Executive Summary

The Federal Managers' Financial Integrity Act (FMFIA) of 1982 (Public Law 97-255) requires ongoing evaluations and reports of the adequacy of internal accounting and administrative control of each executive agency. The Act requires the head of each agency to annually prepare a statement on the adequacy of the agency's systems of internal accounting and administrative control. Office of Management and Budget (OMB) Circular A-123 (Revised), Management's Responsibility for Internal Control, contains guidance for implementing FMFIA. OMB A-123 requires management to annually report on internal control in its Performance and Accountability Report (PAR), including a report on identified material weaknesses and corrective actions. It also provides that the agency head, in preparing the annual assurance statement, should consider input from the Office of Inspector General.

Annually, the OIG performs a review to ensure agency 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 FMFIA.

Our initial assessment of the agency's FY 2007 assurance statement, as conveyed in our October 23, 2007 memorandum (See Attachment A), was that the statement was inaccurate and underreported risk associated with NARA's Preservation and Processing programs.

Subsequently, we performed a detailed review of individual office assurance statements and found inconsistencies in conducting and reporting internal control reviews. We found many of the staff offices did not conduct formal internal control evaluations in accordance with their internal control plans, while other offices did not maintain documentation of such reviews in accordance with agency guidance. This was the result of a lack of familiarity with NARA 114, an incomplete understanding of internal controls, and management control plans which were improperly or too narrowly scoped. As a result of a lack of, improperly documented, or improperly scoped internal control reviews, NARA lacks assurance risks are adequately identified and managed appropriately.

We are making 3 recommendations we believe will address the identified weaknesses.

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, 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 Circular A-123 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 performing an A-127 review and 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 OMB A-123. 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.

Objectives, Scope, and Methodology

The purpose of our evaluation was to determine the extent to which there is sufficient evidence NARA complied with the requirements of the FMFIA, OMB Circular A-123, and NARA 114, to support the Archivist's fiscal year 2007 assurance statement to the President and Congress. Specifically, our objectives were to (1) assess whether management is continually and consistently reviewing critical areas, and (2) verify the

accuracy of information contained in management's assurance statements to the Archivist.

To accomplish our objective, we examined the assurance statements and related internal control evaluation documents submitted by NARA office heads, reviewed additional supporting documentation maintained by the offices, and met with management control liaisons and other management officials. We performed a detailed review of the assurance statements and management control plans for the five major program offices (e.g. NA, NH, NL, NR, and NW), sub offices (e.g. NAA, NAF, NAS), and staff offices (e.g. ISOO, NEEO, NGC). Specifically, we

- reviewed the related evaluation files to assess the timeliness and adequacy of actions planned and taken in response to recommendations from evaluations completed in both the current and previous fiscal years;
- compared information in the evaluation files to the assurance statements to assess the accuracy of information reported in the assurance statements;
- reviewed sub-office (e.g. NAF, NAR, NAS, etc.) assurance statements to determine if the next higher level of management was performing a sufficient review of information passed up to them, and;
- reviewed management's evaluation of controls in accordance with each office's Management Control Plan for FY 2007 and agency guidance concerning the conduct of such evaluations.

To facilitate the submission of NARA's annual assurance statement we performed a preliminary review of the agency assurance statement in October 2007.

This audit was conducted in accordance with generally accepted government auditing standards (GAGAS) between October 2007 and January 2008. 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.

Critical Areas were not Consistently Reviewed

Our review revealed several staff offices did not conduct internal control reviews of critical functions in accordance with their management control plan. This was the result of a lack of familiarity with, and understanding of, proper internal control testing such as is required by OMB A-123 and further defined in NARA 114; and in some cases critical functions that were too narrowly defined to allow proper testing. Furthermore, individuals responsible for reviewing the results of these management control reviews conducted by sub-offices did not question the absence of such information. OMB Circular A-123 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. NARA Directive 114, establishes NARA policy for implementing the requirements of

OMB A-123. Both documents convey the elements necessary for conducting and documenting sufficient internal control reviews. The absence of internal control reviews decreases the likelihood significant risks or weaknesses are identified and properly managed and increases the likelihood the agency's assurance statement is inaccurate.

We found several staff and sub-offices were not conducting internal control reviews of critical functions as identified in their management control plan. Several staff offices, and some sub-offices, were unable to provide us with supporting documentation necessary to establish internal control reviews were being performed. In some cases we were told such reviews were being conducted "informally" or through the course of daily operations and therefore were not specifically documented. In other cases management control liaisons and managers cited confusion as to what constituted an internal control review and unfamiliarity with guidance contained in OMB A-123 and NARA 114. In the case of some of the smaller offices we found critical functions were narrowly defined, more analogous to work processes, hindering the risk assessment and evaluation process.

Internal controls – organization, policies, and procedures – are tools that help program and financial managers achieve results and safeguard the integrity of their programs. Internal controls provide a means of managing the risk associated with Federal programs and operations and require managers to define the control environment (e.g. programs, operations) and then perform risk assessments to identify the most significant areas within that environment in which to place or enhance controls. Management should have a clear, organized strategy with well defined documentation processes containing an audit trail, verifiable results, and specify document retention periods. NARA 114 provides guidance on the types of reviews which can be considered internal control reviews and the documentation required to support such reviews. It requires information created as a result of assessing, correcting, and reporting on internal controls to be maintained in accordance with the NARA Maintenance and Records Disposition Manual (Files 203), item number 220 – Management Control Evaluation Files; and documentation assessing risk to be maintained under item number 219 – Risk Assessment Files.

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.

Critical Area Reviews are not Documented in Accordance with NARA Policy

The OIG found two offices were not properly documenting critical area reviews listed in their management control plan. This condition was attributed to a lack of understanding of, or familiarity with, NARA 114, which specifically addresses the requirements for conducting and documenting internal control assessments. Specifically we found two program offices were not documenting the review of unit self-assessments by a higher level of management.

As a result, information necessary to "close the loop" of the review process, such as review results and corrective actions, was absent from the process.

NARA 114, establishes policy for improving the accountability and effectiveness of NARA programs and operations by establishing, assessing, correcting, and reporting on management controls. Furthermore, subparagraph 6 of the guidance states that internal control assessments must be documented in writing and provide the following information:

- A description of the operation or activity reviewed and the method of testing or examining existing management controls;
- A notation of the date(s) and place(s) the review was conducted and name(s) of the reviewer(s) and program staff involved with the review;
- A statement of the results of the review;
- A statement of the necessary corrective action(s) for any deficiencies found, and;
- Documentation that the review or results of the review were reported to the next level of management.

For self-assessments, NARA 114 requires a party outside a reporting unit who has knowledge of the unit's operations (e.g. a higher level manager or the management control liaison) must evaluate the self-assessment findings and provide the assessed unit with written notice of concurrence or disagreement with the findings and any recommended corrective action.

Without a properly documented review neither the Archivist nor the OIG can (1) determine whether appropriate controls were properly tested, and (2) place reliance on these aspects of the component offices assurance statements.

Recommendation 1. NPOL should stress to management the importance of performing internal control assessments of their critical areas in accordance with their management control plans. This includes ensuring reviews are documented in accordance with NARA 114.6. Management control liaisons and upper managers should be reminded of their responsibility for reviewing sub-office and sub-unit assurance statements and ensuring internal control reviews are conducted and documented.

Management Response

Management concurred with our recommendation.

Recommendation 2. NPOL should revise NARA 114 to require the results of internal control reviews, conducted in accordance with each offices management control plan, be included in each offices assurance statement.

Management Response

Management concurred with our recommendation.

Recommendation 3. The NARA management control liaison should work with the offices and office management control liaisons to review, and revise as necessary, the "critical functions" contained in the management control plans. The revision to these plans should seek to identify and rank risks to major program and functional areas and undertake internal control reviews of major risk areas.

Management Response

Management concurred with our recommendation.

National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

Date : October 23, 2007

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

Subject : Review of NARA's FY 2007 Statement of Assurance

To : Allen Weinstein, Archivist of the United States

Based upon our examination of the subject draft letter and our preliminary assessment of NARA's Management Control Program for fiscal year 2007, we do not agree with the assurance statement for Section 2 of the Federal Manager's Financial Integrity Act (FMFIA) report requirements. We disagree with the letter because it does not reflect material risks identified by the OIG in NARA's Preservation and Processing programs nor does it accurately reflect risks in NARA's Information Security Program.

Preservation Program

NARA' FY 2007 assurance statement reported the Preservation Program material weakness, identified by the OIG in FY 2005, as a reportable condition. Based on our review, NARA has not done sufficient work to minimize the risks found in our report to a reportable condition. Our report identified that: a) items needing preservation have not been identified; b) budget and staffing is inadequate to address preservation needs in a timely manner; c) criteria for assessing preservation need is not consistently applied; d) archival storage facilities are not in compliance with storage standards; and e) preservation performance measurement data is incorrect.

In 2007 NARA refined the methodology and criteria for identifying items needing preservation. However there has not been sufficient time to evaluate whether the new methodology is effective in surveying, identifying, documenting and ranking NARA records needing preservation.

Also, in FY 2007 NARA began updating its preservation at-risk list on an on-going basis instead of once a year. This will increase NARA's backlog of items needing preservation. Management has defined that 71 percent of current items at NARA needs some form of Preservation. Our audit report identified that NARA currently has a backlog of items needing preservation that would take 21 years to complete. Increasing the number of items on the at-risk list will result in NARA taking more than 21 years to

complete the backlog given that the resource levels in preservation have remained relatively static.

NARA has requested additional funding for the Preservation Program but the agency has not received the required funding for the Preservation Program. Until NARA is able to secure additional funding, the backlog of items on the preservation at-risk list will continue to grow rather then be addressed. NARA management recognizes this problem and has changed the performance measure for preservation of holdings to "by 2016, less than 50 percent of archival holdings require preservation action."

Furthermore facilities that hold NARA's permanent records do not meet the Archival Storage Standards which has implications for the preservation of holdings. NARA has included some of its facilities on the Capital Improvements Plan to be funded with new appropriations. NARA management acknowledges the deficiencies in the facilities and has changed the completion dates to have all the facilities compliant with the standards from FY 2009 to FY 2016.

In conclusion, the material risks identified by the OIG in the FY 2005 report still exist and have not been mitigated to the level of a reportable condition. While NARA has continued to initiate improvement efforts in FY 2007, management has not implemented sufficient controls and is not in the position to ensure all items needing preservation are managed and preserved in a timely manner. Therefore NARA records are at risk of lost and the Preservation Program for FY 2007 should still be reported as a material weakness.

Processing Program

The FY 2007 assurance statement did not report the processing of records accessioned into NARA as a material weakness. Based on our audit of this area, NARA is materially constrained in its ability to provide efficient and effective access to, and information about, NARA holdings. This affects NARA's ability to meet its mission of ensuring public access to records as soon as legally possible. This condition is the result of large backlogs of inadequately processed records and records awaiting adequate description and entry into the Archival Research Catalog (ARC). NARA management is 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.

This study of processing found that only 36 percent of textual holdings are adequately processed (i.e., ready for efficient and effective use by the public), meaning that 1.85 million cubic feet of records require additional processing to be considered appropriately processed. The study places the cost for complete processing of these records at a staggering $1.57 billion. Additionally, our review of Performance Management and

Reporting System (PMRS) statistics show that just over half of NARA's traditional holdings are described in ARC. While this meets NARA's strategic goal of having 50 percent of traditional archival holdings described in an online catalog, it still leaves more than 1.6 million cubic feet of traditional archival holdings not described in ARC, making it more difficult for the public to learn about and use these holdings.

In April 2007 management submitted an action plan to our office and indicated that recommendations 1a – 1c were closed. We reviewed the plan and supporting documentation and did not concur that the recommendations were closed. In May 2007 we requested additional documentation from the Office of Policy and Planning (NPOL) which might explain the basis for closing these recommendations. We did not receive a response from NPOL. In this same communication we defined what additional actions we viewed as necessary to successfully implement the recommendations in order to close them out. We consider successful implementation of the recommendations contained in the processing audit report a key component in establishing adequate internal controls and essential to our consideration as to whether the processing of accessioned records can be reduced from the category of Material Weakness.

As a result the Processing program should be defined as a material weakness in your FY 2007 assurance statement.

Information Security Program

In the area of information security, your assurance statement indicated that IT security was being reported as a material weakness based on weaknesses identified in a fourth quarter internal review done by a NH contractor which mirrored many of the OIG findings to date. Specifically, according to your assurance statement the review identified the following areas for inclusion in the material weakness: strengthening processes written policies, improving communication and training for business owners regarding their roles and responsibilities with respect to IT systems, and improving the quality assurance processes for the IT Security Program. However, the language in the transmittal omits the breadth of critical security weaknesses identified in OIG audit reports, specifically:

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 that 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 that 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 that NARA has identified no business need to immediately begin planning a migration from Novell Netware to another type of operating system.

2. Computer Security Incident Response Capability (CSIRC) - NARA officials have not established a 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. No testing has been performed to ensure that the Computer Incident Response Team (CIRT) will function in the most efficient and effective manner possible. 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.

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 that documents the rights of American citizens, the actions of Federal officials, and the national experience. Testing of the contingency plans, to confirm the accuracy of the individual recovery procedures and the overall effectiveness of the plan, was inadequate.

4. Certification and Accreditation (C&A) Process - 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. The preparation of Plans of Action and Milestones (POA&Ms) requires improvement, to provide management with the necessary information for ensuring that system threats and vulnerabilities are accurately identified and properly mitigated or accepted.

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, in violation of the provisions of NARA 802 and, possibly, U.S. copyright laws.

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 - Critical security controls for protecting the confidentiality, integrity, and availability of NARA's IT systems and information were bypassed, because NARA officials do not always follow NIST and agency guidance when establishing new user accounts at the Presidential libraries. Some users had not completed security awareness training before they were granted access to the network. It is important for a new user to understand the basic purpose of the Information Security Program and its implementation, before IT system access is granted. New accounts were created without the required submittal of a New User Request Form. As a result, there was no documentation available to identify who requested the new account and who approved the request. A required Background Investigation, i.e., authentication of an individual's identity, was not always conducted before network access was granted. An accurate determination of identity is needed to make sound access control decisions.

These risk areas, which led us to report IT Security as a material weakness last period, still persist and have not been mitigated. Therefore they should be added to the current IT Security material weakness in your FY 2007 assurance statement.

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

[Signature]

PAUL BRACHFELD
Inspector General

National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

Date: March 6, 2008

To: OIG

From: NPOL

Subject: Comments on OIG Draft Report 08-06,
Evaluation of NARA's Management Control Program for FY 2007

Thank you for the opportunity to comment on this draft report. We also appreciate the time spent by the auditor to work with us regarding concerns in the original version of this draft report. We concur with the three recommendations in the draft report and will proceed with an action plan to address them.

Susan M. Ashtianie
Director
Policy and Planning Staff

National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

Date: March 6, 2008

To: OIG

From: NPOL

Subject: Comments on OIG Draft Report 08-06,
Evaluation of NARA's Management Control Program for FY 2007

Thank you for the opportunity to comment on this draft report. We also appreciate the time spent by the auditor to work with us regarding concerns in the original version of this draft report. We concur with the three recommendations in the draft report and will proceed with an action plan to address them.

Susan M. Ashtianie
Director
Policy and Planning Staff

ATTACHMENT B