Audit of NARA's Internal Control Program

OIG Audit Report No. 10-19

September 29, 2010

Table of Contents

Executive Summary

The National Archives and Records Administration (NARA) Office of Inspector General (OIG) performed an audit of NARA's Internal Control Program. Annually, the OIG performs a review to ensure NARA managers continuously monitor and improve the effectiveness of internal controls associated with their programs. This continuous monitoring, in conjunction with other periodic evaluations, provides the basis for the agency head's annual assessment of, and report on, internal controls as required by the Federal Managers' Financial Integrity Act (FMFIA) of 1982 (Public Law 97-255).

The objectives of the audit were to (1) evaluate NARA's compliance with guidance contained in FMFIA and the Office of Management and Budget's (OMB) Circular A-123, *Management's Responsibility for Internal Control* (the Circular), and the adequacy of the agency's assurance statement and (2) identify and evaluate the system of internal controls using the Government Accountability Office's (GAO), *Standards for Internal Control in the Federal Government* (the Standards), for assessing and evaluating internal controls. Specifically, we (1) examined management's responsibilities for internal control in Federal agencies as outlined in the Circular, and (2) reviewed the status of open recommendations made in prior year reports. Also, to facilitate the submission of NARA's annual assurance statement, we performed a preliminary review of the agency assurance statement in October 2009 (Appendix A).

Our initial assessment of the agency's FY 2009 assurance statement, as conveyed in our October 20, 2009 memorandum (Appendix A), was NARA's statement underreported material risk associated with Preservation and Processing programs and did not accurately reflect the breadth of risks in NARA's Information Security Program. This is the same conclusion we reached and conveyed to the agency in our assessments of their FY 2007 and FY 2008 assurance statements.

Our audit revealed at the end of the FMFIA reporting period, September 30, 2009, NARA did not fully comply with the requirements of the Circular as a formalized internal control program did not exist.[1] Since then NARA has made progress, and should be commended for establishing an implementation plan for a comprehensive internal control program. However, while the plan was established, much more remains to be done on the internal control program. Also, management has not closed the open audit recommendations from the last two years' audit reports. As a result of these conditions, NARA continues to exhibit weaknesses in internal controls first identified in FY 2007 that degrade the effectiveness of internal controls and the accuracy of office assurance statements.

[1] Although NARA is excluded from Appendix A of the Circular, the A-123 requirements in the Circular are for all agencies and require management to develop and maintain effective internal controls.

We are making two recommendations which we believe, once implemented, will address weaknesses cited in this review.

Background

The Federal Managers' Financial Integrity Act (FMFIA), Public Law 97-255, requires each agency to establish controls that reasonably ensure: (1) obligations and costs comply with applicable law, (2) assets are safeguarded against waste, loss, unauthorized use or misappropriation, and (3) revenues and expenditures are properly recorded and accounted for. In addition, the agency head must annually evaluate and report on the systems of internal accounting and administrative control.

The Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Internal Control* (the Circular), defines management's responsibility for internal control in Federal agencies. It provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on internal control. OMB revised the Circular in response to the Sarbanes-Oxley Act, effective in fiscal year 2006. This revision strengthened the requirements for management's assessment of internal control over financial reporting. The new requirements apply only to the 24 Chief Financial Officer Act agencies, thus exempting NARA from reporting pursuant to Section 4 of the FMFIA. However, NARA is still required to report on internal controls pursuant to Section 2 of FMFIA.

NARA issued Directive 114, *Management Controls*, to help managers implement the requirements of the Circular. NARA 114 defines responsibilities; defines the types of reviews that could be considered internal control assessments; identifies documentation that must be maintained in support of an internal control evaluation, and; addresses the development and maintenance of management control plans. Among the responsibilities defined by this guidance, Office Heads are required to identify and analyze risk, and the Policy and Planning Staff (NPOL) are required to provide oversight, guidance, and assistance to NARA offices concerning implementation of the NARA internal control program.

Assurance statements and information relating to FMFIA Section 2, Section 4 (from which NARA is exempt), and internal control over financial reporting should be provided in a single FMFIA report section of the annual Performance and Accountability Report (PAR) labeled "Management Assurances." The section should include the annual assurance statement, summary of material weaknesses and non-conformances, and summary of corrective action plans. Furthermore, FMFIA requires the Archivist to annually submit to the President and Congress (1) a statement on whether there is reasonable assurance that the agency's controls are achieving their intended objectives, and (2) a report on material weaknesses in the agency's controls.[2]

[2] NARA publishes the assurance statement in the annual PAR and no longer sends a separate statement to the President and Congress.

Objectives, Scope, Methodology

The objectives of the audit were to (1) evaluate NARA's compliance with guidance contained in FMFIA and OMB A-123 and the adequacy of the agency's assurance statement and (2) identify and evaluate the system of internal controls using GAO guidance for assessing and evaluating internal controls. Specifically, we (1) examined management's responsibilities for internal control in Federal agencies as outlined in the Circular, and (2) reviewed the status of open recommendations made in prior year reports. Also, to facilitate the submission of NARA's annual assurance statement, we performed a preliminary review of the agency assurance statement in October 2009 (Appendix A).

This audit was conducted in accordance with generally accepted government auditing standards between September 2009 and September 2010. These standards require 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Results

1. Lack of a formal internal control program.

Our review revealed NARA has not fully complied with the requirements of the Circular as there was no formalized internal control program. This condition exists because management has in the past focused on preparing assurance statements and management control plans, rather than implementing all of the standards for internal control. Internal controls are an integral component of an organization's management, and without it there is no reasonable assurance the following objectives were achieved: (1) effectiveness and efficiency of operations, (2) reliability of financial reporting, and (3) compliance with applicable laws and regulations. Also, the lack of a properly maintained internal control environment commensurate with NARA's activities can create issues, including unreliable financial reporting, unauthorized use or misappropriation of funds, and opportunities for fraud, waste, and abuse.

The Circular requires management to develop and maintain effective internal controls. Effective internal controls provide assurance significant weaknesses in the design or operation of internal control, that could adversely affect the agency's ability to meet its objectives, would be prevented or detected in a timely manner. The U.S. Government Accountability Office's (GAO's), *Standards for Internal Control in the Federal Government* (the Standards) outlines the five standards for internal control as (1) control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring. The Standards define the minimum level of quality acceptable for internal controls in the federal government and provide the basis against which internal controls are to be evaluated. Each standard is important, and all have to function together to make an effective control structure. All of the standards need to be implemented to have an effective internal control program, and therefore, NARA cannot continue to piecemeal the program as they have done in the past. Internal controls are likely to function well if management believes those controls are important and communicates that view to employees at all levels. If employees don't think management is committed to putting an internal control environment in place, then internal controls will be regarded as "red tape" and a waste of time.

We noted NARA will not be in full compliance with the Circular until it identifies critical functions, control and monitoring activities, and develops a formal risk management process. In the past management had not shown a comprehensive understanding of risk assessments and therefore did not adequately apply risk assessment as a component of their internal control planning and testing. Furthermore, the agency did not have the structure in place to support adequate, agency-wide/strategic risk identification and risk mitigation strategies.

At of the end of the FMFIA reporting period, September 30, 2009, NARA did not have an adequate internal control program. Since then NARA has made progress in

implementing a program. NPOL is leading the efforts in completing an implementation plan to address the areas NARA is not compliant with for the Circular. The plan identifies key activities, milestones, deliverables, and target dates for implementation. The initial phase of the implementation plan is to establish a baseline which will serve as the initial framework around which the internal control program will be structured. The initial baseline includes identifying the agency's existing critical functions, controls, risks, and monitoring activities. It also includes creating standard risk assessments. The framework will be reflected in the initial build out of a system NPOL would like to procure to automate the internal control program and related processes. NPOL does not expect the system to be fully functional until FY 2012.

The initial phase of the implementation plan will be considered complete once (1) the program baseline has been established and is reflected in the internal control automated system, (2) standard risk assessment questionnaires have been developed and incorporated into the system, and (3) accountable officials, function owners (or line of business owners), and senior managers are trained. After the initial phase, the annual internal control review will consist of review and revision of critical functions, preparation of risk assessments, and detailed control reviews based on the results of the risk assessments.

The OIG believes management is moving in the right direction in complying with the Circular. We will continue to track their efforts in the future**.**

Recommendation 1

The Archivist of the United States should:

a) Demonstrate a commitment to the internal control program by establishing centralized responsibility within NARA's existing organizational structure or within the proposed Performance & Accountability Office (as indicated in the *Proposed NARA Organization Report* from the Archivist's Task Force on Agency Transformation).

b) Formalize the Internal Control program to include the five standards for internal control: (1) control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring.

c) Consider establishing a Senior Management Council to provide oversight and additional accountability for the Internal Control Program.

Management Response

Management concurred with recommendation.

2. Prior year audit recommendations remain open.

Our review found recommendations for corrective actions contained in our FY 2007[3] and FY 2008[4] assurance statement audits have not been implemented. These recommendations were aimed at both addressing non-compliance with provisions of NARA 114 and the Circular, and modifying existing management control plans which too narrowly defined/identified "critical functions" to allow for proper testing and evaluation of controls. This condition exists because for the last two years NPOL planned to revise NARA Directive 114, *Management Controls*, which NARA's Management Control Liaison believed upon implementation by the program offices, would be the first step in addressing the open recommendations from the prior two years. At the end of fieldwork, the directive had not been revised by NPOL.

Our recommendations for the last two years were as follows:

- the Archivist should ensure NARA's policy on internal controls (such as NARA 114) be revised to specifically address the process by which findings are evaluated and categorized; criteria used in the decision making process, and; documentation necessary to support such conclusions;
- the Assistant Archivist for Administrative Services should ensure Annual Information Security Self Inspection results are reviewed in a timely manner, instances of non-compliance are identified, and corrective actions are monitored; and self inspections are reviewed and documented in accordance with guidance concerning self-assessments contained in NARA 114. If a formal process as referred to by the Information Security Officer is not completed, alternate means of reviewing the checklists should be developed.
- the Assistant Archivist for Regional Records Services should ensure all program findings, regardless of whether they are considered major or minor, are tracked to resolution and supported by adequate documentation;
- NPOL work with offices in general, and management control liaisons in particular, to:
    - stress the importance of performing internal control assessments of critical areas in accordance with management control plans and NARA 114;
    - ensure the results of the assessments are included in the assurance statements, and;
    - revise, as necessary, the lists of "critical functions" to be reviewed.

The Circular requires the agency and individual managers to take systematic and proactive measures to assess the adequacy of internal controls in Federal programs and operations, identify needed improvements, take corresponding corrective action, and report annually on internal controls in order to be accountable for their area of control.

[3] OIG Audit Report No, 08-06, Evaluation of NARA's FY 2007 Management Control Program (March 7, 2008). The recommendations in 08-06 were closed and carried forward to OIG Report No. 09-14.
[4] OIG Audit Report No. 09-14, Evaluation of NARA's FY 2008 Management Control Program (August 28, 2009).

NARA Directive 114 provides guidance for establishing, assessing, correcting, and reporting on internal controls. Both documents convey the elements necessary for conducting and documenting sufficient internal control reviews.

Failing to consistently review critical areas/programs weakens management accountability and decreases the likelihood problems will be identified and program risks minimized. Furthermore, it promotes a false sense of assurance about the level of program or function oversight provided by management and could result in an agency assurance statement which inaccurately conveys risk.

Recommendation 2

The Archivist, Assistant Archivist for Administrative Services, Assistant Archivist for Regional Records Services, and Director of Policy and Planning should ensure recommendations from OIG Report No. 09-14 are implemented and previously identified weaknesses are corrected.

Management Response

Management concurred with recommendation.

Appendix A – OIG Review of NARA's FY 2009 Statement of Assurance

National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

Date : October 20, 2009

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

Subject : Review of NARA's FY 2009 Statement of Assurance (FMFIA)

To : Adrienne Thomas, Acting Archivist of the United States

Based upon our examination of NARA's FY 2009 Federal Manager's Financial Integrity Act (FMFIA) statement and our preliminary assessment of NARA's internal controls for FY 2009, we do not agree with the agency assurance statement for Section 2 of the (FMFIA) reporting requirements. We disagree because, just as it has the prior two years, the agency underreports material risks associated with NARA's Preservation and Processing programs and does not accurately reflect the breadth of risks in NARA's Information Security Program. This underreporting of risk reflects a fundamental misunderstanding of the term Material Weakness and the agency's lack of understanding of risk management and internal controls.

In FY 2009 the agency has chosen to categorize both Preservation and Processing as significant deficiencies and therefore excluded them from their FMFIA statement. This extends a decision made in FY 2007 to downgrade these areas from Material Weaknesses, a decision with which the OIG has never agreed. While the agency has made progress in putting controls into place, work remains to be done in addressing outstanding audit recommendations and extensive backlogs persist.

Additionally, this year the agency chose to downgrade its IT Material Weakness, which was solely based on the PRISMA review performed in 2007, to a significant deficiency. In our review and evaluation of NARA's FY 2007 assurance statement we concluded the IT Security Material Weakness was too narrowly defined. In our response the OIG cited nine additional areas where critical security weaknesses were identified through audit work which we believed needed to be addressed before the IT Security Material Weakness could be considered remedied. This year the agency reported that due to significant accomplishments over the last two years IT Security would no longer be included as a Material Weakness and instead would be tracked as a significant deficiency starting in FY 2010. As we have previously stated, we believe the IT Security Material Weakness is predicated on more than just the results of the PRISMA review. Furthermore, in FY 2009 we reviewed documentation provided by NH of their actions to address the PRISMA recommendations and found that sufficient action had been taken on only 2 of 34 recommendations. Therefore, we do not believe sufficient progress has been made and IT Security should remain a Material Weakness.

This year the agency identified a new Material Weakness associated with IT implementation of PII protections. Based on OIG work in this area we agree with and fully support the designation of a Material Weakness in this area.

National Archives and Records Administration

NARA's Preservation Program

The OIG believes the agency should continue to identify a Material Weakness associated with its Preservation Program. We predicate this on several factors:

- Although NARA treated over 57,000 cubic feet of records in FY 2009, the percent of holdings identified as "at risk" remained steady at just under 65%. This represents a significant volume of records awaiting preservation action. The backlog represents a material constraint on NARA's ability to successfully achieve its mission.
- There does not appear to be consistent application or use of preservation information captured in NL, NR, and NW to guide either office-wide or agency-wide decisions on resource requests and allocations.
- Recommendations resulting from preservation program reviews are not tracked by the unit being reviewed or the NW office conducting the review.

NARA's Processing Program

The FY 2009 assurance statement did not report the processing of records accessioned into NARA as a material weakness. Our audit in this area defined that NARA was materially constrained in its ability to provide efficient and effective access to, and information about, NARA holdings. This affected NARA's ability to meet its mission of ensuring public access to records as soon as legally possible. This condition resulted in large backlogs of inadequately processed records and records awaiting adequate description and entry into the Archival Research Catalog (ARC). NARA management was aware of the backlogs, having initiated a study known as the Workload Analysis Study (WAS) that revealed the enormity of the processing backlog in textual records. NARA has made progress in the processing of textual records, reducing the backlog from 70% of holdings in FY 2008 to 60% in FY 2009. However, the majority of NARA textual records remain inadequately processed, posing an obstacle to their efficient and effective use.

In FY 2009, NR joined NW in developing a processing plan aimed at reducing their respective processing backlog. However, NL has not yet submitted to the OIG a processing plan for reducing their processing backlog. Additionally, the OIG has not been provided with evidence that processing plans are regularly monitored and adjusted as necessary and recommendations from the OIG report, aimed at remedying identified weaknesses, remain open.

NARA's IT Security Program

In our response to NARA's FY 2007 assurance statement we stated we believed management was too narrowly defining the IT Security Material Weakness by citing the results of the PRISMA review as the sole basis for the weakness. We identified nine additional IT Security related areas, identified through the course of the year by our office, or the work of outside entities, which we believed needed to be addressed before the Material Weakness could be considered resolved. In FY 2009 we received additional information from NH in support of action taken to address PRISMA related findings. We reviewed this information and found it supported closing only two of the thirty-four PRISMA review related recommendations.

Additionally, most of the IT Security recommendations contained in our FY 2007 FISMA audit remain open, and subsequent FISMA reviews continue to identify weaknesses associated with NARA's IT Security Program. The nine additional IT Security related areas first identified in FY 2007 are:

1. **Information Technology Refresh** - The ability to provide a secure computing environment for the agency's computer network users may soon be hindered, because NARA management has done no planning for the migration of its Novell Netware operating system to another type of software, even though Novell announced it is phasing out this operating system. As a result, future security vulnerabilities will pose a greater risk under the current system due to the lack of available patches and vendor support. In February 2005, Novell released Netware 7.0, Open Enterprise Server (OES), a product aimed at helping its Netware customers move to Linux. At that time, we recommended management immediately begin planning for the migration from Novell Netware to another type of operating system software, e.g., Microsoft or Linux. Although they initially agreed with us, management officials subsequently non-concurred with our recommendation, stating NARA has identified no business need to immediately begin planning a migration from Novell Netware to another type of operating system. NH intends to upgrade its operating system in FY 2010.

2. **Computer Security Incident Response Capability (CSIRC) -** NARA officials have not established 24 hours per day, 7 days per week computer security incident response capability (CSIRC) that can react quickly to investigate, contain, and mitigate security incidents. While portions of the CIRT have responded to actual incidents the full team has not been assembled. In addition, no testing of the Computer Incident Response Team (CIRT) has been performed to see if it functions in an efficient and effective manner. Finally, post incident activities, i.e., holding lessons learned meetings and preparing follow-up reports, have not been conducted, in accordance with the guidance in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, *Computer Security Incident Handling Guide*. Management concurred with recommendations related to these issues in FY 2008, however these recommendations currently remain open.

3. **Contingency Planning/Disaster Recovery -** NARA's recovery strategy of failing-to-paper for quickly and effectively restoring its mission critical IT systems after a severe service disruption or disaster is inadequate because the strategy (a) is not in sync with requirements of the Contingency Plans prepared for the mission critical IT systems; (b) is not in keeping with the President's initiative of an expanded electronic government and the Government Paperwork Elimination Act (GPEA); and (c) will not enable NARA to satisfy its customers' needs in a timely manner, i.e., providing ready access to evidence documenting the rights of American citizens, the actions of Federal officials, and the national experience. In prior years, the testing of contingency plans, to confirm the accuracy of the individual recovery procedures and overall effectiveness of the plan, was inadequate. In FY 2008 and FY 2009, NH officials took positive steps towards improving the contingency planning/disaster recovery of NARA systems. In FY 2009 NARA completed its Business Impact Analysis project, which identified NARA's critical business processes and the systems supporting those processes. Also, in FY 2009, NARA officials improved the contingency plan testing for most systems. However, since contingency

plans have not been updated to reflect changes identified by the BIA project and contingency plan testing, this remains a material weakness.

4. Certification and Accreditation (C&A) Process - The C&A process continues to deviate from NARA procedures. System Security Plans are incomplete, i.e., the plans do not contain all the information necessary for the Certification Authority and the Designated Approving Authority to make an informed, risk-based decision about the system. Assessment of security controls as part of the C&A process needs to be strengthened to ensure assessment procedures detailed in the test plans are followed. Current testing performed does not provide assurance that controls are in place and operating as intended. Management concurred with recommendations related to these issues, first identified in FY 2003, however these recommendations currently remain open.

5. Disk Space Utilization - Valuable disk drive space that could be used to store business-related data is taken up by inappropriate data, i.e., potentially inappropriate media files were stored on the servers (e.g. copyrighted material, movies, music files). While NARA has guidance concerning the appropriate use of office equipment it does not consistently test these controls to ensure compliance.

6. Unmanaged Devices - Unmanaged network devices, such as hubs and multifunction copiers, are connected to the agency's computer network, resulting in the potential for severe performance and security issues.

7. Network Printer Configuration - Network printers pose significant security vulnerabilities because they are not properly configured, i.e., the printers allow unauthenticated administrator changes (no passwords were used); accept telnet and file transfer protocol (FTP) connections; and run unnecessary services such as ping and chargen.

8. Audit Trails - The computer network Novell servers do not have the auditing function turned on. Failure to create, maintain, and protect audit records could allow unauthorized activities to go undetected and prevent the reconstruction of events; result in the failure to detect security violations and prevent further damage to the system; impede the investigation of security incidents; and hamper the ability to troubleshoot system problems.

9. Network User Accounts - Controls are not adequate to ensure NARANET Account Management policies and procedures are consistent with best practices. Management relies on the annual security awareness training process to recertify accounts and determine if users still require system access. Because this process occurs only once per year, this process does not ensure that accounts are removed or disabled in a timely manner. Also this process only covers individuals with login abilities and does not cover accounts that have not been assigned to a specific individual (for example backup accounts, test accounts, and training accounts). Also, inactive accounts are not consistently disabled or removed in a timely manner. In addition, NARANET's maximum password age requirement is not consistent with industry best practices and is ineffective. NARA management has not implemented adequate access controls for their network. 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.

Should you have any questions please contact me (ext. 71532) or James Springs (ext. 73018).

PAUL BRACHFELD
Inspector General

Appendix B – Acronyms and Abbreviations

FMFIA	Federal Managers' Financial Integrity Act
GAO	Government Accountability Office
NARA	National Archives and Records Administration
NPOL	Policy and Planning Staff
OIG	Office of Inspector General
OMB	Office of Management and Budget
PAR	Performance and Accountability Report
The Circular	Circular A-123, Management's Responsibility for Internal Control
The Standards	Standards for Internal Control in the Federal Government

Appendix C – Management's Response to the Report

National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

Date: SEP 27 2010

To: Paul Brachfeld,
Inspector General

From: David S. Ferriero
Archivist of the United States

Subject: Comments on Draft Audit Report 10-19, Audit of NARA's Internal Control Program

Thank you for the opportunity to comment on the above draft audit report. We appreciate the recognition given to efforts during FY 2009, and the acknowledgment that we are moving in the right direction in complying with OMB Circular A-123. We concur with the two recommendations in the draft report and will prepare an action plan to satisfy both.

As part of the reorganization proposed by our Transformation Task Force, internal controls and risk management are being given more prominence and credibility in a Performance and Accountability staff office. Through this office, we will continue our work to roll out an enterprise wide internal controls program that ensures responsibility and accountability for NARA's lines of business, and uses risk assessment as an integral part of managing and monitoring internal controls. We believe this work will result in an increased emphasis on, and appreciation of, internal control and risk management throughout the organization.

If you have any questions concerning these comments, please contact Mary Drak via email at mary.drak@nara.gov or by phone at 301-837-1668.

David S. Ferriero
Archivist of the United States

Appendix D – Report Distribution List

Archivist of the United States
Deputy Archivist of the United States
Assistant Archivist, Office of Administration Services (NA)
Assistant Archivist, Office of Regional Records Services (NR)
Director, Policy and Planning (NPOL)
Chief of Staff
Management Control Liaison, Policy and Planning (NPOL)