APPENDIX A
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 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 10 management challenges. Under these are the related audits, investigations, and reviews that were performed in FY 2004.

1. Electronic Records Archives (ERA)

NARA, in research and development collaboration with national and international partners, is building an Electronic Records Archives (ERA) with the goal of ensuring the preservation of, and access to, Government electronic records. The pace of technological progress makes formats in which the records are stored obsolete within a few years, threatening to make them inaccessible even if they are preserved intact.

ERA is to be a comprehensive, systematic, and dynamic means of preserving virtually any kind of electronic record, free from dependence on any specific hardware or software. The ERA system is targeted to make it possible for Federal agencies to transfer any type or format of electronic record to the National Archives, so that citizens can locate records of interest and the National Archives can deliver these materials in a usable format.

NARA's challenge is to build a system that will accommodate past, present, and future formats of electronic records. To mitigate the risks associated with development and acquisition of an advanced electronic archival system, Congress directed NARA to reassess the ERA project schedule based on estimates of the amount of work and resources required to complete each task. Beginning on October 1, 2002, NARA was required to submit to Congress a quarterly report on the status of the project's schedule, budget, and expenditures as measured against a reported baseline; a prioritization of project risks and their mitigation efforts; and corrective actions taken to manage identified schedule slippage, cost overruns, or quality problems that might occur. By 2007, NARA plans to have initial operating capability for ERA with 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 one of 24 Government-wide initiatives, the Electronic Records Management (ERM) initiative. 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. For many years, Federal records were created on paper and stored in files and boxes with NARA. Now, electronic records are created by Gov-

ernment agencies at an astounding rate, challenging NARA to find ways to manage and preserve them. In 2002, NARA became a key player in e-Government and managing partner for the e-Government ERM initiative. E-Government is part of President Bush's management agenda aimed at making it easier for citizens to obtain high-quality service from the Federal Government while reducing the cost of delivering those services. During 2002, NARA enlisted partner agencies, developed a detailed plan for accomplishing its objectives, and issued the first guidance on transferring e-mail records to NARA.

NARA and its Government partners are challenged with trying to figure out how to manage electronic records in an electronic manner, 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. One way NARA addresses its mission is by assisting agencies with the management of their records from the time that those records are created. Without effective records management, records needed to document citizens' rights, actions for which Federal officials are responsible, and the historical experience of our nation will be at risk of loss, deterioration, or destruction. According to NARA's Strategic Plan, to minimize these risks, NARA will work in active partnership with the Administration, Federal officials, the Congress, and Federal courts to help them create, identify, appropriately schedule, and manage record material. This will enable the Government to preserve records as long as they are needed to protect rights, ensure accountability, document the national experience, and to destroy records as soon as it is practical to do so when they are no longer needed.

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.

4. Information Technology Security

Since FY 2000, the Archivist has identified computer security as a material weakness in his assurance statements to the President. While corrective steps have been taken, some actions have not been completed, and the agency continues to work on additional measures to strengthen NARA's overall information technology (IT) security posture. 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.

IT security becomes even more critical as NARA increases its visibility through the implementation of e-Government initiatives that expand online services to the public. The more NARA increases electronic access to its services and records, the more vulnerable the agency is to intrusions, viruses, privacy violations, fraud, and other

abuses of its systems. The risk related to IT security is endemic to all Federal agencies and has been identified by the GAO as one of its top 10 high-risk challenges.

Audits, investigations, and reviews performed in FY 2004:

- Assessment of the Controls and Security of NARA Classified Systems
- Vulnerability of NARA E-mail to Unauthorized Access
- Evaluation of NARA's Computer Incident Response Capability
- Follow Up Review of OIG Report #00-02, Review of NARA's Process for Investing in IT Projects
- Hacker Exploits NARA IT Vulnerability
- Information on NARA's Public Website Puts NARA at Risk
- Evaluation of the First Performance Period Award Fee Determination Process for the Fixed-Price-Award-Fee (FPAF) Contract with a NARA Contractor
- Investigation of Misuse of Internet by NARA Employee
- Investigation of Child Pornography

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. NARA envisions expanding opportunities for individual citizens, educational institutions, and Federal agencies to make use of those records. New technologies are making it easier to reach all users in their homes, schools, and workplaces. NARA must increase partnerships with Government agencies at all levels and with universities and corporate communities to take advantage of new means to bring the holdings of the National Archives to people no matter where they are located.

Mastering this challenge requires that NARA listen to its customers, and improve access to records in ways that meet customer needs and customer service standards. This will require NARA to enhance activities such as creating comprehensive catalogs and indexes for our holdings so that users can find the records they need; make documentary material available through the Internet; improve reference service; and help Presidents at the beginning of their administrations plan for public access to their records in Presidential libraries.

6. Meeting Storage Needs of Growing Quantities of Records

NARA-promulgated regulation, 33CFR, 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.

Specifically, in January 2000, NARA revised the regulations for public and private facilities that store Federal records to (1) improve the environment and safeguards for Federal records by incorporating stricter facility standards and advances in sprinkler technology; (2) reflect building design measures that may prevent or minimize fire and water damage to records; and (3) ensure uniform facility standards for all records centers, both public and private, that store and protect Federal records. NARA's challenge is

to ensure compliance with these regulations internally as well as by other agencies that house Federal records.

Audits, investigations, and reviews performed in FY 2004:

- Assessment of NARA's Efforts to Comply with New Facility Standards
- Investigation of Train Derailment Carrying IRS Records in NARA's Possession; Contractor Found to be in Violation of Contract

7. Preservation Needs of Records

NARA cannot provide public access to records to support researchers' needs unless it can preserve them for as long as needed. Providing public access to records for future generations requires that NARA assess the preservation needs of the records, provide storage that retards deterioration, and treat or duplicate and reformat records at high-risk for deterioration. NARA must preserve paper records and motion pictures, audio recordings, videotapes, still photography, aerial photography, microfilm and other microforms, and maps and charts in a variety of formats in our holdings. NARA must ensure that its risk management program adequately identifies and addresses all records needing preservation in a timely manner.

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 the following questions: Are we effectively identifying those holdings that are both most at risk and most important in terms of priority. Who makes this determination, upon what criteria is it based, and is it being soundly and properly applied? Are resources and the technology available and sufficient to meet the preservation needs of these records?

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. This will present a challenge to NARA, especially as the OMB accelerates the due date for submitting consolidated audited financial statements and other performance reports into a combined Performance and Accountability Report.

The Federal Government has a stewardship obligation to prevent fraud, waste, and abuse; to use tax dollars appropriately; and to ensure financial accountability to the President, the Congress, and the American people. Timely, accurate, and useful financial information is essential for making day-to-day operating decisions; managing the Government's operations more efficiently, effectively, and economically; meeting the goals of the Federal financial management reform legislation (Chief Financial Officers Act); supporting results-oriented management approaches; and ensuring accountability on an ongoing basis.

In identifying improved financial performance as one of its five Government-wide initiatives, the President's Management Agenda (PMA) stated that a clean financial audit is a basic prescription for any well-managed organization and recognized that "most federal agencies that obtain clean audits only do so after making extraordinary, labor-intensive assaults on financial records." Further, the PMA stated that without sound internal controls and accurate and timely financial information, it is not possible to ac-

complish the President's agenda to secure the best performance and highest measure of accountability for the American people.

The agency will be challenged in its ability to comply with the newly issued Accountability of Tax Dollars Act of 2002 much as Chief Financial Officer (CFO) agencies were challenged in the initial year following the passage of the CFO Act.

Audits, investigations, and reviews performed in FY 2004:

- Audit of the National Archives Records Center Revolving Fund FY 2002 Financial Statements
- Audit of the National Archives Trust Fund FY 2002 Financial Statements
- Audit of the National Archives Gift Fund FY 2002 Financial Statements
- Audit of NARA's Interagency Agreements
- Audit of the Transit Benefit Program
- Review of the Contractor Compliance with Government Auditing Standards (GAS) for the Audit of the National Archives Trust and Gift Funds FY 2002 Financial Statements
- Review of the Contractor Compliance with GAS for the Audit of the National Archives Records Center Revolving Fund FY 2002 Financial Statements
- Evaluation of NARA's FY 2003 Management Control Program
- Review of NARA's Water and Sewer Billing Adjustment Charge
- Review of University of Texas Invoice for Utility Costs for the Lyndon B. Johnson Library
- Investigation of NARA Cashier Pocketing Money Received from Customers
- Investigation of NARA Employee Splitting Purchases with Government Credit Card to Exceed Purchase Authority
- Investigation of NARA Employee Failing to Report Money Found at Presidential Library
- Investigation of Misuse of Government Credit Card
- Investigation of Fraud Involving Transit Benefits
- Investigation of Government Purchase Card Abuse

9. Physical Security

NARA must maintain adequate levels of physical security over our facilities and holdings 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 by persons for a variety of motivations, defaced, or destroyed by fire or other natural disasters.

The Archivist has identified security of collections as a material weakness under the Financial Manager's Financial Integrity Act (FMFIA) reporting process. Our facilities hold records that serve to document the rights of citizens, the actions of Government officials, and the national experience. They also hold a new class of records identified as "Records of Concern" (ROC). These are records that could be useful to individuals or entities in the planning and conduct of hostile acts against this nation.

Three primary challenges facing NARA are to (1) provide quality service to our customers while instituting reasonable internal controls to prevent theft and to maintain

documentation for supporting recovery of disenfranchised holdings and subsequent prosecution of those who would steal from NARA, (2) take every reasonable, appropriate measure possible to limit access to ROC and act expeditiously in coordinating efforts with appropriate law enforcement entities as warranted and appropriate, and (3) protect and safeguard our facilities and the employees who work in them and to mitigate the potential for damage and destruction through both natural and deliberately precipitated acts.

Audits, investigations, and reviews performed in FY 2004:

- Audit of a Subcontractor's Proposal for Archives I Stack Lighting
- Investigation of Alleged Misuses of Government Vehicles
- Investigation of Theft of Personal Checks from NARA Facility by NARA Contractor
- Investigation of Employee Bomb Threat Results in Termination and Criminal Conviction
- Investigation of Recovery of Stolen NARA Computer
- Proactive Identification of Taylor Pardon Stolen by former NARA Employee

10. Strengthening Human Capital

The GAO has identified human capital as a Government-wide high risk. Strategic human capital management should be the centerpiece of any serious change management initiative or any effort to transform the cultures of Government agencies. Serious human capital shortfalls, however, continue to erode the ability of many agencies, and threaten the ability of others, to economically, efficiently, and effectively perform their missions. According to GAO, the major problem is the lack of a consistent strategic approach to marshaling, managing, and maintaining the human capital needed to maximize Government performance and ensure its accountability. People are an agency's most important organizational asset. An organization's people define its character, affect its capacity to perform, and represent the knowledge base of the organization. Agencies can improve their performance by the way that they treat and manage their people and building commitment and accountability through involving and empowering employees.

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. According to NARA's Strategic Plan, NARA must include preparation for training the leaders of tomorrow in its plans. Further, NARA must help those current staff members possessing traditional archival training to add skills necessary for working with new technologies. In addition, NARA must replace valuable staff members lost to retirement with others able to deal with records in the electronic information age. Moreover, NARA must partner with universities and professional associations to determine educational requirements for the 21st century.

Audits, investigations, and reviews performed in FY 2004:

- Investigation of Employee Discipline for Time and Attendance Abuse
- Investigation of Time and Attendance Errors

APPENDIX B
FEDERAL MANAGERS' FINANCIAL INTEGRITY ACT REPORT

National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

November 1, 2004

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 2004 for the National Archives and Records Administration (NARA).

Pursuant to Section 2 of the Integrity Act, we identified two material weaknesses in fiscal years 2000 and 2001. Two corrective action plans are attached (Enclosures B and C) for material weaknesses in computer security and collections security.

- Enclosure B explains our progress on computer security – reported in FY 2000
- Enclosure C explains our progress on collections security – reported in FY 2001

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.

Pursuant to Section 4 of the Integrity Act, the financial subsystems of NARA generally conform to the objectives detailed in OMB Circular A-127, revised. Although three systems (Order Fulfillment Accounting System; Trust Fund – Gift Fund Financial Review, Analysis, and Reporting System; and Records Center Revolving Fund financial management systems) are not in complete conformance because they fail to meet the financial management system requirements, the non-conformances are not deemed material.

Additional details on NARA compliance with the Integrity Act are provided in Enclosure A.

Respectfully,

JOHN W. CARLIN
Archivist of the United States

Enclosures (3)

ENCLOSURE A
STATISTICAL SUMMARY OF PERFORMANCE

Section 2. Management Controls

Number of Material Weaknesses

	Number reported for the first time in	For that year, number that has been corrected	For that year, number still pending
Prior Years	5	4	1
2001 Report	1	0	2
2002 Report	0	0	2
2003 Report	0	0	2
2004 Report	0	0	2
Total	6	4	2

Section 4. Financial Management Systems

Number of Material Non-conformances

	Number reported for the first time in	For that year, number that has been corrected:	For that year, number still pending
Prior Years	0	0	0
2001 Report	0	0	0
2002 Report	0	0	0
2003 Report	0	0	0
2004 Report	0	0	0
Total	0	0	0

ENCLOSURE B
DESCRIPTION OF MATERIAL WEAKNESS IN MANAGEMENT CONTROLS

Computer Security

As a result of internal information technology (IT) security reviews, a network vulnerability assessment, and Inspector General (OIG) audits during FY 2000, NARA reported four computer security vulnerabilities that, together, made a material weakness that was detailed in the agency's FY 2000 FMFIA report.

During FY 2004, NARA made significant progress in resolving IT Security as an FMFIA material weakness. That progress and the additional actions we still need to take are detailed in the action and validation section below.

To summarize, in FY 2004 NARA updated contingency plans for all 43 of our systems and tested the plans for 41 systems. We updated and tested the disaster recovery plan for NARANET.[1] We created and maintain an up-to-date inventory of all existing NARA classified systems. A Web Based Training module for NARA classified IT systems security was implemented and made available online. NARA has implemented a fully functional IT contingency planning program, and we believe the risks to NARA have been reduced significantly over the past year.

In addition, NARA identified no new significant deficiencies in its FY 2004 Federal Information Security Management Act (FISMA) Report submitted October 6, 2004, to the Office of Management and Budget (OMB). NARA's Inspector General, however, did identify six new significant deficiencies in his FISMA Report, all relating generally to computer security. The six deficiencies were derived from preliminary draft potential findings as part of NARA's FY 2004 financial audit and have not been formally delivered as findings by the auditor. If any of the draft potential findings become actual findings, we will develop corrective action plans as needed. We believe we can make any needed corrections in FY 2005.

---

[1] NARANET: a collection of local area networks installed in 34 NARA facilities that are connected to a wide area network at the National Archives at College Park, using frame relay telecommunications, and then to the Internet. NARANET includes personal computers with a standardized suite of software. NARANET was designed to be modular and scalable using standard hardware and software components.

Title and Description of Material Weakness: Computer security

Name of Responsible Program Manager: L. Reynolds Cahoon, Assistant Archivist for Human Resources and Information Services and Chief Information Officer

Source of Discovery: Internal IT security reviews, a network vulnerability assessment, OIG audits, 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 2000
Original Targeted Correction Date: FY 2002
Revised Correction Date: FY 2005

Action and Validation Process Used on Original Material Weakness:

1. Develop policies and procedures for computer security, including a security plan.

Action Taken: IT security policy documents have been updated, reviewed and approved as NARA Directive 804, "Information Technology Systems Security" and supplements. The supplements are the Management, Operations, and Technical Handbooks. This policy is available to all NARA staff through access to our intranet web site. A search tool was included to assist users with electronic searches of the subject matter. In addition, the IT Security Program Plan received its annual update July 30, 2004. This is no longer a vulnerability. **This action is complete.**

2. Develop and implement a security awareness program for NARA employees.

***Action Taken*:** In FY 2002, an IT security awareness program plan was developed, an awareness brochure was distributed to all employees, and awareness messages continue to be distributed through the NARA intranet web site, e-mail notices, and the monthly Staff Bulletin. Since January 2002, new employees have received an introduction to IT security during orientation. However, there was no mechanism to easily identify security issues or transmit security information to all NARA sites.

In May 2003, this omission was resolved by identifying NARA Information System Security Officers (ISSO) and alternate ISSOs at all NARA sites to support on-going

security training and awareness efforts. We developed and conducted a training program for all ISSOs, and alternate ISSOs. We conducted two training sessions, one in July and one in August 2003, at the National Archives at College Park for the ISSOs and other individuals who have significant IT security responsibilities at each NARA site. During the training, each ISSO was given a copy of our video titled, "Safe Data, It's Your Job," to show at each of our facilities as part of an agency-wide training program for employees, contractors, and volunteers. ISSOs have also been trained in providing IT security training as part of orientation, so that besides receiving training, new employees have an identified point-of-contact for IT security issues.

In FY 2004, we required all NARA personnel, including contractors, volunteers, Foundation members, and other users of NARA's information systems, to take annual IT security training online. Three types of training were included:

1. All NARANET users with an e-mail address took the general User Awareness training;

2. Users who have access to classified electronic data took the course in Classified Data Basics; and

3. Product owners, IT managers and security professionals took the NARA Managers and Information Systems Security Officer (ISSO) training course.

This training will be repeated annually. **This action is complete.**

3. Strengthen firewall protection across the entire network to control inbound and outbound traffic.

***Action Taken*:** This was identified as a weakness in OIG Audit 02-12 and was completed on September 15, 2003. Both the firewall and Intrusion Detection System have been enhanced to increase reporting capabilities, and documented procedures for identifying unauthorized access attempts and correcting associated internal weaknesses have been established. **This action is complete.**

4. Formalize, document, and test disaster recovery contingency program.

***Action Taken*:** In FY 2004 we updated IT contingency plans for all 43 IT systems. We tested all but two of the contingency plans. The tests consisted of

either classroom or functional exercises as recommended by NIST Special Publication 800-34, p. 27-28. We also standardized the structure and content of the contingency plans based on NIST 800-34. All plans are now in compliance with this guidance. A system by system business impact analysis was performed as a part of contingency planning in FY 2003 and FY 2004. Impact statements can be found in each contingency plan. Testing for 41 systems was completed on September 30, 2004.

The two contingency plans that were not tested were PRISM, an acquisition support system, and the application services provided to NARA by the General Services Administration (GSA). PRISM was not tested due to the impact of testing on NARA's Acquisition Services Division resources at year end. Testing for PRISM is scheduled to be completed by the end of the first quarter in FY 2005. Applications provided as a service by GSA (Pegasys, Fed Desk TMR, CHRIS, and ETAMS) have not been tested by NARA. Efforts to obtain documentation from GSA are underway.

NARA has defined responsibility for contingency planning, dedicated budget, contracted for resources, and integrated contingency planning metrics in our computer security program. The aforementioned actions were completed as part of implementation and operation of our IT contingency planning program.

In FY 2004 we also updated and tested the disaster recovery plan for NARANET. In FY 2005 we will create and test an overall disaster recovery plan for the National Archives at College Park, where our central IT operations reside. We also will document our disaster and contingency testing methodology.

5. Ensure that the inventory of classified IT systems is up-to-date, ensure central control for managing the systems, and certify and accredit the systems.

***Action Taken*:** NARA included classified IT systems security as a module in the IT security training. We created and maintain an up-to-date inventory of all existing NARA classified systems. We certified and accredited each classified system, including a risk assessment, systems security plan, security controls testing and vulnerability analysis, and contingency plan. We are developing a new policy directive for classified IT security, which will be finalized and issued in FY 2005.

Results Indicators

Major Milestones	Milestone Dates
1. Develop policies and procedures for computer security, including a security plan.	**Completed:** September 1, 2003
2. Develop and implement a security awareness program for NARA employees.	**Completed:** September 30, 2003
3. Strengthen firewall protection across the entire network to control inbound and outbound traffic.	**Completed:** September 15, 2003
4. Formalize, document, and test disaster recovery contingency program.	**IT contingency plans:** Completed Sept. 30, 2004 **Disaster recovery plans:** July 31, 2005 **Testing methodology:** March 31, 2005 **IT contingency plan testing:** July 31, 2005 **Disaster recovery plan testing:** July 31, 2005
5. Ensure that the inventory of classified IT systems is up-to-date, ensure central control for managing the systems, and certify and accredit the systems.	**Inventory:** Completed September 30, 2004 **C&A:** Completed September 30, 2004 **Training:** Completed September 30, 2004 **Policy:** June 30, 2005

ENCLOSURE C
DESCRIPTION OF MATERIAL WEAKNESS IN MANAGEMENT CONTROLS
Collections Security

NARA reported a material weakness in collections security in FY 2001. Corrective steps have been taken, and many actions have been completed.

Title and Description of Material Weakness: Collections security

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

Source of Discovery: OIG investigation

Appropriation/Account: 110

Pace of Corrective Action

Year Identified: FY 2001
Targeted Correction Date: FY 2005

Action and Validation Process That Will Be Used

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

1. Pre-employment screening (for all staff that have access to archival records)

- Update and strengthen recruitment policies to
  - Verify resume information
  - Require and check references
  - Document all application and screening activities
  - Require application and screening process for volunteers and interns

2. Staff training and monitoring

- Train staff and supervisors annually on collections security
- Closely supervise interns and volunteers who work with records
- Require more records personnel to file financial disclosure statements

3. Security for records storage areas

- Review and revise, as necessary, security procedures in all records facilities
- Analyze costs and benefits of additional measures such as
  - Separating staff work areas from records storage areas
  - Installing electronic card readers or CCTV systems

  - Reducing number of entry and exit points
- Improve enforcement of existing policies on records handling and transport

4. Records control

- Compile accurate container counts and location information for all holdings
- Make back-up copies of finding aids and store as vital records
- Isolate in secure storage intrinsically valuable records
- Analyze costs and benefits of marking, duplicating, or otherwise protecting valuable records

5. Theft prevention and response

- Monitor auction sites, dealer lists, and other sources for possible stolen items
- Improve communication with collections community about possible stolen items
- Publicize widely incidents of theft and the penalties
- Conduct regular audits of collections security policies and practices

Results Indicators:

Major Milestones	Milestone Dates
1. Update and strengthen recruitment policies	*Staff:* ***To be completed in FY 2005*** **Volunteers:** Completed April 2004
2. Implement annual training program on collections security	Completed. Training held October 2003 and September 2004.
3. Review and revise records security policies	To be completed in FY 2005
4. Compile accurate container counts and locations for all holdings	**Pilot Marking Project:** To be completed by March 2005 **RFID Testing:** To be completed in FY 2005
5. Isolate valuable records	To be completed by December 2004

1. **Update and strengthen recruitment policies:** NARA issued interim guidance on the recruitment and use of volunteers on April 23, 2004. This guidance includes requirements for background checks. NARA offices verify resumes, conduct reference checks, and document application and screening activities

for staff position hires where employees have access to records. This practice will be documented in official policy in FY 2005.

2. **Implement annual training program on collections security:** Regional archives directors received security training at their annual conference in October 2003. They will receive refresher training this October. In addition, in our continuing effort to improve collections security, NARA contracted with the Society of American Archivists (SAA) to hold a special security training session for research room and facility supervisors in September 2004. The training included experts from SAA and representatives from the OIG, Space and Security Management Division, and Federal Bureau of Investigation. **This action is complete.**

3. **Review and revise records security policies.** In FY 2004, NARA offices drafted a comprehensive security policy which consolidates and expands upon existing NARA policies and procedures. During the policy development process, each program area reviewed internal records security policies and procedures and made changes to increase security in specific areas. For example, NARA requires that staff workstations be moved out of archives stack areas as soon as possible and tightened restrictions on researcher access to stack areas. NARA units reviewed and implemented a "clean research room" policy to better control what researchers can bring in to rooms where they work with original records. NARA also reviewed procedures for delivering records to researchers in research rooms. Closed circuit televisions were installed, improved or repaired in many locations. New records handling and shipping protocols were developed for moving records nationwide to NARA's secure underground storage caves. The comprehensive update to NARA's collections security policies will be completed and issued in FY 2005.

4. **Compile accurate container counts and locations for all holdings:** In FY 2003 NARA improved container location controls, created security copies of records finding aids, and identified and created special storage for additional intrinsically valuable records. In FY 2004, NARA continued analysis of techniques and costs to physically mark records. A pilot project is underway and will be completed by March 2005. NARA also developed contracted with the University of Maryland to investigate the use of Radio Frequency Identification Tag (RFID) technology as a possible means of marking and tracking the location of records. A pilot application of this technology will be tested in FY 2005.

5. **Isolate valuable records.** NARA offices undertook a major effort to identify valuable records and completed the assessment in May 2004**.** Sufficient storage capacity was installed as needed at each site to secure valuable records. As other

high-value records are identified or accessioned, NARA will ensure that they are stored in secure locations. NARA created web pages containing information to assist the public and manuscript collectors in identifying material that might be estrayed or stolen Federal records. The web pages, which will be posted this fall, include contact information for a specific e-mail address to report suspected stolen items to the OIG. NARA also developed procedures to be followed in checking the accuracy of any information provided from any source about possible stolen or estrayed documents. NARA has an ongoing program to regularly monitor auction sites and dealer catalogs. During FY 2004, NARA worked with a manuscript collector's journal, professional organizations, and a private auction site to share information about the issues and risks involving possible Federal records and documentary materials that may be stolen from the National Archives. There is an ongoing investigation begun in 2004 of selected items that were previously in the holdings of the National Archives and alleged to be stolen and, in some cases, later offered for sale. These items were discovered for sale on an auction site.