SECTION 4
OTHER ACCOMPANYING INFORMATION

INSPECTOR GENERAL'S ASSESSMENT OF MANAGEMENT CHALLENGES FACING NARA

Under the authority of the Inspector General Act, the NARA OIG conducts and supervises independent audits, investigations, and other reviews to promote economy, efficiency, and effectiveness and to prevent and detect fraud, waste, and mismanagement. To fulfill that mission and help NARA achieve its strategic goals, we have aligned our programs to focus on areas that we believe represent the agency's most significant challenges. We have identified those areas as NARA's top ten management challenges and have identified the related audits, investigations, and reviews that were performed in FY 2007.

1. Electronic Records Archives (ERA)

NARA's challenge is to build a system that will accommodate past, present, and future formats of electronic records. The ERA Program did not meet its September 2007 goal of producing an initial operating capability for ERA with planned incremental improvements that will eventually result in full system capability. Instead, the ERA program has experienced delivery delays, cost overruns and staffing shake-ups. The success of this mission critical program is uncertain. The challenge will be to deliver and maintain a functional ERA system that will preserve electronic records for as long as needed.

> *Audits, investigations, and reviews performed in FY 2007:*
> - Management Letter relating to the Independent and Objective Oversight of the Electronic Records Archive Program

2. Electronic Records Management (ERM)

NARA directs the Electronic Records Management (ERM) initiative, one of 24 Government-wide initiatives. The ERM initiative will provide guidance to agencies in managing and transferring to NARA, in an increasing variety of data types and formats, their permanent electronic records. NARA and its Government partners are challenged with determining how to manage electronic records, and how to make ERM and e-Government work more effectively.

3. Improving Records Management

Part of NARA's mission is to ensure that Federal officials and the American public have continuing access to records. NARA must work with Federal agencies to make scheduling, appraisal, and accessioning processes more effective and timely. The challenge is how best to accomplish this component of our overall mission and identify and react to agencies with critical records management needs.

> *Audits, investigations, and reviews performed in FY 2007:*
> - Audit of the Processing of Records Accessioned into NARA.

- Audit of Management Controls for Safeguarding NARA's Specially Protected Records and Artifacts (SPRA) Stored in Secured Stacks, Vaults, and Safes
- Investigation related to the Potential Compromise of Classified Material

4. Information Technology Security

Information technology security continues to present major challenges for NARA. The authenticity, reliability, and availability of our electronic records and information technology systems are only as good as our IT security infrastructure. Each year, the risks and challenges to IT security continue to evolve. NARA must ensure the security of its data and systems or risk undermining the agency's credibility and ability to carry out its mission.

Audits, investigations, and reviews performed in FY 2007:
- Review of Archives II File Server Disk-Space Utilization
- Review of Selected Security Aspects of NARA's Computer Network Environment
- Management Letter related to Contingency Planning for Information Technology Systems
- Investigation related to Computer Hacking

5. Expanding Public Access to Records

In a democracy, the records of its archives belong to its citizens. NARA's challenge is to more aggressively inform and educate our customers about the services we offer and the essential evidence to which we can provide access. Of critical importance is NARA's role in ensuring the timeliness and integrity of the process of declassifying classified material held at NARA.

Audits, investigations, and reviews performed in FY 2007:
- Audit of the Processing of Records Accessioned into NARA.
- Audit of Management Controls for Safeguarding NARA's Specially Protected Records and Artifacts (SPRA) Stored in Secured Stacks, Vaults, and Safes
- Investigation related to the Fraudulent Request for Veteran's Records

6. Meeting Storage Needs of Growing Quantities of Records

NARA-promulgated regulation 36 CFR Part 1228, "Disposition of Federal Records," Subpart K, "Facility Standards for Records Storage Facilities," requires all facilities that house Federal records to meet defined physical and environmental requirements by FY 2009. NARA's challenge is to ensure compliance with these regulations internally as well as by other agencies that house Federal records.

7. Preservation Needs of Records

The Archivist identified preservation as a reportable condition under the FMFIA reporting process in FY 2006. NARA cannot provide public access to records to support researchers' needs unless it can preserve them for as long as needed. As in the case of our national infrastructure (bridges, sewer systems, etc.), NARA holdings grow older

daily and are degrading. NARA is challenged to address this condition and related challenges.

8. Improving Project Management

Effective project management is essential to obtaining the right equipment and systems to accomplish NARA's mission. Complex and high dollar contracts require multiple program managers often with varying types of expertise. NARA is challenged with planning projects, developing adequately defined requirements, analysis and testing to support acquisition and deployment of the systems and oversight to ensure effective or efficient results within costs. These projects must be managed and tracked to ensure cost, schedule and performance goals are met.

9. Physical and Holdings Security

The Archivist has identified security of collections as a material weakness under the FMFIA reporting process. NARA must maintain adequate levels of security to ensure the safety and integrity of persons and holdings within our facilities. This is especially critical in light of the new realities that face this nation, post–September 11, and the risks that our holdings may be pilfered, defaced, or destroyed by fire or other natural disasters.

> *Audits, investigations, and reviews performed in FY 2007:*
> - Audit of Management Controls for Safeguarding NARA's Specially Protected Records and Artifacts (SPRA) Stored in Secured Stacks, Vaults, and Safes
> - Audit of Suitability Determination of Contract Employees
> - Investigation related to the Recovery of Stolen Passport Photographs
> - Investigation related to the Recovery of Robert E. Lee and W.D. Pender Letters
> - Investigation related to the Recovery of Bureau of Indian Affairs Record from Trash
> - Investigation related to the Recovery of Civil War Records
> - Investigation related to Contract Fraud/False Claims
> - Investigation related to the Recovery of Stolen Presidential Pardon
> - Investigation related to Security Violations in A1 Classified Research Room/SCIF

10. Strengthening Human Capital

The GAO has identified human capital as a Government-wide high risk. NARA's challenge is to adequately assess its human capital needs in order to effectively recruit, retain, and train people with the technological understanding and content knowledge that NARA needs for future success.

> *Audits, investigations, and reviews performed in FY 2007:*
> - Audit of Suitability Determination of Contract Employees
> - Investigation related to the Recovery of Civil War Records
> - Investigation related to the Recovery of Stolen Presidential Pardon

- Investigation related to Fraudulent Claim of Time Recorded on Time Sheets
- Investigation related to the Destruction of Government Property
- Investigation related to the Inappropriate Access to Classified Material

FEDERAL MANAGERS' FINANCIAL INTEGRITY ACT REPORT

National Archives and Records Administration

700 Pennsylvania Avenue, NW
Washington, DC 20408-0001

October 25, 2007

FY 2007 STATEMENT OF ASSURANCE

Managers of the National Archives and Records Administration (NARA) are responsible for establishing and maintaining effective internal controls and financial management systems that meet the objectives of the Federal Managers' Financial Integrity Act (FMFIA). I am able to provide a qualified statement of assurance that with the exception of two material weaknesses, NARA's internal controls are achieving their intended objectives:

(1) programs achieve their intended results;
(2) resources are used consistent with NARA's mission;
(3) programs and resources are protected from waste, fraud, and mismanagement;
(4) laws and regulations are followed; and
(5) reliable and timely information is obtained, maintained, reported, and used for decision making.

This assessment is based on results of audits and evaluations conducted by the Government Accountability Office (GAO), the Office of Government Ethics (OGE), NARA's Office of Inspector General (OIG), management control evaluations, and other written evaluations conducted in the 12 NARA offices and staff organizations. It is also based on senior management's knowledge gained from the daily operations of NARA programs and systems. I have also relied upon the advice of the Office of the Inspector General concerning this statement of assurance. Specific exceptions to this statement include material weaknesses in collections security and our IT security program as discussed in the following report. Efforts to fully resolve both material weaknesses are monitored by NARA's senior staff and results are reported directly to me.

ALLEN WEINSTEIN
Archivist of the United States

FY 2007 REPORT ON INTERNAL CONTROLS

Background on FMFIA requirements

The objective of the Federal Managers' Financial Integrity Act of 1982 (FMFIA) is to provide reasonable assurance that "(i) obligations and costs are in compliance with applicable law; (ii) funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation; and (iii) revenues and expenditures applicable to agency operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports and to maintain accountability over the assets."

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

NARA's internal controls objective noted in the Archivist's statement of assurance are consistent with FMFIA objectives.

The following tables reflect the number of material weaknesses reported by NARA under Section 2 of FMFIA in recent years.

NUMBER OF MATERIAL WEAKNESSES

	Number at Beginning of Fiscal Year	Number Corrected	Number Added	Number Remaining at End of Fiscal Year
FY 2004	2	0	0	2
FY 2005	2	1	1	2
FY 2006	2	1	0	1
FY 2007	1	0	1	2

EFFECTIVENESS OF INTERNAL CONTROL OVER OPERATIONS
Statement of Assurance: Qualified

Material Weakness	Beginning Balance	New	Resolved	Consolidated	Reassessed	Ending Balance
Collections Security	✓					
IT Security Program		✓				
Total Material Weaknesses	1	1				2

Continuing Improvements in NARA Collections Security

NARA reported a material weakness in collections security in FY 2001 based on investigative findings from our Office of Inspector General (OIG). As reported in prior years, corrective steps have been taken, and many actions have been completed. In FY 2006, NARA convened an intra-office Collections Security Working Group to address remaining issues. Improved collections security is an ongoing and high priority concern, which will result in continuing reduction of risk.

During 2007, the working group:

- identified employment screening policies in preparation for a review and assessment of practices in 2008
- prepared a standardized training program that will be implemented in 2008;
- improved physical security at facilities
- completed the establishment of special storage areas for "treasure" holdings
- instituted standard collection security checklists for program audits at all locations
- worked with the OIG to improve communications with the public regarding prevention and response

In FY 2008, NARA will conduct a comprehensive review of all corrective actions to date and reassess the status of this material weakness. We will also continue efforts in five critical areas:

- Employment screening,

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

- Staff training and monitoring,
- Security for records storage areas,
- Records control, and
- Theft preventions and response.

Improvement needed in the NARA IT Security Program

In the fourth quarter of FY 2007, NARA's Office of Information Services (NH) conducted an independent assessment of the IT security program using the Program Review for Information Security Management Assistance (PRISMA) methodology developed by the National Institute for Standards and Technology (NIST). The report of that assessment indicated that NARA's IT security program was functioning at a level of "partially compliant" in all areas tested, but warned that the program was overly dependent on the personnel implementing it, and was immature with respect to key processes.

Specifically, the assessment identified significant deficiencies in the areas of policy development, authorization, and communication of security responsibilities to system owners and other stakeholders. The assessment indicates that these deficiencies are rooted in the current level of staffing and resources, and are driving the over-dependency on the IT Security staff for implementation of the security program. The report points out that the dedication and proficiency of the security staff cannot substitute for the processes and procedures necessary to meet the security challenges on the immediate horizon. If not addressed, these deficiencies will limit the program's ability to mature to the level necessary to support future demands imposed by external mandates such as HSPD-12, or internal system development projects, such as the Electronic Records Archives.

These programmatic deficiencies, described in the PRISMA assessment, do not represent a technical risk to agency IT systems, the data they hold, or to the agency's external partners. However, the threshold condition for a significant deficiency is met by the report's conclusion that existing management resources are not sufficient to overcome the weaknesses that have been identified.

Because this issue is so recently defined, we do not yet have a detailed plan of corrective action. At a high level, we know that in FY 2008 we will address the following areas:

- 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.

Other Internal Control Weaknesses

In past FMFIA reports, NARA has included information on internal control weaknesses that we deemed to meet the criteria of a reportable condition. Although we are no longer required to do so in this report, we choose to include this information in FY 2007. In both cases noted below, NARA's Inspector General characterizes the weaknesses as material. The essence of the difference in our positions on the characterizations of the weaknesses in preservation and processing lies in two areas: we do not agree that the existence of a backlog or the lack of resources are indicators of a material weakness. Other agencies experience these conditions, a fact that was noted in the OIG's audit report on textual processing issued in February 2007. We have noted these areas in our ten-year Strategic Plan and have established annual performance measures. We do not concur with the OIG assessment of the severity of risk associated with either weakness.

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

Preservation Program

As a result of an OIG audit in FY 2005, NARA opened a material weakness related to its Preservation Program. Our FY 2006 FMFIA report noted that significant work against the original audit recommendations had been accomplished, and determined that the remaining issues no longer met the criteria for a material weakness. We constructed an action plan to address remaining issues and met all FY 2007 targets and milestones. We will continue to monitor this program in FY 2008. We do not agree with the OIG that additional time to test controls and a future audit are required to justify our decision to maintain this as a reportable condition.

Textual Processing

In FY 2006, NARA completed its own study of textual records processing to quantify the known backlog of textual records requiring processing to make them efficiently available to the public. NARA set a goal in its new 2006 Strategic Plan to address this backlog, which has been growing for decades, and we shifted resources in the Washington, DC, area in FY 2007 to apply more staffing to the problem. We included discussion of the backlog in our assessment of major challenges facing the agency in our FY 2006 and FY 2007 PARs. We do not consider this challenge to meet the criteria for a reportable condition or a material weakness. We know about the problem, are taking steps to address it, and are able to serve the records to the public despite their unprocessed status.

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

PROGRESS ON 2006 AUDIT RECOMMENDATIONS

The NARA Inspector General (OIG) contracted with Clifton Gunderson, LLP (CG) to audit financial statements as well as internal controls and operations. CG performed an audit of the consolidated financial statements of the National Archives and Records Administration as of September 30, 2006. In its final report dated November 3, 2006, CG reported certain matters involving the internal control and its operation two of these were considered to be reportable conditions and one of these was considered to be a material weakness. CG made 21 recommendations to correct these conditions. (The 2006 Independent Auditor's Report may be found beginning on page 103 of NARA's 2006 Performance and Accountability Report.)

Area 1: Information Technology (IT)

CG noted this area a material weakness and made 18 recommendations related to access controls, the entity-wide security program, system software, and contingency planning. They are:

1. Develop and utilize a script or command line to identify inactive network accounts that have been inactive for more than 90 days and disable them.

2. Institute a process of recertifying network accounts (including system administrators) and remote user access (which are not covered during an application user re-certification process).

3. User IDs (other than system ID) not associated with an individual or not designated for testing purposes should be deleted.

4. Develop a contractor exit checklist that will require formal sign-offs by functional managers. Additionally, the functional managers should indicate that the contractor's access be removed.

5. (a) Regularly recertify all physical access to sensitive NARA facilities, and (b) review agreements where contractors may act as an agent on behalf of NARA with third parties (e.g., Iron Mountain, etc.). (c) Documented evidence of these re-certifications should be maintained for future reference.

6. Enable account lockouts for the RCPBS application in accordance with NARA IT policies.

7. Maintain employee clearance records (Form 3009) for every separating employee.

8. Require supervisors of departing employees to ensure the Form 3009 is completed no later than an employee's last day of work.

9. Perform a risk assessment of the NARANET environment to identify risks posed by the upgrade on the NARANET system environment and controls.

10. Update the NARANET System Security Plan to reflect the current status of the system.

11. Develop a Plan of Actions and Milestones to address the risks identified within the updated NARANET risk assessment

12. Officially re-authorize the NARANET general support system to continue processing.

13. Background investigations should be immediately conducted on the four noted individuals.

14. (a) NARA should be conducting background investigations on new hires prior to accessing NARA systems, and (b) implement a process to independently validate on an annual basis that such investigations are being performed in a timely manner.

15. Document and implement patch management procedures for all Novell systems.

16. Implement the milestones and target dates identified in the Plan of Actions and Milestones (POA&M) to address the four open firewall weaknesses identified.

17. Revise the COOP to reflect systems/applications that are currently in use, and specifically identify mission critical applications and related vital files, records and databases necessary to restore essential functions

18. Revise the NARANET and NH disaster recovery plans to reflect the current Novell GroupWise environment, describe procedures to recover Novell GroupWise and identify the storage location of backup tapes (identified as essential material, data, record, or communication).

Through September 30, 2007, Clifton Gunderson has accepted documentation and closed recommendations 1, 2, 3, 5, 8, 9, 10, 11, 12, 13, 15, 16, and 18. Recommendations 4, 6, 7, 14, and 17 in this group will remain open in the upcoming report.

Area 2: Review of Obligations

CG noted this area a reportable condition and made 1 recommendation related to quarterly review of obligations.   That recommendation is:

19. Consistently implement the NARA Interim Guidance 400-6.

Clifton Gunderson has accepted documentation and closed this recommendation.

Area 3: Financial Reporting

20. Ensure that documentation supporting payroll transactions is properly maintained and readily available for examination.

21. Enforce the policy of signing and dating the Supervisor Time and Attendance Certification Report.

Clifton Gunderson has accepted documentation for recommendation 20 and closed it. Recommendation 21 will remain open in the upcoming management letter.