revision 3, requires the following:

> *CM-6 CONFIGURATION SETTINGS*
>
> *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.*

Additionally, NARA IT Security Methodology for Configuration Management, dated January 13, 2010, requires the following:

> *6 Configuration Settings [CM-6]*
>
> *This section describes how NARA meets the NARA IT Security Architecture control [CM-6] for Configuration Settings.*
>
> *NARA's security policy for Configuration Settings is as follows:*

> *NARA Office of Information Services (NH) establishes mandatory configuration settings for information technology products employed within the information system, configures the security settings of information technology products to the most restrictive mode consistent with operational requirements, documents the configuration settings, and enforces the configuration settings in all components of the information system.*
>
> *NARA's security requirements for Configuration Settings are as follows:*
> *[CM-6.1] NH shall establish mandatory configuration settings for information technology products employed within the information system, configure the default security settings of information technology products to the most restrictive mode consistent with operational requirements, document the configuration settings, and enforce the configuration settings in all components of the information system.*
>
> *[CM-6.2] NH shall monitor and control changes to the configuration settings in accordance with NARA policies and procedures.*
>
> *[CM-6.3] NIST SP 800-70 shall be used for guidance on producing and using configuration settings (i.e., checklists) for information technology products employed in NARA information systems.*
>
> *[CM-6.4] For high integrity information systems, NARA shall employ mechanisms to centrally manage, apply and verify configuration settings.*

The absence of documented full configuration baselines increases the risk that: unauthorized access may occur, security weaknesses could exist within the NARANet architecture and not be detected by management in a timely manner, and computing resources are not in compliance with established baselines.

Recommendation 4. We recommend that the NARA CIO improve upon NARA's current router and firewall build process by updating their standard configuration file to be based on NIST-approved security checklists for router and firewall platforms and devices in use by NARA. We also recommend that the final standard configuration be documented and compared against devices to monitor for configuration compliance on a periodic basis.

STATUS OF PRIOR-YEAR RECOMMENDATIONS

We reviewed the status of NARA's corrective actions with respect to the significant deficiencies from the prior-year report on internal control. Appendix A to this report provides details of the status of recommendations.

NARA's management response to the significant deficiency identified in our report is included as Appendix B to this report. We did not audit NARA's response and, accordingly, we provide no opinion on it.

In addition to the significant deficiency described above, we noted certain matters involving internal control and its operation that will be reported to NARA management in a separate letter.

This report is intended solely for the information and use of management of NARA, NARA Office of Inspector General, Government Accountability Office, OMB, and Congress, and is not intended to be and should not be used by anyone other than those specified parties.

COTTON & COMPANY LLP

Colette Y. Wilson, CPA
Partner

Alexandria, Virginia
November 12, 2010

APPENDIX A
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION
STATUS OF PRIOR-YEAR RECOMMENDATIONS
SEPTEMBER 30, 2010

APPENDIX A
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION
STATUS OF PRIOR-YEAR RECOMMENDATIONS
SEPTEMBER 30, 2010

Condition/Audit Area and Recommendations	Status as of September 30, 2010
Personal Property	
1. Finalize and implement its personal property policies and procedures manual during the first quarter of FY 2010.	Closed
2. Provide personal property-related training to NARA employees.	Closed
3. Design and implement monitoring procedures to ensure NARA employees adhere to personal property-related policies and procedures.	Closed
4. Design and implement procedures to ensure the accountability of assets in the custody of contractors.	Closed
5. Continue to implement personal property accounting functionality within the Maximo system, and in doing so, ensure that the application has adequate functionality to meet the requirements articulated by the Joint Financial Management Improvement Program (JFMIP) in its document titled, Property Management Systems Requirements.	Open, however no longer a significant deficiency. This deficiency will be reported to management in a separate report.
6. Perform a risk assessment to determine if it has sufficient procedures in place to mitigate risks posed by the manual processes used to account for personal property transactions.	Closed
7. Design and implement controls, as necessary, to address significant risks identified during the risk assessment.	Closed
Access Controls	
8. Implement a process for managing NARANET accounts that:	Partially Open (Termed users are not having access removed in a timely manner. Generic accounts are not catalogued and assigned ownership to an individual.)
a) Requires a recertification of all system accounts at least annually.	
b) Ensures all accounts are tied to a specific individual who has the responsibility for managing the account, and determining the ongoing need for non-login accounts.	
c) Identifies inactive accounts on a regular basis and removes access in a timely manner.	
d) Ensures all access and privileges of terminated employees are promptly removed.	
9. Implement a more restrictive password age control for NARANET that is consistent with requirements for Federal information systems.	Closed

Condition/Audit Area and Recommendations	Status as of September 30, 2010
10. Implement a process for managing RCPBS accounts that:	
a) Requires a recertification of all system accounts at least annually.	Open
b) Identifies inactive accounts on a regular basis and removes or disables access in a timely manner.	Closed
c) Implements a more restrictive password age control that is consistent with requirements for federal information systems.	Open
11. Implement compensating logging and monitoring controls for PPMS to ensure that the risk of unauthorized access is mitigated.	Closed
12. Enforce its current policies and procedures used to manage systems and accounts to ensure all access and privileges of terminated employees are promptly removed.	Closed (see 8 d), above)
13. Ensure that supervisors receive training in their exit clearance process responsibilities, including alerting applicable personnel when employees and contractors under their supervision no longer require access.	Open
14. Continue effort to finalize the contract with the independent contractor to provide an assessment of NARA's incident response program, provide targeted training to NARA personnel involved with incident response, and to conduct simulated exercises.	Closed
15. Develop and implement policies and procedures that prohibit RCPBS users from having multiple accounts as well as the ability to enter and approve their own transactions.	Open
Contingency Planning	
16. Fully implement a contingency planning policy consistent with guidance provided in NIST SP 800-34, Contingency Planning Guide for Information Technology Systems. The policy should include requirements for updating the contingency plan to reflect current operating conditions.	Closed
17. Update the contingency and disaster recovery plans for OFAS to reflect current operating conditions.	Closed
18. Update the contingency and disaster recovery plans for RCPBS to reflect current operating conditions.	Open
Security Management	
19. Complete risk assessments for all NARNET components.	Open
20. Finalize and approve security plans for all NARANET components.	Open

Condition/Audit Area and Recommendations	Status as of September 30, 2010
21. Certify each NARANET component, then certify and accredit the entire NARANET general support system.	Open
22. Implement policies and procedures which require the completion of security and awareness training before being granted access to NARA information systems.	Open

APPENDIX B
MANAGEMENT COMMENTS

NATIONAL
ARCHIVES

Date: November 9, 2010

To: Paul Brachfeld, OIG

From: David S. Ferriero, N

Subject: FY10 Management Response to Audit Report

Thank you for the opportunity to review and comment on the draft reports entitled, *Independent Auditor's Report on Internal Control* and *Independent Auditor's Report on Compliance with Laws and Regulations*. We appreciate your efforts and cooperation throughout this audit process.

We are pleased that the Independent Auditor recognizes our progress, as evidenced by an "unqualified" audit opinion on this year's financial statements, downgrading of prior year significant deficiency in personal property management, and recognition of NARA's efforts in addressing the Information Technology control environment.

While challenges remain, I believe NARA has demonstrated its commitment to improved financial management and ability to produce accurate and reliable financial statements. NARA will continue to work diligently to address its challenges, as well as to further improve its financial management processes and related internal controls. We would like to again thank the Office of Inspector General and the Cotton & Company, LLP for working with NARA staff in a professional and dedicated manner.

DAVID S. FERRIERO
Archivist of the United States

Cotton & Company

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

P: 703.836.6701
F: 703.836.0941
www.cottoncpa.com

The Inspector General
National Archives and Records Administration

INDEPENDENT AUDITOR'S REPORT ON COMPLIANCE AND OTHER MATTERS

We have audited the financial statements of the National Archives and Records Administration (NARA) as of, and for the year ended September 30, 2010 and 2009, and have issued our report thereon dated November 12, 2010. We conducted our audits in accordance with auditing standards generally accepted in the United States of America; standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) audit guidance.

NARA's management is responsible for complying with laws and regulations applicable to NARA. As part of obtaining reasonable assurance about whether NARA's financial statements are free of material misstatements, we performed tests of NARA's compliance with certain provisions of laws and regulations that have a direct and material effect on the financial statements. We did not test compliance with all laws and regulations applicable to NARA. We limited our tests of compliance to those provisions of laws and regulations required by OMB audit guidance that we deemed applicable to the financial statements for the fiscal year ended September 30, 2010. We caution that noncompliance may have occurred and may not have been detected by these tests, and that such testing may not be sufficient for other purposes.

The results of our tests of compliance with laws and regulations described in the preceding paragraph disclosed no instances of material noncompliance that are required to be reported under *Government Auditing Standards* and OMB audit guidance. Providing an opinion on compliance with certain provisions of laws and regulations was not, however, an objective of our audit, and, accordingly we do not express such an opinion.

This report is intended solely for the information and use of management of NARA, NARA Office of Inspector General, the Government Accountability Office, OMB, and Congress, and is not intended to be and should not be used by anyone other than those specified parties.

COTTON & COMPANY LLP

Colette Y. Wilson
Partner

Alexandria, Virginia
November 12, 2010