National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

Date : December 11, 2009

Reply to Attn of : Office of Inspector General (OIG)

Subject : Audit Report No. 10-02 Cotton & Company LLP (C&C) Audit of the National Archives and Records Administration FY 2009 Financial Statements

To : David Ferriero, Archivist of the United States (N)

Enclosed for your review are the reports prepared by Cotton & Company, LLP (C&C) for the subject audit. C&C issued an unqualified opinion on NARA's FY 2009 financial statements.

C&C reported two significant deficiencies in internal control over financial reporting in the areas of Personal Property and Information Technology resulting in 18 recommendations that if implemented, should correct the matters reported. C&C disclosed no material weaknesses and no instances of noncompliance with certain provisions of laws and regulations.

In connection with the contract, we reviewed C&C's report and related documentation and inquired of its representatives. Our review, as differentiated from an audit in accordance with U.S. Generally Accepted Government Auditing Standards (GAGAS) was not intended to enable us to express, as we do not express, an opinion on NARA's financial statements or conclusions about the effectiveness of internal control or on whether NARA's financial management system substantially complied with FFMIA; or conclusions with laws and regulations. C&C is responsible for the attached auditor's report dated November 12, 2009 and the conclusions expressed in the report. However, our review disclosed no instances where C&C did not comply, in all material respects, with GAGAS.

In accordance with NARA 1201, your written response to each recommendation is due within 45 days. We appreciate the cooperation and assistance NARA extended to C&C and my staff during the audit. If you have any questions, please contact me or James Springs, Assistant Inspector General for Auditing at (301) 837-3000.

Paul Brachfeld
Inspector General

Enclosure: Cotton & Company's NARA FY 2009 Financial Statements
Independent Audit Report

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

P: 703.836.6701
F: 703.836.0941
www.cottoncpa.com

Independent Auditor's Report

The Inspector General
National Archives and Records Administration

We have audited the accompanying consolidated balance sheet of the National Archives and Records Administration (NARA) as of September 30, 2009, and the related statement of net cost, changes in net position and budgetary resources, for the year then ended (hereinafter collectively referred to as the "financial statements"). These financial statements are the responsibility of NARA's management. Our responsibility is to express an opinion on these financial statements based upon our audit. The financial statements of NARA, as of September 30, 2008, were audited by other auditors whose report dated November 12, 2008, expressed an unqualified opinion on those statements.

We conducted our audit 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 and significant estimates made by management, as well as evaluating the overall financial statements' presentation. We believe our audit provides 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, 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, 2009, 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 audit.

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 the methods of measurement and presentation of this information. However, we did not 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

Jeffrey A. Long, CPA, CISA, CGFM
Partner

November 12, 2009
Alexandria, VA

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

P: 703.836.6701
F: 703.836.0941
www.cottoncpa.com

Independent Auditor's Report on Compliance and Other Matters

The Inspector General
National Archives and Records Administration

We have audited the financial statements of the National Archives and Records Administration (NARA) as of, and for the year ended September 30, 2009, and have issued our report thereon dated November 12, 2009. We conducted our audit in accordance with auditing standards generally accepted in the United States of America; the 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, 2009. 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. However, providing an opinion on compliance with certain provisions of laws and regulations was not 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 (GAO), OMB, and Congress, and is not intended to be and should not be used by anyone other than those specified parties.

COTTON & COMPANY LLP

Jeffrey A. Long, CPA, CISA, CGFM
Partner

November 12, 2009
Alexandria, VA

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

P: 703.836.6701
F: 703.836.0941
www.cottoncpa.com

Independent Auditor's Report on Internal Control

The Inspector General
National Archives and Records Administration

We have audited the financial statements of the National Archives and Records Administration (NARA) as of, and for the year ended September 30, 2009, and have issued our report thereon dated November 12, 2009. We conducted our audit in accordance with auditing standards generally accepted in the United States of America; the 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 audit, we considered NARA's internal control over financial reporting by obtaining an understanding of the design effectiveness of NARA's internal control, determining whether these controls had been placed in operation, assessing control risk, and performing tests of the controls in order to determine our auditing procedures for the purpose of expressing our opinion on the consolidated financial statements, and not to provide an opinion on the internal controls. Accordingly, we do not express an opinion on the effectiveness of NARA's internal control over financial reporting.

We limited our internal control testing to those controls necessary to achieve the objectives described in OMB audit guidance. We did not test all internal controls relevant to operating objectives, as broadly defined by the Federal Managers' Financial Integrity Act of 1982 (FMFIA), such as those controls relevant to ensuring efficient operations.

A control deficiency 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 misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects NARA's ability to initiate, authorize, record, process, or report financial data reliably, in accordance with generally accepted accounting principles, such that there is more than a remote likelihood that a misstatement of NARA's financial statements that is more than inconsequential will not be prevented or detected by NARA's internal controls.

A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by NARA's internal controls.

Our consideration of internal controls was for the limited purpose described in the second and third paragraphs of this report, and would not necessarily identify all deficiencies in internal control that might be significant deficiencies or material weaknesses.

We identified two deficiencies in internal control over financial reporting that we consider to be significant deficiencies. However, we do not believe that the significant deficiencies described below are material weaknesses over financial reporting.

****

SIGNIFICANT DEFICIENCIES

I. Personal Property

NARA's processes and internal control procedures used to ensure the proper accountability of personal property assets and related accounting transactions need improvement. Improvements are needed in the following key areas:

A. **Adherence to Policies and Procedures -** NARA employees do not always follow operating policies and procedures implemented by the Facilities and Personal Property Management Division (NAF) regarding the accountability of personal property items. Specifically, staff members do not always report or document the acquisition, transfer, or disposition of personal property items.

B. **Personal Property in the Hands of Contractors** - NARA does not have policies and procedures in place to ensure the physical accountability of NARA-owned assets that are in the custody of contractors. In addition, NARA property managers do not barcode or inventory personal property used by and in the possession of contractors.

C. **Personal Property Systems** - Personal property is tracked in the Personal Property Management System (PPMS), which does not interface with the general ledger. NARA has determined that the cost of integrating PPMS with the general ledger would exceed the benefits; therefore, these two systems will not be integrated. NARA's Financial Reports Staff (NAX) has been unable to rely on PPMS for certain property accounting functions due to the system's instability. Instead, personal property transactions (e.g. acquisitions, disposals, and depreciation) are valued on Microsoft Excel spreadsheets using PPMS information and manual processes. These processes are prone to human error and sufficient compensating controls are not in place to provide reasonable assurance that errors will be identified and corrected in a timely manner.

OMB Circular A-123, *Management's Responsibility for Internal Control* states:

> *It is management's responsibility to develop and maintain effective internal control…Agency managers should continuously monitor and improve the effectiveness of internal control associated with their programs.*

In addition, Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* states:

> *An agency must establish physical control to secure and safeguard vulnerable assets. Examples include security for and limited access to assets such as cash, securities, inventories, and equipment which might be vulnerable to risk of loss or unauthorized use.*

Failing to implement adequate processes and internal control procedures over personal property transactions could result in assets being stolen or misplaced and not being detected by management in a timely manner. In addition, personal property related account balances could be misstated because accounting personnel are not notified of acquisitions and disposals in a timely manner. The following issues were noted when testing personal property transactions as of June 30, 2009.

1. **Stewardship of Accountable Items** – While performing testing of NARA's internal control over accountable personal property assets, we noted the following issues:

- NARA was unable to locate one asset in our sample, and thus, we could not verify the existence of the item.

- Nine sampled items were recorded as being physically located in Archives II in PPMS, but the results of our audit procedures indicated the items were located at various other NARA field locations.

- Two accountable items were identified at NARA facilities and were not recorded in PPMS.

2. **Account Balance Misstatements** - While performing testing of personal property accounting transactions, we noted the following issues:

   - NARA improperly recorded disposal transactions for fully depreciated personal property items with a total acquisition cost of roughly $21 million. In FY 2009, NARA recorded disposal transactions for all fully depreciated personal property assets without first verifying the physical status of the asset. These improper entries were subsequently reversed.

   - In addition, we noted several insignificant errors in depreciation calculations that were caused by human error.

   Recommendations

   We recommend that NAF should:

   1. Finalize and implement its personal property policies and procedures manual during the first quarter of FY 2010.

   2. Provide personal property-related training to NARA employees**.**

   3. Design and implement monitoring procedures to ensure NARA employees adhere to personal property-related policies and procedures.

   4. Design and implement procedures to ensure the accountability of assets in the custody of contractors.

   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*.

   We recommend that NAX should:

   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.

   7. Design and implement controls, as necessary, to address significant risks identified during the risk assessment.

II. Information Technology

During FY 2009 NARA continued to make improvements in its information technology (IT) control environment by addressing recommendations made in previous audits. However, improvements are still

needed in the following IT control areas: access control, segregation of duties, and contingency planning. Deficiencies noted in each area are discussed in sections A through C below. The issues discussed below, combined with the open recommendations from the previous fiscal year's (see Appendix A) financial statement audit, collectively represent a significant deficiency in internal control over financial reporting.

A. Access Controls

Access controls provide reasonable assurance that access to computer resources is reasonable and restricted to authorized individuals. NARA access control procedures must be improved in the following areas: account management, exit clearance process and incident response programs. Specific issues identified during testing are discussed below.

1. <u>Account Management</u>

NARA has not implemented sufficient controls to ensure that account management policies and procedures are consistent with National Institute of Standards and Technology (NIST) requirements and industry best practices. Application-specific issues noted during testing are discussed below:

a) NARANET

- NARA management relies on the annual security awareness training process to recertify accounts and determine if users still require system access. This process does not ensure that all applicable accounts are removed or disabled in a timely manner because the certification only occurs once per year. Additionally, this process only reviews individuals with login abilities; it does not review accounts that are not assigned to a specific individual (e.g. backup accounts, test accounts, and training accounts).

- Numerous NARANET accounts exist that are used for testing, training, and back-up. The responsibility for managing and determining the ongoing need for these accounts are not associated to a specific individual. Therefore, unnecessary accounts may be still active due to a lack of oversight responsibilities.

- Inactive accounts are not consistently disabled or removed in a timely manner. We noted 224 accounts in which the user had either never logged on to NARANET or had not logged on in over a year. In all 224 cases, the accounts were not disabled.

- NARANET's maximum password age requirement of 365 days is not consistent with NIST and OMB requirements and is not effective for providing adequate protection against unauthorized use. The password age requirement of 365 days was put in place based upon a standard designed for public use systems, NIST Special Publication (SP) 800-63 *Electronic Authentication Guideline*, which is not meant for internal government use systems. In addition, our testing identified 37 active accounts that had not changed their password in over 365 days. These password practices and issues increase the risk that unauthorized users could effectively guess passwords and gain access to NARA's computing resources.

b) Records Center Program Billing System (RCPBS)

- RCPBS does not have configurable lockout policy settings. Also, RCPBS does not have a configurable password policy that requires users to change their password periodically; prohibits the reuse of passwords for a specific length of time; and automatically expiries user passwords.

- Additionally, inactive accounts are not consistently disabled or removed in a timely manner. We identified 34 accounts that were inactive for over 365 days.

c) Personal Property Management System (PPMS):

Our testing noted that PPMS cannot enforce a configurable password or lockout policy.

NIST SP 800-53, Revision 2: *Recommended Security Controls for Federal Information Systems*, requires the following:

AC-2 ACCOUNT MANAGEMENT
The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts at least annually.

The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. Account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know/need-to-share changes.

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS
The information system enforces a limit of 5 consecutive invalid access attempts by a user during a 15-minute time period. The information system automatically locks the account until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

IA-5 AUTHENTICATOR MANAGEMENT
The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.

For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations.

In addition, the Federal Desktop Core Configuration (FDCC) requires the following:

MAXIMUM PASSWORD AGE
All desktop operating systems in the Federal government are required to meet the minimum security controls defined in the ***Federal Desktop Core Configuration (FDCC)*** *guidance provided by NIST. This guidance that applies to Windows desktops requires a maximum password age of 60 days.*

Center for Internet Security (CIS), *Novell eDirectory 8.7, Consensus Baseline*, requires the following:

MAXIMUM PASSWORD AGE
The 60 day recommendation from FDCC guidance is also consistent with the ***Center for Internet Security's Novell eDirectory 8.7 Consensus Baseline Security****, Security Settings Version 1document which requires a maximum password age setting of 90 days or less.*

Without proper account management procedures, there is an increased risk that malicious users will be able to access NARA systems and resources. Such unauthorized access could result in the loss of data confidentiality, integrity, or availability.

Recommendations

We recommend that that the NARA Chief Information Officer (CIO):

8. Implement a process for managing NARANET accounts that:

    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.

10. Implement a process for managing RCPBS accounts that:

    a) Requires a recertification of all system accounts at least annually.

    b) Identifies inactive accounts on a regular basis and removes or disables access in a timely manner.

    c) Implements a more restrictive password age control that is consistent with requirements for federal information systems.

11. Implement compensating logging and monitoring controls for PPMS to ensure that the risk of unauthorized access is mitigated.

2. <u>Exit Clearance Process</u>

NARA has not implemented sufficient controls to ensure that its exit clearance policies and procedures are consistent with NIST requirements. Specific, issues noted during testing were:

a) NARANET accounts for terminated employees were not consistently disabled or removed in a timely manner. Out of 45 sampled terminated employees, we identified five accounts that were not disabled or removed a month after their effective termination date. Three of these accounts were still active at the time of our testing. In addition, two of the terminated employees had accessed NARANET at least once after their effective termination date.

b) RCPBS accounts of terminated employees were not consistently disabled or removed in a timely manner. We identified four instances in which terminated employees accounts were not disabled or removed because the IT Helpdesk, or other appropriate personnel, were not notified of their separation.

NIST SP 800-53, Revision 2: *Recommended Security Controls for Federal Information Systems*, requires the following:

PS-4 PERSONNEL TERMINATION
The organization, upon termination of individual employment, terminates information system access, conducts exit interviews, retrieves all organizational information system-related property, and provides appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems.

An ineffective exit clearance process increases the risk that disgruntled former employees could use their continued system access to negatively impact the organization. Such unauthorized access could result in the loss of data confidentiality, integrity, or availability.

Recommendations

We recommend that the Office of Policy and Planning Staff (NPOL):

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.

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.

3. Incident-Response Program

Currently, NARA's incident response methodology does not include testing of the incident response plan or NARA-specific training for incident response roles. NARA is currently in the process of finalizing a contract with an independent contractor to provide incident response program support. This support will include an assessment of NARA's incident response program, targeted training to NARA personnel involved with incident response, and a simulation of incident response exercises.

NIST SP 800-53, Revision 2: *Recommended Security Controls for Federal Information Systems*, requires the following:

IR-2 INCIDENT RESPONSE TRAINING
The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training at least annually.

IR-3 INCIDENT RESPONSE TESTING AND EXERCISES
The organization tests and/or exercises the incident response capability for the information system at least annually using organization-defined tests and/or exercises to determine the incident response effectiveness and documents the results.

Without strong incident response training and testing, NARA cannot ensure that its current incident response procedures will be handled effectively by those with incident response roles and responsibilities or will properly mitigate all detected security incidents.

Recommendation

14. We recommend that that the NARA CIO continue its 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.

B. Segregation of Duties

Segregation of duties controls provide reasonable assurance that incompatible duties are effectively segregated. NARA does not have sufficient controls in place to ensure that incompatible roles in RCPBS are not assigned to individual system users. Specifically, when reviewing Webtally (a component system of RCPBS), we found that:

1. Seventy-seven users were assigned the "MANAGER" role in Webtally, and can both enter and approve transactions without the transaction being reviewed by a second party.

2. Users can be assigned multiple accounts with incompatible roles. For example, individuals with user accounts (e.g. "ACCTREP", "MANAGER") can also be given accounts with security administration capabilities ("ADMIN"). We noted 3 instances in which users were assigned security administration rights in addition to their user rights.

NIST SP 800-53, Revision 2: *Recommended Security Controls for Federal Information Systems,* states the following:

AC-5 SEPARATION OF DUTIES
The information system enforces separation of duties through assigned access authorizations.

The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.

Improper segregation of duties increases the risk of fraudulent acts, which could lead to financial, data and service loss, as well as potentially compromise the integrity, confidentiality, and availability of RCPBS data.

Recommendation

We recommend that the Assistant Archivist for Regional Records Services (NR):

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.

C. Contingency Planning

Contingency planning helps protect information resources by minimizing the risk of unplanned interruptions and provides for the recovery of critical operations, should interruptions occur. NARA did not have sufficient controls in place to ensure that contingency and disaster recovery plans for financial systems reflected current operating conditions. Specifically, our testing noted that the Order Fulfillment and Accounting (OFAS) contingency plan and the RCPBS disaster recovery plan did not reflect current operating conditions.

NIST SP 800-53, Revision 2: *Recommended Security Controls for Federal Information Systems*, states the following:

CP-5 CONTINGENCY PLAN UPDATE
The organization reviews the contingency plan for the information system at least annually and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

Not having complete and up-to-date disaster recovery and contingency plans for key financial systems increases the risk that NARA would be unable to respond to an emergency situation, which could lead to financial loss and loss of important data or service(s).

Recommendations

We recommend that the NARA CIO:

16. Fully implement a contingency planning policy that is 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.

We recommend that the Assistant Archivist for Administration (NA):

17. Update the contingency and disaster recovery plans for OFAS to reflect current operating conditions.

We recommend that NR:

18. Update the contingency and disaster recovery plans for RCPBS to reflect current operating conditions.

STATUS OF PRIOR YEAR COMMENTS

We have reviewed the status of NARA's corrective actions with respect to the significant deficiency from the previous year's report on internal control. Details of the status of the recommendations are reported in Appendix A to this report.

****

NARA's management response to the significant deficiencies 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 deficiencies described above, we noted certain matters involving internal control and its operation that we reported to NARA management in a separate letter, dated November 12, 2009.

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

COTTON & COMPANY LLP

Jeffrey A. Long, CPA, CISA, CGFM
Partner

November 12, 2009
Alexandria, VA

Appendix A
NATIONAL ARCHIVES AND RECORDS ADMINSTRATION
STATUS OF PRIOR YEAR FINDINGS AND RECOMMENDATIONS
September 30, 2009

Condition/Audit Area	Recommendation Number	Recommendation	Current Status
Significant Deficiency			
Access Controls	1	Develop and implement VPN user access recertification procedures to require regular user access reviews for reasonableness.	Closed
	2	Revise NARA IT Security Requirements to specify a specific time frame (i.e., 24 or 48 hours) in which system access is to be removed upon an employee's separation of employment.	Closed – Revised during FY 2009.
	3	Develop and implement Novell administrator user access recertification procedures to require regular user access reviews for reasonableness.	Closed
	4	Enable Novell audit logging activity for user logins, ACL changes, add group member or delete group member events in accordance with NARA policy.	Closed
	5	Update attack signatures for NARA NIDS to the most recent version.	Closed
Entity-Wide Security Program	6	Complete risk assessments for all NARNET components.	Open
	7	Finalize and approve security plans for all NARANET components.	Open
	8	Certify each NARANET component, then certify and accredit the entire NARANET general support system	Open
	9	Implement policies and procedures which require the completion of security and awareness training before being granted access to NARA information systems.	Open
	10	Complete exit clearance forms (Form 3009) for all separating employees which include formal sign offs by functional managers and maintain these documents in accordance with NARA document retention policies.	Closed – Revised during FY 2009.
	11	Modify IT security requirements for new hires prior to accessing NARA systems which map to interim clearance procedures for badge	Closed

		issuance.	
Contingency Plan	12	Finalize and approve the COOP in accordance with HSPD 7, 51, and 20, FCD 1, and NIST SP 800-34.	Closed
	13	Finalize and approve the NARANET general support system contingency plan.	Closed

Management Response to Auditor's Report (FY 2009)

National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

Date: November 12, 2009

To: Paul Brachfeld, NARA Inspector General

From: Adrienne Thomas, Acting Archivist of the United States

Subject: Response to Draft Independent Auditor's Report on NARA's Internal Controls and Compliance with Laws and Regulations for FY 2009

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.

NARA has worked hard to improve financial management processes and to resolve the information technology control issues. We are pleased that your reports recognize the notable progress that has been made.

While we generally agree with the assessments contained in the report, we offer the following comments on the Personal Property Significant Deficiency:

> NARA had recognized that its Property Management internal controls needed improvement. To that end, it initiated a Business Process Reengineering effort in FY 2008. New processes and procedures have been developed as a result of the Business Process Re-engineering effort. Many have already been implemented through various interim policy directives and the remainder will be implemented by the new Property Management Directive and Standard Operating Procedure, currently under review. These new procedures more clearly define roles, place a greater emphasis on training, and hold management accountable for property under their control, closing many of the loopholes found in the old procedures.
>
> Full implementation of the newly developed processes, coupled with ongoing implementation of the new Personal Property Management System (projected timeline for completion is April 2010) should address the audit finding on stewardship for accountable items.

In closing, while challenges remain, I believe NARA has demonstrated its commitment to producing accurate and reliable financial statements. NARA will continue its efforts to further improve its financial management processes and related internal controls.

ADRIENNE C. THOMAS
Acting Archivist of the United States

NARA's web site is http://www.archives.gov