

APPENDIX A

## INSPECTOR GENERAL'S ASSESSMENT OF MANAGEMENT CHALLENGES FACING NARA

Under the authority of the Inspector General Act, the NARA Office of the Inspector General 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 2006.

### 1. Electronic Records Archives (ERA)

NARA's challenge is to build a system that will accommodate past, present, and future formats of electronic records. By September 2007, NARA plans to have initial operating capability for ERA with planned incremental improvements that will eventually result in full system capability. The challenge will be to deliver and maintain a functional ERA system that will preserve electronic records for as long as needed.

### 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

NARA's mission is to ensure that Federal officials and the American public have ready access to essential evidence. 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 2006:*

- Evaluation of NARA's Affiliated Archives Program
- 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 and reliability 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 2006:*

- Audit of NARA's Network Perimeter
- Review of Modifications Made to the Performance-Based Task Order for Information Technology Support Services (ITSS)
- Investigation related to the Compromise of the Case Management Reporting System server and the Presidential Electronic Records Library server
- Review of NARA's Information Security Program
- Audit of System Administrator Rights and Controls
- OIG Monitoring of the Novell Netware/GroupWise Upgrade Project

## **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 2006:*

- Evaluation of NARA's Affiliated Archives Program

## **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 material weakness under the FMFIA reporting process in FY 2005. 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.

*Audits, investigations and reviews performed in FY 2006:*

- Evaluation of NARA's Affiliated Archives Program

## **8. Improving Financial Management**

By inclusion under the Accountability of Tax Dollars Act of 2002, NARA is required to prepare audited financial statements in compliance with prescribed standards, subject to independent audit. NARA's challenge is to present timely, accurate, and useful financial

information for making day-to-day operating decisions supporting results-oriented management approaches and ensuring accountability on an ongoing basis.

*Audits, investigations and reviews performed in FY 2006:*

- Audit of NARA's Fiscal Year 2005 Financial Statements
- Evaluation of NARA's FY 2005 Management Control Program
- Management Letter related to Flawed Contract Performance Work Statement Could Have Adverse Impacts on NARA's Budgetary Resources

## **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 important 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 2006:*

- Review of NARA's Internal Control Procedures for Loan Items
- Management Letter related to Security over Holdings in Stack Areas
- Investigation related to Destruction of Federal Records
- Investigation related to the Recovery of Stolen G.E. Pickett Letter
- Investigation related to Mishandling and Improper Investigation of a Theft of Classified Documents
- Evaluation of NARA's Affiliated Archives Program
- Investigation related to possession of illicit drugs and potential firearms at Archives I
- Investigation related to inappropriate conduct during work hours

## **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 2006:*

- Investigation related to a threat against NARA employees
- Investigation related to possession of illicit drugs and potential firearms at Archives I
- Investigation related to inappropriate conduct during work hours
- Investigation relating to an NARA employee that forged a NARA employment reference letter

APPENDIX B  
**FEDERAL MANAGERS' FINANCIAL INTEGRITY ACT  
REPORT**



*National Archives and Records Administration*

700 Pennsylvania Avenue, NW  
Washington, DC 20408-0001

October 23, 2006

The President  
The White House  
Washington, DC 20500

Dear Mr. President:

Enclosed is the Federal Managers' Financial Integrity Act (Integrity Act) report for Fiscal Year 2006 for the National Archives and Records Administration (NARA).

Pursuant to Section 2 of the Integrity Act, we identified a material weakness in our collections security program in FY 2001. In FY 2005, we identified a weakness in our preservation program. We have made progress in our actions to remedy the collections security weakness, but still have substantive work to do before we can remove it as a material weakness. Significant work was completed in FY 2006 to improve internal controls for our preservation program. We are downgrading it from a material weakness to a reportable condition and will continue close monitoring of the program through our agency's risk review board. We are also declaring a new reportable condition related to Information Technology (IT) documentation and will use the agency's risk review board to monitor improvements to internal controls. The following enclosures detail these actions:

- Enclosure A provides statistical summaries of NARA compliance with the Integrity Act
- Enclosure B summarizes progress in collections security and provides FY 2007 milestones and target dates
- Enclosure C summarizes progress on preservation program controls
- Enclosure D describes the reportable condition regarding IT documentation

It is my informed judgment that there is reasonable assurance that NARA's management controls are achieving their intended objectives. This assessment is based on management control evaluations and other written evaluations conducted in the 12 NARA offices and staff organizations and 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.

Respectfully,

A handwritten signature in cursive script that reads "Allen Weinstein".

ALLEN WEINSTEIN  
Archivist of the United States

Enclosures (4)

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

**ENCLOSURE A**  
**STATISTICAL SUMMARY OF PERFORMANCE**

**Section 2. Management Controls**

Number of Material Weaknesses

	<u>Number reported for the first time in</u>	<u>For that year, number that has been corrected</u>	<u>For that year, number still pending</u>
Prior Years	6	5	1
2004 Report	0	0	1
2005 Report	1	0	2
2006 Report	0	1	1
Total	7	6	1

**Section 4. Financial Management Systems**

Number of Material Non-conformances

	<u>Number reported for the first time in:</u>	<u>For that year, number that has been corrected:</u>	<u>For that year, number still pending</u>
Prior Years	0	0	0
2004 Report	0	0	0
2005 Report	0	0	0
2006 Report	0	0	0
Total	0	0	0

A-1 and 2

**ENCLOSURE B**  
**DESCRIPTION OF MATERIAL WEAKNESS IN INTERNAL CONTROLS**  
 Collections Security

NARA reported a material weakness in collections security in FY 2001. 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.

**Title and Description of Material Weakness:** Collections security

**Name of Responsible Program Manager:** Thomas Mills, Assistant Archivist for Regional Records Services

**Source of Discovery:** OIG investigation

**Appropriation/Account:** 110

**Pace of Corrective Action**

**Year Identified:** FY 2001

**Targeted Correction Date:** FY 2007

**Action and Validation Process That Will Be Used**

NARA will take further action in these areas to address this material weakness:

- 1. Employment screening** (for all staff that have access to archival records)
  - Ensure agency-wide procedures that address suitability for employment are in place
- 2. Staff training and monitoring**
  - Offer initial and annual training on collections security
- 3. Security for records storage areas**
  - Address costs and benefits of potential new security measures
  - Implement an internal control mechanism to regularly review access controls
- 4. Records control**
  - Regional records operations will maintain a current listing of all identified specially protected records and artifacts (SPRAs) that are stored in cages, vaults, safes, and other areas within regional archives.
  - Ensure that annual inspections of SPRAs are conducted.
  - Ensure that annual inventories are performed by two staff members.
- 5. Theft prevention and response**
  - Conduct regular audits of collections security policies and practices

**Results Indicators:**

Major Milestones	Milestone Dates
a. Review, and revise as appropriate, existing guidance on employment screening to ensure that all categories of staff, contractors, interns, and volunteers whose job duties permit them access to non-public areas are adequately covered in the guidance.	Second quarter, FY 2007
b. Prepare holdings security briefing for agency wide use with new hires. Implement policy where this	

**National Archives and Records Administration**  
**Performance and Accountability Report, FY 2006**

briefing is conducted and documented within 30 days of hire.	Second quarter, FY 2007
c. Include annual staff refresher training in holdings security in agency-wide program unit work-plans	First quarter, FY 2007
d. Implement annual holdings security refresher training for staff, contractors, interns, volunteers, and other whose job duties provide access to non-public areas.	FY 2007
d. Program units agency-wide will document a review to ensure that local written policies for security in records storage areas are current. Documentation will include recommendations to strengthen local policies and intended actions where appropriate.	First quarter, FY 2007
e. Program units agency-wide will conduct an annual self-assessment as part of their management assurance protocols.	Third quarter, FY 2007
f. A collections security review will be incorporated into regular Physical and Life Safety Reviews. These reviews will cover at least 1 office of each major program area each year.	FY 2007
g. Program offices will include a collections security review as part of their formal program reviews. These reviews will cover at least 1 office of each major program areas each year.	FY 2007

**ENCLOSURE C**  
**DESCRIPTION OF MATERIAL WEAKNESS IN INTERNAL CONTROLS**

Preservation Program

NARA reported a material weakness in our preservation program in FY 2005. As noted below, significant works was done during FY 2006 to improve internal controls. We are downgrading this material weakness to a reportable condition for FY 2007 and will continue close monitoring of the program through our agency's risk review board.

**Title and Description of Material Weakness:** Preservation Program

**Name of Responsible Program Manager:** Michael J. Kurtz, Assistant Archivist for Records Services, Washington, DC

**Source of Discovery:** OIG audit and the Program Manager's assurance statement to the Archivist of the United States

**Appropriation/Account:** 110

**Pace of Corrective Action on Original Material Weakness**

**Year Identified:** FY 2005

**Original Targeted Correction Date:** FY 2007

**Status Change to Reportable Condition:** October 1, 2006

**Validation Process Used:** NARA has taken action in four areas to address this material weakness.

1. Identification of at-risk records
  - Refine risk assessment process  
NW, NR, NL and NWT have aligned the levels of risk and processes used to apply those criteria. The offices have created Risk Assessment Instructions and Definitions for all three offices.
  - Develop usage criteria that is standard across NARA program areas  
Differences in the usage criteria have been reconciled to ensure consistency.
  - Develop and implement staff training  
Training, to reflect consistency and changes in the at-risk criteria and integrated Instructions and Definitions, has been developed. This training will be provided during the first quarter of FY 2007.
2. Facilities standards
  - Create a Capital Improvements Plan  
NAS has completed a Capital Improvements Plan. This draft plan includes planned space changes to NARA-owned buildings such as renovations or expansions. All of this information will be further analyzed to determine funding priorities.
3. Performance Measurement
  - Develop a performance metric to track for medium- and low-risk projects  
NARA has developed a method to ensure that preservation work on medium- and low-risk projects is tracked.
4. Budget
  - Develop budgetary resources for baseline preservation requirements.  
NW, in cooperation with NR and NL, has identified budgetary resources required for preservation, and submitted budget initiatives for FY 2007 and FY 2008 budgets to the Archivist for consideration.

C-1



**Results Indicators:**

<b>Major Milestones</b>	<b>Milestone Dates</b>
Refine Risk Assessment Process	<b>COMPLETED:</b> April 30, 2006
Develop risk assessment usage criteria that are standard across NARA program areas.	<b>COMPLETED:</b> October 31, 2005
Develop and implement staff training for identification of at-risk records	<b>ON SCHEDULE:</b> October 31, 2006
Create a Capital Improvements Plan.	<b>COMPLETED:</b> August 1, 2006
Develop a performance metric to track medium- and low-risk.	<b>COMPLETED:</b> October 1, 2006
Develop budgetary resources for baseline preservation requirements for FY 2007 Budget Request	<b>COMPLETED:</b> September 16, 2005
Develop budgetary resources for baseline preservation requirements for FY 2008 Budget Request	<b>COMPLETED:</b> September 11, 2006

**ENCLOSURE D**  
**DESCRIPTION OF REPORTABLE CONDITION IN INTERNAL CONTROLS**  
Information Technology (IT) Documentation

**Title and Description of Reportable Condition:** Information Technology (IT) Documentation

In response to NARA's demonstrated progress since FY 2000, the OIG supported management's FY 2005 determination to remove IT security as a material weakness under provisions of FMFIA. Although the OIG has recommended that IT security be re-opened as a material weakness, we do not agree. We have found inconsistent levels of documentation within the IT Program, and believe that this constitutes a reportable condition in internal controls. An action plan will be devised and monitored internally by the NARA Risk Review Board.

The breadth of any IT program is enormous and touches an entire Federal agency. Another truth about IT is that it is the most rapidly changing aspect of how we do business. The scope of IT responsibilities is reflected in the intense work being done by the National Institute for Standards and Technology (NIST), which has been mandated by Congress to publish a compendium of computer security policy and guidance designed to assist Federal agencies in managing and securing their IT assets. The guidance documents are known as the "800 series" special publications.

Over the last two years especially, NIST has released a draft or final version of a major policy guidance every several months. The full set of the 800 series special publications is estimated to be greater than 10,000 pages, the majority of it recently published. In addition, NIST issued two Federal Information Processing Standards Publications (FIPS PUBS), which were mandated by FISMA and which require federal agencies to categorize all information systems and apply a recommended set of minimum security controls to those systems.

The NIST framework is distinguished by its primary criteria: that security measures be developed in a manner that is reasonable and appropriate to the business mission of the agency. The comprehensive and rigorous risk management approach to security is unique to the unclassified IT systems of the Federal Government, and has no parallel in private industry. While the guidance documents that support the FIPS requirements are superb in their own right, agencies are understandably hard-pressed to keep up with the tasks of interpreting the guidance as it is published, making the appropriate risk management decisions necessary to apply it in practice and documenting compliance with the underlying requirements. Management responsibility is further complicated by the novelty of the guidance, and even specialists with considerable computer security knowledge at the system level are "learning on the job" as the Government embraces this discipline of risk-management based IT security.

Revising old policy documentation and guidance to reflect new procedures and practices is the most time consuming and labor intensive part of this discipline, and it is in that area where agencies are most likely to fall behind. Nonetheless, proper documentation illuminates the intersection of the business mission and the expenditure of funds and resources to secure the assets needed to accomplish the mission, and is a critical element of the FISMA implementation project.

Recent NARA audit findings have highlighted numerous areas where IT documentation is lacking, out of date, or does not properly reflect the implementation decisions that are associated with requirements tied to FISMA, FMFIA, and other regulations that govern the acquisition and management of IT systems. Areas that are targeted for review and improvement include:

- Review and update of interim guidance and other policies in the 800 management series of directives
- Review and update of Capital Planning and Investment Control, Project Management, and Systems Development Lifecycle documentation
- System security documentation.

**Name of Responsible Program Manager:** Martha Morphy, Assistant Archivist for Information Services and Chief Information Officer.

D-1

**Source of Discovery:** Internal review and the Program Manager's assurance statement to the Archivist of the United States

**Appropriation/Account:** 110

**Pace of Corrective Action**

**Year Identified:** FY 2006

**Targeted Correction Date:** FY 2008

D-2

## APPENDIX C

### PROGRESS ON 2005 AUDIT RECOMMENDATIONS

The NARA Office of the 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, 2005. In its final report dated November 3, 2005, CG reported certain matters involving the internal control and its operation. One of these was considered to be a reportable condition and one of these was deemed a material weakness. CG made 25 recommendations to correct these conditions. (The 2005 Internal Auditor's Report may be found on page 108 of NARA's 2005 Performance and Accountability Report.)

#### ***Area 1: Investments***

CG noted this area a material weakness and made one recommendations related to NARA's method of reporting obligations and outlays of non-federal investments held for sale. That recommendation is:

1. Continue to pursue with U.S. Treasury USSGL groups the SGL transactions and accounting scenarios for accounting for investments in non-federal securities and specifically in mutual funds.

Through September 30, 2006, NARA has provided documentation to the OIG and CG to satisfy this recommendation.

#### ***Area 2: Information Technology (IT)***

CG noted this area a reportable condition and made 13 recommendations related to software development and change controls, NARA's entity-wide security program, controls to protect the agency's information, and the agency's contingency plan. They are:

1. Obtain proper approvals before moving RCPBS application changes into the production environment.
2. Document test plans and test results for all RCPBS application changes.
3. Maintain documentation of Employee Clearance Records for all departing employees, with clear identification of which system/application access has been removed.
4. Revise Plan of Action and Milestones (POA&M) to include all required components as dictated per OMB M-04-25 instructions.
5. Ensure all current and future Records Center Program Billing System (RCPBS) and PRISM application users have documentation indicating approved access by their supervisor and system owner.
6. Review password configurations of all NARA maintained (i.e., RCPBS and PRISM) applications and applications outsourced to the Bureau of the Public

Debt (BPD) to ensure passwords are implemented in accordance with specifications for password usage established by the National Institute of Standards and Technology in Federal Information Processing Standards Publication 112, PASSWORD USAGE, and NARA's IT Security Handbook.

7. Enforce Directive 804 and ensure that user access to all NARA (i.e., PRISM and RCPBS) and Bureau of the Public Debt (BPD) hosted applications are re-certified on a regular basis in a joint effort by NARA IT managers and system owners.
8. Review all individuals with access to the computer room, determine if access is needed to perform their job responsibilities, and remove any access not required on either a frequent or emergency basis.
9. Modify NARA's records system (NARS5) user permissions to restrict access to the DAU file to only those individuals who require this access in order to perform their position responsibilities.
10. Incorporate logging (of user activity and failed logon attempts) functionality within the NARS5 and PRISM applications to the extent configurable within the application. Implement a process to review these logs on a regular basis. Also, incorporate such logging and audit trails in the functional requirements/design/configuration of any replacement systems (i.e., hosted by NARA or the Bureau of the Public Debt (BPD)).
11. Ensure all NARA point of contacts (POC) for outsourced applications maintain an up-to-date documented listing of all NARA user names and permissions.
12. Implement manual or automated validation edits to ensure daily batch transaction data transferred from the NARS5 application to the RCPBS application are received completely and accurately.
13. NARA should update the agency COOP plan to reflect all business functions at each NARA location.

Through September 30, 2006, NARA has provided documentation to the OIG and CG to satisfy numbers 1, 2, 4, 6, 8, 9, and 12 above. Partial documentation has also been provided for numbers 5, 7, and 11 above.

### ***Area 3: Financial Reporting***

CG made three recommendations related to the general ledger (GL) system setup and posting model definition, review of obligations, and an integrated financial management system. They are:

1. Ensure that the GL system setup and posting model definition of the new service provider is in compliance with USSGL.
2. Develop a timetable that will permit the periodic timely review of obligations to meet the timelines established for external reporting in OMB Bulletin A-136, *Financial Reporting Requirements*.
3. Continue to evaluate the functional requirements to integrate the financial reporting, billing systems, property and equipment and a cost system with the

GL system and assess the degree of integration necessary to have a single, unified financial management system.

Through September 30, 2006, NARA has provided documentation to the OIG and CG to satisfy the above three recommendations.

#### ***Area 4: Property, Plant and Equipment (PPE)***

CG made three recommendations in this area. They are:

1. Finalize the policies and procedures for software development and completed software.
2. Track costs and maintain documentation related to the various software development phases to ensure compliance with Federal accounting capitalization standards..
3. Create a certification in-service document to evidence acceptance of the software by its owner and maintain the document as support for the depreciation start date.

Through September 30, 2006, NARA has provided partial documentation to the OIG and CG for numbers 1 and 2 above.

#### ***Area 5: Payroll***

CG made five recommendations in this area. They are:

1. Ensure that NARA's service provider(s) are in compliance with NARA's policy of maintaining appropriate supporting records for payroll deductions authorized by the employees and have them readily available for examination.
2. Enforce the policy of recording leave earned and used in ETAMS.
3. Ensure that documentation supporting payroll transactions is properly maintained and readily available for examination.
4. Enforce the policy of signing and dating the Supervisor Time and Attendance Certification Report.
5. Periodically review and reconcile payroll related records to ensure accuracy of information.

Through September 30, 2006, NARA has provided documentation to the OIG and CG to satisfy numbers 2 through 5 above.