



OFFICE *of* INSPECTOR GENERAL

**SEMIANNUAL REPORT**

*to* **CONGRESS**

OCTOBER 1, 2010 *to* MARCH 31, 2011



---

---

# FOREWORD

---

---

*Under the leadership of David S. Ferriero, the National Archives and Records Administration (NARA) is undergoing a major transformation restructuring the organization and operations of this agency. When asked why NARA had embarked upon this journey the Archivist responded, “if we continue with the status quo, we will not be able to respond successfully to the challenges that we and the records we care for are now facing. We cannot afford not to change.”*

*Since my appointment, the Office of Inspector General (OIG) has sought to be an agent of positive change. Much like the Archivist, I initially viewed NARA as an “outsider” would. I had a different perspective than many of my colleagues in the agency, and thought back to my days at the U.S. Customs Service and our “Day One” project. The premise of the project was simple, if you were starting a brand new agency, what would it look like and what services would it provide. I thought NARA could benefit from such an examination. Now the results are in and fresh air is in the offing.*

*The OIG will partner with our stakeholders to play a constructive role in helping the “new” NARA better achieve its mission. As NARA is faced with technological challenges and opportunities, we will continually strive to provide valuable assistance and unique perspective. This posture is best illustrated by our ongoing focus on the Electronic Records Archive (ERA) program. In January 2011, we reported to the Archivist our concerns on search capacity constraints that could impede the ability of users to access records in a timely and efficient manner. Now, our focus turns to the process and technology by which electronic records will be ingested into ERA upon transfer from originating agencies. We will also examine whether the prime contractor has met base system requirements.*

*While technology is ever evolving, we will “stay home” and continue to focus upon physically protecting all facets of this agency. The adoption of recommendations put forth by our auditors in this reporting period will result in a security guard force better able to protect NARA facilities, staff, visitors and holdings. OIG Special Agents will continually test and evaluate security measures in place and detect and investigate those that abuse their privileges when accessing our holdings, be they researchers or staff. This commitment was recently on full display in the case of the NARA researcher who confessed orally and in writing to altering the date on a historic Abraham Lincoln Presidential Pardon.*

*It continues to be my honor to serve as the NARA Inspector General. A sound democracy is built upon a foundation of accountability, which in turn is anchored in the records we maintain. Our vast and unique holdings tell the history of our people and our country. To provide some measure of stewardship over the holdings of the National Archives remains a rewarding yet humbling experience.*



Paul Brachfeld  
Inspector General

# TABLE OF CONTENTS

---

Foreword.....	<i>i</i>
Executive Summary .....	2
Introduction .....	7
Activities .....	9
Audits .....	12
Investigations.....	19
Top Ten Management Challenges .....	25
Reporting Requirements .....	30

Visit <http://www.archives.gov/oig/> to learn more about the National Archives Office of Inspector General.

# *EXECUTIVE SUMMARY*

---

This is the 45th Semiannual Report to the Congress summarizing the activities and accomplishments of the National Archives and Records Administration (NARA) Office of Inspector General (OIG). A summary of NARA's top ten management challenges is included as well. The highlights of our major functions are summarized below.

## Audits

The Audit Division continued to examine the security of NARA's Information Technology (IT) systems, the development of NARA's Electronic Records Archives (ERA) system, and assess the economy and efficiency of NARA's programs and operations. During the reporting period, we issued the following audit reports and management letters.

### **Information Technology (IT)**

- **Network Vulnerability Assessment and Penetration Testing.** This audit found vulnerabilities in NARA's IT systems allowing an intruder to intentionally or accidentally gain access to NARA's network or systems. We identified several improvements which needed to be made to the configuration, upgrade, and patch management processes at NARA, and made 14 recommendations to correct these weaknesses. Management concurred with all the recommendations and initiated corrective actions. (OIG Report #11-02, dated November 8, 2010. See page 13. )
- **Controls over Inappropriate Personal Use of the Internet.** Controls over internet usage are inadequate, and NARA employees continue to access prohibited material. NARA has worked to monitor and prevent inappropriate internet usage, and the filter application used is generally successful in blocking the majority of NARA staff who carelessly or inadvertently attempt to access inappropriate material. However, with little effort, NARA staff have been able to bypass the web filter. Further, while the filter maintains a record of all NARA staff internet usage, the limited amount of information reviewed and analysis conducted by NARA allowed excessive personal and inappropriate use to go undetected or unaddressed. Our audit identified several needed improvements, and made five recommendations to more thoroughly ensure internal controls are enforced and risks are minimized. Management concurred with the recommendations. (OIG Report #11-10, dated March 9, 2011. See page 13.)
- **NARANET Server Upgrade Project.** We audited NARA's project to upgrade the server hardware and software infrastructures of the current NARANet system installed across NARA. This upgrade was necessary because the current system was at risk of failure due to outdated hardware and unsupported software. Our review found this project was not adequately managed and monitored to ensure requirements were met in the most economic and efficient manner. Planning was not adequate, and critical stakeholders were not included in the decision to continue with Novell. There was no comprehensive analysis of alternatives, and other platforms which could have improved productivity and increased efficiencies were not fully considered. Finally, monthly status reports used to monitor the project did not accurately reflect the full cost and risks. To mitigate these risks and prevent similar occurrences, we made seven

# EXECUTIVE SUMMARY

---

recommendations to aid in the completion of this project and improve NARA's IT Investment Management Process. Management concurred with the recommendations. (OIG Report #11-06, dated November 30, 2010. See page 14.)

- **NARA's Work-At-Home System (WAHS).** The OIG initiated follow-up work to the Audit of NARA's Work at Home System (OIG Audit Report No. 09-15) due to concerns about the management of RSA tokens, the hardware devices providing two-factor authentication for remote access to NARA's IT systems. However, during the audit substantial improvements were made in token management. We made several suggestions, and encouraged NARA to consider using acknowledgement statements for token holders to accept the responsibility for security and following all organizational policies for remote access, as suggested by the National Institute of Technology and Standards (NIST). (Audit Memorandum #11-09, dated January 31, 2011. See page 15.)

## Electronic Records Archives (ERA)

- **ERA Lacks Ability to Search Records' Contents.** ERA will not allow users to search the content of the full inventory of public electronic records ERA will store. However, NARA will manually select certain records to copy to the Online Public Access interface to allow full content searching. Aside from this select group, the default will be that ERA only allows users to locate records by searching through metadata and descriptions generated about the records. In a computer system that does not search the content of records, the record descriptions take on additional importance as the only searchable narrative of the record's contents. However, as ERA has now been set-up, such descriptions will not be automatically generated by the system, but instead must be done manually. Considering the massive amount of data expected to be put into the system, such a manual process will invariably create substantial, perhaps insurmountable, bottlenecks. (Management Letter #11-08, dated January 5, 2011.)
- **Defense Contract Audit Agency (DCAA) Audits.** The Defense Contract Audit Agency (DCAA) reviewed contractor invoices submitted for work on ERA. The reviews consisted of verifying direct labor charges, subcontractor labor charges, other direct costs, and overhead. DCAA assists with this effort because of their experience with performing this type of review and their access to contractor records. DCAA issued eight audit reports, none of which contained any significant findings. (DCAA Audit Report Numbers 6271-2011N25000001-002, 6271-2010N25000001-013 and 6271-2010N25000001-014 dated October 22, 2010; DCAA Audit Report Numbers 6271-2010N17900006, 6271-2010N17900003, and 6271-2010N17900004, 6271-2010N17900005 and 6271-2010N17900007 dated March 14, 2011.)

## Programs and Operations

- **NARA's Security Guard Contract for Archives I and II.** The contractor was not following the firearm qualification requirements of the contract; scenario test and exercises were not conducted to assess security officer's response to real-world type situations; and the contractually required physical fitness program was not in place to

# EXECUTIVE SUMMARY

---

ensure officers remained physically fit to be able to perform all the duties required of the job. We made seven recommendations to assist NARA in administration and oversight of the contract and management concurred. (OIG Report #11-05, dated February 18, 2011. See page 15.)

- **Oversight of Selected Grantees' Use of Grant Funds.** NARA does not employ a formal structured or systematic risk management approach to monitoring grants. As a result, NARA's grant program is at risk of waste and abuse. Grantees reviewed were not always following grant regulations or the intent of their grant contracts, and they did not always use grant funds as intended. Our review of a sample of active and closed grants resulted in questioned costs of \$789,479, and funds to better use of \$434,589. We made four recommendations to assist management in improving program stewardship, and management concurred. (OIG Report #11-03, dated February 16, 2011. See page 16.)
- **NARA's Photocopier Security.** We performed this audit to determine if appropriate security measures were in place to safeguard and prevent inappropriate release of sensitive information and personally identifiable information (PII) residing on NARA photocopiers containing hard drives. We found opportunities existed to strengthen controls to ensure photocopier hard drives are protected from potential exposure, and made seven recommendations to assist NARA in providing appropriate administrative, technical, and physical safeguards over sensitive information and PII. Management concurred with all the recommendations. (OIG Report #11-07, dated March 22, 2011. See page 16.)
- **Movement of Freight.** This audit was initiated as a result of a FY 2007 investigation by the OIG where a NARA employee was indicted for theft of government property and conspiracy to embezzle \$958,280 from the United States. The audit sought to determine if controls are effective and efficient to ensure NARA obtains the best value and most economical prices for the movement of freight. Our review disclosed NARA has taken several significant steps to improve controls since FY 2007. We made three recommendations to further assist NARA in enhancing controls in freight management, most notably in the area of separation of duties. Management concurred with all the recommendations. (OIG Report #11-01, dated November 3, 2010. See page 17.)
- **NARA's Fiscal Year 2010 Financial Statements.** Cotton & Company LLP (C&C) was contracted to audit NARA's consolidated balance sheets as of September 30, 2010, and the related statement of net cost, changes in net position and budgetary resources. For the fifth year in a row NARA received an unqualified opinion on their financial statements. C&C reported one significant deficiency in internal control over financial reporting in Information Technology, resulting in four recommendations. C&C disclosed no material weaknesses, and no instances of noncompliance with certain provisions of laws and regulations. (OIG Report #11-04, dated November 26, 2010. See page 17.)

# *EXECUTIVE SUMMARY*

---

## Investigations

During this reporting period, the Office of Investigations (OI) opened eight investigations and closed 19 investigations, four of which are closed pending an administrative response from NARA. The OI also received 46 complaints and closed 51 complaints, six of which are closed pending an administrative response from NARA. More than 1,100 NARA holdings were recovered during the period. The OI worked with the IRS and the Naval Criminal Investigative Service, as well as the Offices of Inspectors General at the Veterans Administration and the Government Printing Office. The OI also worked with a number of local and state law enforcement entities to include: Office of the States Attorney in Cook County, Illinois, DC Metro Police Department, Montgomery County Maryland Police Department and the Maryland States Attorney's Office. At the close of the period, there remained 56 open complaints and 23 open investigations.

The OI completed investigations in a variety of areas including the following:

- Security Guard Misconduct
- Improper Use of Government Computer
- Improper Government Credit Card Use
- Threatening Phone Calls
- Procurement Fraud
- Contract Fraud
- Theft of Government Property
- Obstruction of Federal Audit
- Destruction of Federal Records
- Mishandling of Classified Material
- Stolen/Missing Records

The Office of Investigations is presently staffed with six 1811 series Special Agents, an Investigative Archivist, a Computer Forensic Analyst, and an Assistant Inspector General for Investigations. This team provides investigative coverage to an approximately 3,000-person, 44-facility, nationwide agency which includes the Presidential library system. The OI conducts both responsive and proactive investigations in order to support our statutory mission. During the period, the OI began proactive work on a contract fraud initiative, as well as a holdings protection assessment. Additionally, the OI closed two procurement fraud cases preventing \$1.2 million in the procurement of grey market and counterfeit computer equipment by NARA. At present our law-enforcement authority is through special deputation from the U.S. Marshals Service. Our application to the Attorney General for statutory law enforcement authority is under review at the Department of Justice. We are based in NARA's College Park, Maryland facility and staff a satellite office in NARA's Washington, D.C. facility

# ***EXECUTIVE SUMMARY***

---

## **Management Assistance and Other Work**

- OIG personnel discovered the contractor developing the Electronic Records Archive (ERA) had been issued a patent on the ERA unbeknownst to NARA management. NARA management was notified and is currently taking steps to protect the government's interests.
- Referred one case from the Archival Recovery Team to the Office of General Counsel pursuant to NARA Directive 1462.
- Members of the Office of Investigations, and particularly, the Archival Recovery Team, met routinely with staff from NARA's Holdings Protection Program in an effort to marshal our collective resources to discover new avenues and approaches to providing adequate security and control of our nation's historical records.
- Counsel to the IG assisted the Information Security Oversight Office (ISOO) in the implementation of the Reducing Over-Classification Act, coordinating actions between ISOO and affected Inspectors General.
- Responded to multiple requests for OIG records under the Freedom of Information Act
- Assisted NARA in an agency effort to stem illegal access to freight cars containing NARA material.
- Reviewed legislative proposals and provided feedback to appropriate entities and reviewed newly passed legislation for its affect on NARA and the NARA OIG.
- Provided comment and input into several NARA directives covering a variety of topics such as access control at facilities and reports of survey on lost or missing property.

# ***INTRODUCTION***

---

## **About the National Archives and Records Administration**

### **Mission**

The National Archives and Records Administration serves American democracy by safeguarding and preserving the records of our Government, ensuring the people can discover, use, and learn from this documentary heritage. Further, the agency ensures continuing access to the essential documentation of the rights of American citizens and the actions of their government; and supports democracy, promotes civic education, and facilitates historical understanding of our national experience.

### **Background**

NARA, by preserving the nation's documentary history, serves as a public trust on which our democracy depends. It enables citizens to inspect for themselves the record of what the Government has done. It enables officials and agencies to review their actions and helps citizens hold them accountable. It ensures continuing access to essential evidence documenting the rights of American citizens, the actions of Federal officials, and the national experience.

Federal records reflect and document America's development over more than 200 years. They are great in number, diverse in character, and rich in information. NARA's traditional holdings amount to 4.1 million cubic feet of records. These holdings also include, among other things, letters, reports, architectural/engineering drawings, maps and charts; moving images and sound recordings; and photographic images. Additionally, NARA maintains nearly 600,000 artifact items and more than 130 terabytes of electronic records. The number of records born and stored solely in the electronic world will only continue to grow, thus NARA is developing the Electronic Record Archives to address this burgeoning issue.

NARA involves millions of people in its public programs, which include exhibitions, tours, educational programs, film series, and genealogical workshops. In FY 2010, NARA had 39 million online visits in addition to hosting 3.6 million traditional museum visitors, all while responding to 1.5 million written requests from the public. NARA also publishes the *Federal Register* and other legal and reference documents, forming a vital link between the Federal Government and those affected by its regulations and actions. Through the National Historical Publications and Records Commission, NARA helps preserve and publish non-Federal historical documents that also constitute an important part of our national heritage. Additionally, NARA administers 13 Presidential libraries preserving the papers and other historical materials of all past Presidents since Herbert Hoover.

### **Resources**

In fiscal year (FY) 2011, NARA was appropriated an annual budget of approximately \$434 million and 3,380 (estimated) Full-time Equivalents (FTEs), including appropriations of \$339 million for operations, \$72 million for the Electronic Records Archives (ERA) program, \$11.8 million for repairs and restorations of facilities, and \$6.98 million for grants. NARA operates 44 facilities nationwide.

# ***INTRODUCTION***

---

## **About the Office of Inspector General (OIG)**

### **The OIG Mission**

The OIG's mission is to ensure NARA protects and preserves the items belonging in our holdings, while safely providing the American people with the opportunity to discover, use and learn from this documentary heritage. We accomplish this by providing high-quality, objective audits and investigations; and serving as an independent, internal advocate for economy, efficiency, and effectiveness.

### **Background**

The Inspector General Act of 1978, as amended, along with the Inspector General Reform Act of 2008, establishes the OIG's independent role and general responsibilities. The Inspector General reports to both the Archivist of the United States and the Congress. The OIG evaluates NARA's performance, makes recommendations for improvements, and follows up to ensure economical, efficient, and effective operations and compliance with laws, policies, and regulations. In particular, the OIG:

- assesses the effectiveness, efficiency, and economy of NARA programs and operations;
- recommends improvements in policies and procedures to enhance operations and correct deficiencies;
- recommends cost savings through greater efficiency and economy of operations, alternative use of resources, and collection actions; and
- investigates and recommends legal and management actions to correct fraud, waste, abuse, or mismanagement.

Further, the OIG investigates criminal and administrative matters concerning the agency, helping ensure the safety and viability of NARA's holdings, customers, staff, and resources.

### **Resources**

In FY 2010, a separate appropriation was established for the OIG in compliance with the Inspector General Reform Act of 2008. Previously funds for the OIG came from NARA's Operating Expenses appropriation. For FY 2011, Congress provided \$4.1 million for the OIG, including resources for 23 FTEs. At the beginning of the period, the OIG had one audit and one special agent vacancy to fill. During the period the special agent position was filled, but the auditor position remains vacant. Currently the OIG has one Inspector General, one support staff, 10 FTEs devoted to audits, nine FTEs devoted to investigations, and a counsel to the Inspector General.

# ***ACTIVITIES***

---

## **Involvement in the Inspector General Community**

### **Counsel of Inspectors General on Integrity and Efficiency (CIGIE) Investigations Committee**

The IG served as a member of the CIGIE Investigations Committee. The mission of the Investigations Committee is to advise the IG community on issues involving investigative functions, establishing investigative guidelines, and promoting best practices.

### **Assistant Inspectors General for Investigations (AIGI) Committee**

The AIGI served as vice-chair to the AIGI Committee, which serves as a standing subcommittee to the CIGIE Investigations Committee. The AIGI Committee provides guidance, assistance and support to the CIGIE Investigations Committee in the performance of its duties. In addition, the AIGI Committee serves as a conduit for suggestions, issues and concerns that affect the OIG investigations community to the CIGIE Investigations Committee for appropriate action.

### **Council of Counsels to Inspectors General (CCIG)**

The OIG counsel continues to be an active member of the CCIG, and communicated regularly with fellow members. The CCIG provides a rich environment where legal issues can be raised and interpretations can be presented and reviewed with an experienced network of OIG lawyers. During regular meetings multiple topics were discussed and addressed.

### **Federal Audit Executive Council (FAEC)**

The Assistant Inspector General for Audits (AIGA) continued to serve as a representative to the FAEC. During the period, the AIGA attended FAEC's meeting to discuss topics such as financial statement audit issues, audit training, opinion reports on internal controls, and information security.

# ***ACTIVITIES***

---

## **Peer Review Information**

### **Peer Review of the Appalachian Regional Commission's OIG Audit Organization**

In accordance with the Government Accountability Office's *Government Auditing Standards* (GAS) and CIGIE guidelines, we reviewed the system of quality control for the audit organization of the Appalachian Regional Commission Office of Inspector General (ARC OIG) in effect for the year ended September 30, 2010. A system of quality control encompasses an OIG's organizational structure and the policies adopted and procedures established to provide it with reasonable assurance of conforming to GAS.

During the course of the review, ARC OIG notified us that they did not perform any audits during the period under review, but rather performed inspections. It is ARC OIG's current policy not to perform audits or any other work under generally accepted government auditing standards because of its staff size. We took this into consideration in rendering our opinion on the ARC OIG quality control program. We concluded, except for the scope limitation cited, the system of quality control in effect for the two years ended September 30, 2010 has been suitably designed to provide reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. (OIG Audit Report #11-11, dated March 18, 2011)

### **Peer Review of NARA OIG's Audit Organization**

NARA OIG's audit organization was last peer reviewed by the Library of Congress in April of 2008. There are no outstanding recommendations from this review.

### **Peer Review of NARA OIG's Office of Investigations**

NARA OIG's Office of Investigations was last peer reviewed by the National Science Foundation in May of 2008. There are no outstanding recommendations from this review.

# ***ACTIVITIES***

---

## **Response to Congressional Items**

### **Request for Freedom of Information Act (FOIA) Request Information**

We provided the Committee on Oversight and Government Reform information on FOIA requests made to the OIG for the preceding five years. A spreadsheet was provided containing (with limited exceptions) the (a) name of the requestor; (b) the date of the request; (c) a brief description of the documents or records sought; (d) any tracking number assigned by the OIG; (e) date the request was closed; (f) whether any records were provided in response and (g) any additional identification number or code assigned by the OIG for internal use.

### **Request for Information on Non-Public Cases**

In accordance with a written request, we provided Senator Charles Grassley and Senator Tom Coburn with a biannual report on all closed investigations, evaluations, and audits that were not disclosed to the public.

### **Federal Information Security Management Act (FISMA) Report**

As required by the Federal Information Security Management Act (FISMA), the OIG completed an independent assessment as to the quality of NARA's information security program. Our review focused on NARA's performance in the following FISMA-related areas outlined by the Office of Management and Budget (OMB): certification and accreditation (C&A); configuration management; security incident management; security training; remediation/plans of actions and milestones (POA&M); remote access; identity management; continuous monitoring; contingency planning; and contractor oversight.

NARA needed significant improvements in each of these ten program areas to be consistent with FISMA and National Institute of Standards and Technology (NIST) requirements. Specifically, previously identified weaknesses continued in NARA's management of their C&A, POA&M, incident response, and contingency planning processes. Agency-wide improvements were also needed in NARA's remote access and identity management programs. Further, a continuous monitoring program had not been fully implemented and was still in its infancy at NARA. During fiscal year 2010, progress was made in NARA's management of security configurations and security training. However, additional work was still needed to meet NIST requirements. Finally, although NARA policy required contractor systems to meet the same requirements as agency-owned systems, we found instances of contractor systems not meeting all requirements.

# AUDITS

---

## Overview

This period, we issued:

- ten final audit reports, and
- one management letter.<sup>1</sup>

We completed fieldwork on the following audits:

- an audit of OMB's Trusted Internet Connections Initiative to determine whether NARA is prepared to meet the goals and objectives of the initiative;
- an audit of Premium and Foreign Travel to determine whether this type of travel is appropriately authorized and properly managed in accordance with agency and federal travel regulations; and
- an audit of NARA's Drug Testing Program to determine whether controls are in place to facilitate an effective drug testing program.

We continued work on the following assignments:

- a follow-up audit of the Process of Safeguarding and Accounting for Presidential Library Artifacts to evaluate NARA efforts to implement recommendations contained in OIG Audit Report 08-01, and to determine whether actions taken provide reasonable assurance management controls are adequate to safeguard and account for library artifacts;
- an audit of the Management of Records at the Washington National Records Center (WNRC) to evaluate and assess the adequacy of controls over the management and handling of records;
- an audit of NARA's Classified Systems to determine whether NARA's classified systems are properly managed and adequately secured; and
- an audit of NARA's Telework Program to determine whether NARA is fully capitalizing on the identified benefits of telework and administering its telework program in accordance with federal regulation and NARA policy.

---

<sup>1</sup> Management letters are used to address issues which need to be quickly brought to the Archivist's or management's attention.

# **AUDITS**

---

## **Audit Summaries**

### **Network Vulnerability Assessment and Penetration Testing**

The OIG contracted with Clifton Gunderson LLP (CG) to perform vulnerability assessment and penetration testing of NARA's internal and external network infrastructure and environment. The overall objective of the audit was to assess the chances an intruder could intentionally or accidentally gain access to NARA's network or systems. This assessment helps the effectiveness of NARA's information systems security in preventing and detecting unauthorized external and internal access to logical assets, and provides a snapshot evaluation of NARA's security posture and potential vulnerabilities that should be remediated.

The audit found vulnerabilities in the environment could result in an intruder intentionally or accidentally gaining access to NARA's network or systems. CG validated that several vulnerabilities identified could be used to potentially compromise NARA's network, and in several cases, actually exploited vulnerabilities to obtain unauthorized access or escalation of user privileges. CG identified several improvements to be made to the configuration, upgrade, and patch management processes at NARA and made 14 recommendations to correct these weaknesses. Management concurred with all the recommendations and initiated corrective actions. (OIG Report #11-02, dated November 8, 2010.)

### **Controls over Inappropriate Personal Use of the Internet**

The objective of this audit was to determine whether controls were adequate in preventing and deterring NARA staff from using their government-assigned workstations to access inappropriate internet material. Specifically, our review focused on whether NARA employees were in compliance with directives restricting access to inappropriate web sites, and whether controls and administrative processes in place effectively prevent NARA staff from accessing these sites.

Our audit disclosed that, although NARA has invested in tools and implemented procedures to monitor and prevent inappropriate internet usage by its staff, controls remain inadequate and NARA employees continue to access prohibited material. Specifically, the audit found NARA: (a) is overly confident in the effectiveness of its web filter application, (b) does not fully utilize the features of its web filter application, and (c) has not established adequate procedures to consistently enforce its policy on inappropriate internet usage. As a result, NARA is at risk for decreased public trust, reduced employee productivity, legal liability, and degradation of network performance.

We identified a number of methods used by NARA staff to bypass its web filter application, as well as specific features of the web filter application that were not fully utilized in preventing these bypass methods. In extreme cases, individuals at NARA accessed inappropriate material for multiple hours per day and thousands of different explicit websites during the review period. Other NARA employees used web proxies and adult forums to access websites with inappropriate content. Further, the audit discovered the web filter application in use by NARA was not able to handle the amount of internet traffic flow, leading to an overload of the application and intermittent web filter failures.

# AUDITS

---

We made five recommendations intended to strengthen the effectiveness of the controls over the staff's access to inappropriate internet material and allow management to more adequately enforce its policy on proper internet usage. Management concurred with each of the recommendations included in the report. (OIG Report #11-10, dated March 9, 2011.)

## **NARANET Server Upgrade Project**

Our objective was to determine whether the NARANet Server Upgrade (NSU) Project was developed in accordance with NARA requirements, and whether system development was adequately managed and monitored to ensure project requirements were met. The purpose of the NSU Project was to upgrade the server hardware and software infrastructures across NARA, which were based on a Novell environment. The system in place was at risk of failure due to outdated hardware and unsupported software.

We found this project was not adequately managed and monitored to ensure requirements were met in the most economic and efficient manner. Specifically, while the project development met most of the NARA requirements, planning was not adequate and critical stakeholders were not included in the decision to continue with Novell. Further, a comprehensive analysis of alternatives was not completed. Other platforms which could have improved productivity and increased efficiencies were not fully considered during project planning. Finally, monthly status reports used by management to monitor the project did not accurately reflect the full cost and risks of the project.

As a result, the best alternative to maximize value or minimize risk may not have been chosen, and limited resources may have been wasted. Further, opportunities were missed to switch to a new environment. Had NARA considered an alternative environment or platform, such as Microsoft, only one upgrade or transition would have been necessary. Instead, NARA was upgrading its Novell environment with the possibility of needing to transition to another platform, resulting in the expenditure of additional funds. With adequate planning, NARA could have avoided this \$2.9 million upgrade of Novell products.

Finally, unnecessary risks were placed on NARA's IT infrastructure and alternative solutions were limited. Specifically, the operational hardware platforms were past the end of their useful lifecycle, thereby creating an increased risk for hardware failures and consequent disruptions of business services such failures entail. This unstable environment limited NARA's ability to seek other alternatives.

To mitigate these risks and prevent similar occurrences, we made seven recommendations to aid in the completion of the project and to improve management of NARA's IT Investment Management Process. Management concurred with all seven recommendations. (OIG Report #11-06, dated November 30, 2010.)

# AUDITS

---

## **NARA's Work-At-Home System**

In 2010, the OIG initiated follow up audit work to the previously issued Audit of NARA's Work at Home System (WAHS), (OIG Audit Report No. 09-15), as a result of concerns relating to RSA tokens, the hardware devices used by NARA to provide two-factor authentication for remote access through the WAHS. Specifically, we were concerned with the utilization and associated cost of these tokens managed and paid for by NARA. Previously, we found NARA paid a yearly maintenance cost of \$215,000 for 3,000 RSA tokens, even though only a significantly smaller number, approximately 50 tokens, were distributed and being used. However, during the audit, improvements were made in the management of these tokens. For example, the number of tokens paid for by NARA was lowered to a more realistic number and 80% of the tokens were distributed to users. Also, former employees were no longer assigned RSA tokens and improvements were made in NARA's account management and inventory of tokens. Finally, users were provided with training to help identify social engineering techniques used to obtain sensitive or confidential information such as user-created personal identification numbers (PINs).

Therefore, we suggested NARA continue to monitor the usage of RSA tokens, terminate and collect tokens of former employees, disable lost or stolen tokens, and provide continual reminders of the risks and tactics of social engineering. Also, we encouraged NARA to consider using acknowledgement statements, for token holders to accept the responsibility for ensuring security and following all organizational policies for remote access, as suggested by the National Institute of Technology and Standards (NIST). (Audit Memorandum #11-09, dated January 31, 2011)

## **NARA's Security Guard Contract for Archives I and II**

We audited NARA's \$6.5 million contract for providing an armed, uniformed protective security force 24 hours per day, seven days a week for the physical protection of the National Archives properties located in Washington, D.C. and College Park, Maryland. The purpose of this audit was to determine whether NARA was properly administering the contract, and whether the contractor was performing in accordance with contract requirements.

We found additional oversight was needed in several areas. For example, security officers were not following the firearm qualification requirements of the contract. Although officers must have a Maryland handgun permit and DC Special Police Officer certification, the firearm qualification used to qualify for these designations did not meet the level of skill required by the contract. Therefore, NARA was not receiving the level of service contracted for, and security officers may not be as proficient in the use of firearms as needed to stand post at NARA.

We identified additional areas of concern related to testing and training of the security officers and the physical fitness of the officers. Specifically, scenario tests and exercises were not conducted to assess security officer's response to real-world type situations. By not conducting these tests, NARA is missing an opportunity to determine whether the security officers are familiar with their post orders and emergency action procedures and whether additional training

# **AUDITS**

---

is needed. Further, the contractually-required physical fitness program was not in place for ensuring officers remained physically fit to be able to perform all the duties required of the job. We made seven recommendations for improvement. Management concurred with each recommendation. (OIG Report #10-15, dated June 23, 2010.)

## **Oversight of Selected Grantees' Use of Grant Funds**

The objective of this audit was to determine whether management controls were adequate to ensure (1) grants were properly administered, (2) grant goals and objectives were met, and (3) grant funds were adequately accounted for and appropriately used. Audit procedures focused on evaluating the system of management controls over grant oversight and included an evaluation of whether National Historical Publication and Records Commission (NHPRC) grantees used grant funds in accordance with federal regulations.

While we found NHPRC has established adequate management controls to ensure grant goals and objectives were identified and met, NHPRC did not employ a formal structured or systematic risk management approach to monitoring grants. As a result, NHPRC cannot adequately: (1) determine whether a grantee has the ability to administer, monitor, and account for grant funds prior to the award of a grant; (2) determine how frequently to perform a grant review, recognize how comprehensive a grant review should be, and identify potential troubled grants; and (3) mitigate risk and request appropriate refunds associated with grantees not meeting their cost share obligations. As a result of these conditions, NHPRC's grant program is at risk of waste and abuse. Our review of the active and closed grants assessed during this audit resulted in questioned costs of \$789,479, and funds put to better use of \$434,589. In addition, the audit identified that grantees were not always following grant regulations, the intent of the grant contract, and did not always use grant funds as intended. We made four recommendations to assist management in improving program stewardship. Management concurred with our recommendations. (OIG Report #11-03, dated February 16, 2011).

## **NARA's Photocopier Security**

The objective of this audit was to determine if appropriate security measures were in place to safeguard and prevent inappropriate release of sensitive information and Personally Identifiable Information (PII) residing on NARA photocopiers containing hard drives. Specifically, our review focused on whether (1) NARA used photocopiers containing hard drives capable of retaining sensitive information, and (2) actions taken by NARA to mitigate risks posed by the potential exposure of this sensitive information were adequate.

Our audit found opportunities exist to strengthen controls to ensure photocopier hard drives are protected from potential exposure. Specifically, the audit found (1) NARA lacks appropriate controls to ensure all photocopiers across the agency are accounted for and that any hard drives residing on these machines are tracked and properly sanitized or destroyed prior to disposal; (2) there are no policies documenting security measures to be taken for photocopiers utilized for general use nor are there procedures to ensure photocopier hard drives are sanitized or destroyed prior to disposal or at the end of the lease term; and (3) photocopier lease agreements and contracts did not include a "keep disk" or similar clause as required by NARA's policy. As a

# **AUDITS**

---

result of the lack of accountability and controls, NARA is at risk of inappropriate release of sensitive information and PII data that may be on photocopier hard drives. We made seven recommendations to assist in providing administrative, technical, and physical safeguards over sensitive information and PII that may be on photocopier hard drives. Management concurred with the seven recommendations. (OIG report 11-07, dated March 22, 2011)

## **Movement of Freight Shipments**

The review was initiated as a result of a fraud investigation performed by the OIG Office of Investigations. Specifically, in FY 2007, a Facilities and Personal Property Management Division (NAF) employee was indicted for theft of government property and conspiracy to embezzle \$958,280 from the United States. The employee was responsible for large transportation procurements and often circumvented NARA controls. The employee had authority to set up transportation service orders and to approve invoices for payment. The employee commonly used the same vendors over and over again. Management officials discarded other employees' complaints about this employee not following NARA controls.

The objective of the audit was to determine if controls are effective and efficient to ensure NARA obtains the best value and most economical prices for the movement of freight. We found NARA has taken several significant steps to improve controls since FY 2007. Controls over separation of duties were implemented. The person requesting freight shipments is not the same person setting up the transportation order in the General Services Administration's (GSA) Transportation Management Services System, and is also different from the person authorized to approve freight invoices for payment. A NAF manager tracks all transportation transactions from inception through payment, reviews invoices after U.S. Transportation Consultants (USTC) audits the invoice, and reviews transactions to ensure vendors are rotated. The results of our testing indicate the separation of controls over requesting freight and shipping service, setting up the obligation, and approving payment are working effectively. The transactions tested were appropriately pre-audited by USTC before payment and reported to GSA in the required quarterly reports. However, we could not come to the same conclusion in our test work in determining whether NAF selected the Transportation Service Provider (TSP) that provided the best value to the government. NAF is working to track reasons why TSP's with a lower price were not selected.

Since the investigation, NAF has implemented stronger controls over freight and shipping. We believe NARA is on the right track in continuing to improve controls over transportation services. We made three recommendations which, when implemented by management, will assist the agency in enhancing controls in freight management. (OIG Report #11-01, dated November 3, 2010.)

## **NARA's Fiscal Year 2010 Financial Statements**

Cotton & Company LLP (C&C), a public accounting firm, audited NARA's Consolidated Balance Sheets as of September 30, 2010 and the related Statement of Net Cost, Changes in Net Position and Budgetary Resources, for the year then ended.

# AUDITS

---

C&C issued NARA an unqualified opinion on NARA's FY 2010 financial statements. This is the fifth year in a row NARA received an unqualified opinion. For FY 2010, C&C reported one significant deficiency in internal control over financial reporting in the area of Information Technology resulting in four recommendations that, if implemented, should correct the matters reported. C&C disclosed no material weaknesses and no instances of noncompliance with certain provisions of laws and regulations. Management concurred with the recommendations.

We monitored C&C's performance of the audit to ensure it is conducted in accordance with the terms of the contract and in compliance with Government Accountability Office (GAO) *Government Auditing Standards* and other authoritative references, such as OMB Bulletin No. 07-04, Audit Requirements for Federal Financial Statements. We are involved in the planning, performance, and reporting phases of the audit through participation in key meetings, discussion of audit issues, and reviewing of C&C's work papers and reports. Our review disclosed no instances wherein C&C did not comply, in all material respects, with the contract or *Government Auditing Standards*. (OIG Report #11-04, dated November 26, 2010.)

# ***INVESTIGATIONS***

---

## **Investigations Overview**

During this reporting period, the Office of Investigations (OI) opened eight investigations and closed 19 investigations, four of which are closed pending an administrative response from NARA. The OI also received 46 complaints and closed 51 complaints, six of which are closed pending an administrative response from NARA. More than 1,100 NARA holdings were recovered during the period. The OI worked with the IRS and the Naval Criminal Investigative Service, as well as the Offices of Inspectors General at the Veterans Administration and the Government Printing Office. The OI also worked with a number of local and state law enforcement entities to include: Office of the States Attorney in Cook County, Illinois, DC Metro Police Department, Montgomery County Maryland Police Department and the Maryland States Attorney's Office. At the close of the period, there remained 56 open complaints and 23 open investigations.

## **Updates on Previously Reported Investigations**

### **Alleged Wire Fraud, Theft of Public Money, Money Laundering**

A former NARA employee plead guilty to theft of public money and was sentenced to 15 months in prison and full restitution for his role in a scheme to embezzle \$958,280 from NARA. His co-conspirator, a former NARA contractor, also plead guilty and received the same sentence during the previous reporting period.

### **Mishandling of Classified Documents**

Continuing security violations at the Washington National Records Center (WNRC) prompted the Office of Inspector General to initiate an investigation in the interest of National Security. Pursuant to the completion of an inventory at NARA's Suitland facility of Top Secret and/or Restricted Data materials, 81 boxes of this material remain missing. This investigation was closed subject to continuing updates regarding the recovery of remaining material.

### **Counterfeit/Grey Market IT Contract Fraud**

An IT contractor provided NARA with counterfeit and "grey market," or resold equipment in violation of the contract terms. The case was ultimately declined for prosecution, but resulted in the prevention of a \$1.1 million procurement for grey market and counterfeit IT equipment. The case is being prepared for referral to NARA for a suspension/debarment determination.

### **Grey Market Server Components**

NARA's acquisitions division notified OIG that Hewlett Packard (HP) server components procured from a vendor had been identified as potentially grey market products in violation of NARA's contract. Ninety-six of 121 pieces were identified by OIG as grey market. The remaining pieces could not be identified. The contract was terminated. The Computer Crime and Intellectual Property Section of the U.S. Department of Justice declined prosecution, but the investigation prevented a \$91,000 fraudulent procurement.

# **INVESTIGATIONS**

---

## **False Billing**

The subject company was initially investigated for allegations of a bid-rigging scheme to steer government contracts to the subject company and its alleged co-conspirators. While that charge was not substantiated and prosecution was declined by an Assistant United States Attorney, a civil case remains pending for an outstanding debt of more than \$250,000 owed to NARA.

## **Alienated Lincoln Document**

An endorsement by President Lincoln on a letter was offered for sale by an autograph dealer. The document included markings indicating it was a federal record. The markings were consistent with a NARA record group, and the OIG's Archival Recovery Team referred this case to NARA recommending it be recovered and returned to NARA's holdings. The Archival Recovery Team is working with NARA's Office of General Counsel to recover the document.

## **Harassing Phone Calls**

A NARA employee received multiple threatening phone calls from an individual. The subject was contacted but refused to stop making the calls. The local jurisdiction accepted the case for prosecution and the subject was subsequently arrested, but failed to show for her court appearance. She was found guilty in absentia and an arrest warrant was issued. Upon her arrest, the subject was placed in pretrial confinement. Because her pretrial confinement reached an equivalent duration of the statutory maximum in the local jurisdiction, the judge dismissed the case.

## **Inappropriate Security of NARA System Passwords**

During the course of routine audit work, OIG personnel discovered a file containing passwords to NARA system servers. NARA took steps to prevent future disclosure of such a file and indicated the password policy was under review and subject to future changes to prevent recurrence of such an incident.

## **Veteran Record Fraud**

A local chapter of the Military Order of the Purple Heart alleged an individual was misrepresenting his service record. In an attempt to verify his record, the individual fabricated NARA letterhead and a NARA record form. This case is being investigated jointly with the Veterans Administration OIG, and remains open and ongoing.

## **Misconduct at Presidential Library Gift Shop**

When there was a shortage of funds from a Presidential Library gift shop cash register, the gift shop supervisor failed to notify library management and asked staff to contribute personal funds to cover the shortage. An investigation substantiated theft was occurring at the gift shop, and a subject, not the supervisor, was identified. The subject ultimately confessed to theft, and the case was accepted for prosecution by the local district attorney's office. Both the subject employee and the supervisor were reprimanded.

## **Rape/Identify Theft**

OIG joined with the Baltimore County Police Department in the investigation of a rape allegation against a NARA employee. The rape allegation was subsequently disproved.

# ***INVESTIGATIONS***

---

However, the subject employee corresponded with the alleged victim using another NARA employee's identity and inappropriately used a NARA computer. These parts of the case were referred to NARA for administrative action. The subject was reprimanded for improper use of a NARA computer.

## **Grand Jury Secrecy and Record Recovery**

Potential grand jury and other federal records were inappropriately donated to an institution outside of the federal government more than 30 years ago. These records were brought to NARA's attention by a researcher doing work on the particular subject matter at the outside institution. The case was referred to the Department of Justice due to the potential of exposure of grand jury information. NARA archivists reviewed the material and negotiation of terms for the return of the material are underway.

## **Wrongful Access to IRS Records in Transit**

The lock and seal on storage containers containing IRS records shipped to a NARA federal records center were missing. There was no evidence the records in the container had been damaged. While the investigation was ongoing a subsequent incident occurred. Investigation revealed unknown persons were breaking into freight cars at a rail yard searching for merchandise to steal and resell. The case was referred to NARA to implement tighter security of these shipments. NARA changed to the use of a more sophisticated lock for the containers and made incremental changes in the Statements of Work between NARA and the IRS and between NARA and its respective shipping companies to prevent this from recurring.

## **Credit Card Theft**

A NARA employee reported the theft of personal credit cards on NARA premises. While the theft did occur, it could not be determined that it took place on NARA property. Two subjects were arrested for using the stolen credit cards. The case was accepted for prosecution by the local jurisdiction.

## **New Investigation Highlights**

### **Employee Misconduct/Threats**

A NARA employee inappropriately referenced a recent shooting incident in official email correspondence and made a variety of veiled threats toward NARA. The case was referred to NARA for appropriate administrative action. The employee was counseled.

### **Stolen Microfilm**

A NARA employee inappropriately removed 152 microfilm rolls from NARA and stored them in an assigned personal locker. The subject confessed to taking the microfilm, as well as two NARA ledgers. The case was declined for criminal prosecution by the jurisdictional Assistant United States Attorney. The subject was placed on administrative leave and subsequently resigned in lieu of further administrative action.

### **Altered Lincoln Record**

A researcher, known to have accessed a particular Lincoln pardon, confessed to altering the date of the pardon accompanying Lincoln's signature. The case was declined for criminal

# ***INVESTIGATIONS***

---

prosecution because the act occurred outside of the statute of limitations for this offense. The researcher was barred from NARA facilities.

## **Missing Presidential Photograph**

Prints from a missing negative of a particular photograph of President Kennedy, which had been kept by an official White House Photographer, were put up for sale in California by a private filmmaker. Whereabouts of the negative are presently unknown, but it is believed to be NARA property. This investigation remains open and ongoing.

## **Stolen NARA records**

A former NARA employee is alleged to have stolen multiple NARA records while employed at the Archives. Many of these records were recovered during the reporting period. The case has been accepted for prosecution by the jurisdictional Assistant United State Attorney. The investigation remains open and ongoing.

## **External Access of Child Pornography**

A NARA employee was alleged to be accessing child pornography from his home computer by an external law enforcement entity. An examination of the employee's NARA computer found no indication that child pornography was accessed from the workplace. The case has been accepted by the jurisdictional Assistant United State Attorney and remains open and ongoing.

## **Other Office of Investigation Activity**

### **Archival Recovery Team**

During this period, the Archival Recovery Team (ART) fielded 17 complaints and opened four investigations. Eleven complaints and one investigation were closed. In addition, six non-criminal ART cases were referred to NARA for a recovery determination, or to external entities of primary jurisdiction. At the close of the period, 25 ART complaints and seven ART investigations remained open. During the period 1,152 NARA holdings were recovered.

- **Social Media:** The ART facebook page reflected continued growth totaling nearly 1,400 "friends" at the close of the reporting period. The site updates the public about upcoming shows and happenings with the ART, along with other newsworthy items about document thefts, investigations, and recoveries at NARA and other institutions worldwide. Visit the site at <http://www.facebook.com/archivalrecoveryteam>.
- **Other Media:** The work of ART appeared in a variety of publications around the country during the period. Additionally, ART was featured in *The Washington Post*, on C-Span, and on National Public Radio. ART staff, along with the Inspector General, participated in a panel discussion on holdings security with the Inspectors General from the Library of Congress and the Smithsonian Institute, as well as NARA's own Holdings Protection Team.

# INVESTIGATIONS

---

- **Outreach:** As part of the ART's outreach program working with individuals and groups who may have interactions with historic records, Office of Investigations staff participated in the following shows:
  - Papermania, Hartford, Connecticut
  - The Show of Shows, Louisville, Kentucky
  - Baltimore Arms Collector Show, Baltimore, Maryland
  - The Civil War Show, Fredericksburg, Virginia
  - The Civil War Symposium, Atlanta, Georgia

## Computer Crimes Unit

During the reporting period, the Computer Crimes Unit (CCU) provided digital forensic support to several criminal investigations, including:

- The CCU participated in the execution of a search warrant during which several computers, external storage devices, and other digital equipment and media were seized. Ultimately, the CCU obtained and processed over three terabytes of digital evidence in support of this investigation. The examination of evidence in this matter is ongoing.
- The CCU obtained, processed, and examined over 500 gigabytes of digital evidence from three computer workstations and a GroupWise email account in support of a Naval Criminal Investigative Service (NCIS) child pornography investigation.
- The CCU provided support to two investigations being conducted by the Government Printing Office (GPO) OIG. In one case, the CCU obtained and examined over 300 gigabytes of digital evidence from two laptop computers as part of an employee embezzlement investigation. In the other, the CCU copied subpoena response material related to a procurement fraud case in a forensically sound manner.

In addition to providing forensic support to investigations, the CCU also visited the Financial Crime Enforcement Network (FinCEN) operated by the Department of the Treasury on several occasions to run database searches related to criminal investigations. During the reporting period a forensic examiner obtained the Certified Forensic Computer Examiner (CFCE) certification offered by the International Association of Computer Investigative Specialists (IACIS).

# INVESTIGATIONS

---

## OIG Hotline

The OIG Hotline provides a confidential channel for reporting fraud, waste, abuse, and mismanagement to the OIG. In addition to receiving telephone calls at a toll-free Hotline number and letters to the Hotline post office box, we also accept e-mail communication from NARA's internal network or the Internet through the Hotline e-mail system. Walk-ins are always welcome. Visit <http://www.archives.gov/oig/> for more information, or contact us:

- **By telephone**  
Washington, DC, Metro area: (301) 837-3500  
Toll-free and outside the Washington, DC, Metro area: (800) 786-2551
- **By mail**  
NARA OIG Hotline  
P.O. Box 1821  
Hyattsville, MD 20788-0821
- **By e-mail**  
[oig.hotline@nara.gov](mailto:oig.hotline@nara.gov)
- **By online referral form**  
<http://www.archives.gov/oig/referral-form/index.html>

The Office of Investigations promptly and carefully reviews calls, letters, and e-mail to the Hotline. We investigate allegations of suspected criminal activity or civil fraud and conduct preliminary inquiries on non-criminal matters to determine the proper disposition.

Where appropriate, referrals are made to the OIG audit staff, NARA management, or external authorities. Hotline contacts are captured as complaints in the Office of Investigations. The following table summarizes complaints received and Hotline activity for this reporting period:

Complaints received	46
Complaints closed pending response from NARA	6
Complaints closed final	45
Complaints open to Investigations	3

## Contractor Self Reporting Hotline

To comply with the self-reporting requirements in the Federal Acquisition Regulation, a web-based form has been created to allow NARA contractors to satisfy the requirement they notify the OIG, in writing, whenever the contractor has credible evidence that a principal, employee, agent, or subcontractor of the contractor has committed a violation of the civil False Claims Act or a violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations in connection with the award, performance, or closeout of a contract or any related subcontract. The form can be accessed through the OIG's home page, or found directly at: <http://www.archives.gov/oig/contractor-form/index.html>

# ***TOP TEN MANAGEMENT CHALLENGES***

---

## **Overview**

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 our mission and help NARA achieve its strategic goals, we have aligned our programs to focus on areas we believe represent the agency's most significant challenges. We have identified those areas as NARA's top ten management challenges.

Based on Congressional interest, GAO conducted an evaluation of NARA's Information Security Program and NARA's ability to effectively carry out its mission of overseeing the management of Federal records while preserving those of historic and intrinsic value. Final reports from these audits were not issued during the reporting period, and they may impact management challenges.

### **1. Electronic Records Archives**

NARA's mission with the Electronic Records Archives (ERA) is to build a system accommodating the government's vast amounts of electronic records stored in past, present, and future formats. The challenge is to deliver and maintain a functional system for preserving and providing access to our nation's electronic records for as long as needed. Electronic records are vital to how our government works, and their preservation through the ERA will define what information future generations will be able to access and use. However, the ERA Program has experienced delivery delays, budgeting problems, and contractor staffing problems. Initial Operating Capacity (IOC) for the ERA Program was delayed from September 2007 until June 2008, and even then program functions available at IOC were less than the original requirements. Also, the component to handle all White House records, the Executive Office of the President (EOP) System, was separated out due to delays, and pursued down a separate line of development. The success of this mission-critical program is uncertain. NARA staff was not able to clearly define what the ERA Program would be able to do, or what functions it would provide to NARA, when the program was scheduled to reach Full Operating Capability in 2012.

In August 2010, OMB placed the ERA Program on its high-priority list of 26 high-risk IT projects selected from across the Federal government. The major problems NARA must remedy for ERA are the lack of detailed plans for the final two increments, low usage of the system, and need for improved strategic planning. NARA's actions planned to correct these problems include preparing a detailed plan that focuses on accelerated user adoption of the ERA System, and updating ERA implementation plans to reflect an end to system development on September 30, 2011. System development had been planned to extend through March 2012. As a result of unknown funding levels and the decision by OMB to end ERA development at the end of FY 2011, NARA is planning on deferring implementation of 20 percent of the original system requirements. Agency officials reported that, as of the beginning of August 2010, 41 percent of the requirements have been implemented, and the plan is to have 80 percent implemented by the end of FY 2011.

# ***TOP TEN MANAGEMENT CHALLENGES***

---

## **2. Improving Records Management**

Part of NARA's mission is safeguarding and preserving the records of our government, thereby ensuring people can discover, use, and learn from this documentary heritage. NARA provides continuing access to the essential documentation of the rights of American citizens and the actions of their government. The effective management of these records is key to accomplishing this mission. NARA must work with Federal agencies to ensure the effective and efficient appraisal, scheduling, and transfer of permanent records, in both traditional and electronic formats. The major challenge is how best to accomplish this component of our overall mission while reacting and adapting to a rapidly changing technological environment in which electronic records, particularly e-mail, proliferate. In short, while the ERA system is intended to work with electronic records received by NARA, we need to ensure the proper electronic and traditional records are in fact preserved and sent to NARA in the first place.

NARA also directs the Electronic Records Management (ERM) initiative, one of 24 government-wide initiatives under the E-Government Act of 2002. The ERM initiative will provide guidance to agencies in managing and transferring their permanent electronic records to NARA, in an increasing variety of data types and formats. In June 2008, GAO recommended NARA develop and implement an approach to provide oversight of agency electronic records management programs, to provide adequate assurance that NARA guidance is effective and the agencies are following electronic records guidance. NARA, its Government partners, and Federal agencies are challenged with determining how best to manage electronic records and how to make ERM and e-Government work more effectively.

## **3. Information Technology Security**

The Archivist identified IT Security as a material weakness under the Federal Managers' Financial Integrity Act reporting process beginning in 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) in FY 2007. The assessment stated NARA's policy and supporting procedures for IT security were weak, incomplete, and too dispersed to be effective. Twelve of the 29 weaknesses identified during the assessment remain open.

IT security continues to present major challenges for NARA, including physical security of IT hardware and technical vulnerabilities within our electronic systems themselves and how NARA operates them. The confidentiality, integrity, and availability of our electronic records and information technology systems are only as good as our IT security infrastructure. A GAO review conducted in 2010 identified significant weaknesses in access controls, and other information security controls, impairing NARA's ability to ensure the confidentiality, integrity, and availability of its information systems. Each year, risks and challenges to IT security continue to be identified. NARA must ensure the security of its data and systems or risk undermining the agency's credibility and ability to carry out its mission.

## **4. Expanding Public Access to Records**

The records of a democracy's 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

# ***TOP TEN MANAGEMENT CHALLENGES***

---

can provide access. Unfortunately, over half of NARA's textual holdings have not been processed to allow efficient and effective access to these records. To meet its mission, NARA must work to ensure it has the processes and resources necessary to establish intellectual control over this backlog of unprocessed records.

Another challenge for NARA, given society's growing expectation for easy and near-immediate access to information on-line, will be to provide such access to records created digitally (i.e., "born digital") and to identify those textual records most in demand so they can be digitized and made available electronically. NARA's role in ensuring the timeliness and integrity of the declassification process of classified material held at NARA is also vital to public access.

## **5. 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 housing Federal records to meet defined physical and environmental requirements by FY 2009. NARA's challenge is to ensure its own facilities, as well as those used by other Federal agencies, are in compliance with these regulations; and effectively mitigate risks to records which are stored in facilities not meeting these new standards.

## **6. Preservation Needs of Records**

As in the case of our national infrastructure (bridges, sewer systems, etc.), NARA holdings grow older daily and face degradation associated with time. This affects both traditional paper records, and the physical media that electronic records and audio/visual records are stored on. In FY 2006 NARA downgraded preservation from a material weakness under the Federal Managers' Financial Integrity Act reporting process to a reportable condition. However, in FY 2010, preservation was once again elevated to a material weakness. NARA should be commended for taking this step, but much work remains to be done. Preserving and providing access to records is a fundamental element of NARA's duties to the country, and NARA cannot provide access to records unless it can preserve them for as long as needed. The backlog of records needing preservation action continues to grow. NARA is challenged to address this backlog and future preservation needs, including the data integrity of electronic records. The challenge of ensuring NARA facilities meet environmental standards for preserving records (see OIG Challenge #5) also plays a critical role in the preservation of Federal records.

## **7. Improving Project Management**

Effective project management, particularly for IT projects, 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, analyzing and testing to support acquisition and deployment of the systems, and providing oversight to ensure effective or efficient results within costs. Currently, IT systems are not always developed in accordance with established NARA guidelines. These projects must be better managed and tracked to ensure cost, schedule, and performance goals are met.

# ***TOP TEN MANAGEMENT CHALLENGES***

---

GAO reports NARA has been inconsistent in its use of earned value management (EVM), a project management approach providing objective reports of project status and early warning signs of cost and schedule overruns. As a result, NARA did not fully implement practices necessary to make effective use of EVM, limiting the reliability of its progress reports.

GAO also reported NARA does not document the results of briefings to its senior management oversight group, and thus there is little evidence this body reviewed and approved the progress of the ERA Program. There is also little evidence the group identified or took appropriate corrective actions, or ensured such actions were taken and tracked to closure. Without adequate oversight evaluating project progress, including documenting feedback and action items from senior management, NARA will not be able to ensure ERA is being implemented at acceptable cost and within reasonable and expected time frames.

Inconsistent use of key project management disciplines like Earned Value Management limits NARA's ability to effectively manage projects and accurately report on their progress.

## **8. Physical and Holdings Security**

The Archivist has identified security of collections as a material weakness under the FMFIA reporting process. Document and artifact theft is not a theoretical threat; it is a reality NARA has been subjected to time and time again. 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 security realities facing this nation and the risk our holdings may be pilfered, defaced, or destroyed by fire or other man-made and natural disasters. Not only do NARA's holdings have immense historical and financial value, but we hold troves of national security information as well. Developments such as the creation of the Holdings Protection Team and implementation of stricter access controls are welcome additions to NARA's security posture and should be commended. However, NARA must continually strive to improve in this area.

## **9. Contract Management and Administration**

The GAO has identified Commercial Services Management (CSM) as a government-wide initiative. The CSM initiative includes enhancing the acquisition workforce, increasing competition, improving contract administration skills, improving the quality of acquisition management reviews, and strengthening contractor ethics requirements. Effective contract management is essential to obtaining the right goods and services at a competitive price to accomplish NARA's mission. NARA is challenged to continue strengthening the acquisition workforce and to improve the management and oversight of Federal contractors. NARA is also challenged with reviewing contract methods, to ensure a variety of procurement techniques are properly used in accordance with Federal laws and regulations.

## **10. Strengthening Human Capital**

The GAO has identified human capital as a government-wide high risk, explaining it is critical to ensure agencies have the talent and skill mix they need to address their current and emerging human capital challenges. In August 2009, NARA published its first Strategic Human Capital Plan (SHCP), covering FYs 2009 through 2014. The SHCP discusses strategies for achieving

# *TOP TEN MANAGEMENT CHALLENGES*

---

each of its five human capital goals. However, NARA has yet to develop an agency-wide workforce plan. Based on NARA's SHCP, the agency is supposed to develop and deploy an integrated workforce plan enabling it to hire and retain "the right talent, at the right time, in the right place," by December 31, 2014. While NARA should be commended for some accomplishments, such as implementing their 2010 Hiring Reform Action Plan, more work remains to be done.

Recently the Partnership for Public Service ranked NARA very low in its "Best Places to Work in the Federal Government" rankings. The rankings are based on employee responses to the Federal Human Capital Survey (FHCS) administered biannually by the U.S. Office of Personnel Management (OPM). In response, NARA created an Employee Viewpoint Survey Task Force and conducted a survey to gather feedback and ideas. This information is being used to help transform NARA and address employee concerns during the current major reorganization. NARA's challenge is to adequately address its workforce's concerns and assess its human capital needs in order to effectively recruit, retain, and train people needed to achieve its mission, both now and in the future.

# ***REPORTING REQUIREMENTS***

---

## **MANDATED BY THE INSPECTOR GENERAL ACT OF 1978, AS AMENDED, AND OTHER LAWS**

<b><u>REQUIREMENT</u></b>	<b><u>SUBJECT</u></b>	<b><u>PAGE(s)</u></b>
Section 4(a)(2)	Review of legislation and regulations	6, 9
Section 5(a)(1)	Significant problems, abuses, and deficiencies	2 – 4, 13 – 18, 19 – 22
Section 5(a)(2)	Significant recommendations for corrective action	2 – 4, 13 – 18
Section 5(a)(3)	Prior significant recommendations unimplemented	35
Section 5(a)(4)	Summary of prosecutorial referrals	32 – 33
Section 5(a)(5)	Information or assistance refused	35
Section 5(a)(6)	List of reports issued	33
Section 5(a)(7)	Summaries of significant reports	2 – 4, 13 – 18
Section 5(a)(8)	Audit Reports—Questioned costs	34
Section 5(a)(9)	Audits Reports—Funds put to better use	35
Section 5(a)(10)	Prior audit reports unresolved	35
Section 5(a)(11)	Significant revised management decisions	35
Section 5(a)(12)	Significant revised management decisions with which the OIG disagreed	35
P.L. 110-181	Annex of completed contract audit reports	34
P.L. 111-203	Reporting on OIG peer review	10

# REPORTING REQUIREMENTS

## STATISTICAL SUMMARY OF INVESTIGATIONS

<i>Investigative Workload</i>	
Complaints received this reporting period	46
Investigations pending at beginning of reporting period	29
Investigations opened this reporting period	8
Investigations closed this reporting period	19
Investigations carried forward this reporting period	23
<i>Categories of Closed Investigations</i>	
Fraud	1
Conflict of Interest	0
Contracting Irregularities	4
Misconduct	6
Larceny (theft)	3
Other	5
<i>Investigative Results</i>	
Cases referred – accepted for prosecution	1
Cases referred – declined for prosecution	2
Cases referred – pending prosecutive decision	1
Arrest	0
Indictments and informations	0
Convictions	2
Fines, restitutions, judgments, and other civil and administrative recoveries	4
NARA holdings recovered	1,152
<i>Administrative Remedies</i>	
Employee(s) terminated	0
Employee(s) resigned in lieu of termination	2
Employee(s) suspended	0
Employee(s) given letter of reprimand or warnings/counseled	3
Employee(s) taking a reduction in grade in lieu of administrative action	0
Contractor (s) removed	1
Individual(s) barred from NARA facilities	2

# REPORTING REQUIREMENTS

---

## SUMMARY OF PROSECUTORIAL REFERRALS Requirement 5(a)(4)

### Accepted for Prosecution

#### **Harassing Phone Calls**

A NARA employee received multiple threatening phone calls from an individual. The subject was contacted but refused to stop making the calls. The local jurisdiction accepted the case for prosecution and the subject was subsequently arrested, but failed to show for her court appearance. She was found guilty in absentia and an arrest warrant was issued. Upon her arrest, the subject was placed in pretrial confinement. Because her pretrial confinement reached an equivalent duration of the statutory maximum in the local jurisdiction, the judge dismissed the case.

#### **Misconduct at Presidential Library Gift Shop**

When there was a shortage of funds from a Presidential Library gift shop cash register, the gift shop supervisor failed to notify library management and asked staff to contribute personal funds to cover the shortage. An investigation substantiated theft was occurring at the gift shop and a subject, not the supervisor, was identified. The subject ultimately confessed to theft, and the case was accepted for prosecution by the local district attorney's office. Both the subject employee and the supervisor were reprimanded.

#### **Credit Card Theft**

A NARA employee reported the theft of personal credit cards on NARA premises. While the theft did occur, it could not be determined it took place on NARA property. Two subjects were arrested for using the stolen credit cards. The case was accepted for prosecution by the local jurisdiction.

#### **Stolen NARA records**

A former NARA employee is alleged to have stolen multiple NARA records while employed at the Archives. Many of these records were recovered during the reporting period. The case has been accepted for prosecution by the jurisdictional Assistant United State Attorney. The investigation remains open and ongoing.

### Declined for Prosecution

#### **Stolen Microfilm**

A NARA employee inappropriately removed 152 microfilm rolls from NARA and stored them in an assigned personal locker. The subject confessed to taking the microfilm, as well as two NARA ledgers. The case was declined for criminal prosecution by the jurisdictional Assistant United States Attorney. The subject was placed on administrative leave and subsequently resigned in lieu of further administrative action.

#### **Altered Lincoln Record**

A researcher, known to have accessed a particular Lincoln pardon confessed to altering the date of the pardon accompanying Lincoln's signature. The case was declined for criminal prosecution because the act occurred outside of the statute of limitations for this offense. The researcher was barred from NARA facilities.

# REPORTING REQUIREMENTS

## Pending Prosecutorial Determination

### **Grand Jury Secrecy and Record Recovery**

Potential grand jury and other federal records were inappropriately donated to an institution outside of the federal government more than 30 years ago. These records were brought to NARA's attention by a researcher doing work on the particular subject matter at the outside institution. The case was referred to the Department of Justice due to the potential of exposure of grand jury information. NARA archivists reviewed the material and negotiation of terms for the return of the material are underway.

### **LIST OF REPORTS ISSUED Requirement 5(a)(6)**

<b>Report No.</b>	<b>Title</b>	<b>Date</b>	<b>Questioned Costs</b>	<b>Unsupported Costs</b>	<b>Funds Put to Better Use</b>
11-01	Audit of NARA's Movement of Freight Shipments	11/03/2010	0	0	0
11-02	Clifton Gunderson LLP Network Vulnerability Assessment and Penetration Testing	11/08/2010	0	0	0
11-03	Audit of NARA's Oversight of Selected Grantees' Use of Grant Funds	02/16/2011	0	0	\$434,589
11-04	Cotton & Company's NARA FY 2010 Financial Statements Independent Audit Report	11/26/2010	0	0	0
11-05	Audit of NARA's Security Guard Contract for AI and AII	02/18/2011	0	0	0
11-06	Audit of the NARANET Server Upgrade Project	11/30/2010	0	0	0
11-07	Audit of NARA's Photocopier Security	03/22/2011	0	0	0
11-09	Follow-Up Audit of NARA's Work-At-Home System	01/31/2011	0	0	0
11-10	Audit of the Controls over Inappropriate Personal Use of the Internet at NARA	03/09/2011	0	0	0
11-11	System Review Report on the Appalachian Regional Commission's Office of Inspector General Audit Organization	03/18/2011	0	0	0

# REPORTING REQUIREMENTS

## AUDIT REPORTS WITH QUESTIONED COSTS

### Requirement 5(a)(8)

Category	Number of Reports	DOLLAR VALUE	
		Questioned Costs	Unsupported Costs
A. For which no management decision has been made by the commencement of the reporting period	1	\$27,159	\$27,159
B. Which were issued during the reporting period	0	0	0
Subtotals (A + B)	1	\$27,159	\$27,159
C. For which a management decision has been made during the reporting period	0	0	0
(i) dollar value of disallowed cost	0	0	0
(ii) dollar value of costs not disallowed	0	0	0
D. For which no management decision has been made by the end of the reporting period	1	\$27,159	\$27,159
E. For which no management decision was made within 6 months	1	\$27,219	\$27,159

## ANNEX ON COMPLETED CONTRACT AUDIT REPORTS

Section 845 of the 2008 Defense Authorization Act, Public Law 110-181, requires certain information on completed contract audit reports containing significant audit findings be included as an annex to this report. While the OIG completed audits on the ERA and other contracts during this period, they were generally program audits as opposed to contract audits, and the DCAA audits of the ERA program this period do not rise to the level of Section 845 requirements.

# REPORTING REQUIREMENTS

## AUDIT REPORTS WITH RECOMMENDATIONS THAT FUNDS BE PUT TO BETTER USE Requirement 5(a)(9)

CATEGORY	NUMBER	DOLLAR VALUE
A. For which no management decision has been made by the commencement of the reporting period	0	0
B. Which were issued during the reporting period	1	\$434,589
Subtotals (A + B)	1	\$434,589
C. For which a management decision has been made during the reporting period	0	0
(i) dollar value of recommendations that were agreed to by management	0	0
Based on proposed management action	0	0
Based on proposed legislative action	0	0
(ii) dollar value of recommendations that were not agreed to by management	0	0
D. For which no management decision has been made by the end of the reporting period	1	\$434,589
E. For which no management decision was made within 6 months of issuance	0	0

## OTHER REQUIRED REPORTS

REQUIREMENT	CATEGORY	SUMMARY
5(a)(3)	Prior significant recommendations unimplemented	None
5(a)(5)	Information or assistance refused	None
5(a)(10)	Prior audit reports unresolved	None
5(a)(11)	Significant revised management decisions	None
5(a)(12)	Significant revised management decisions with which the OIG disagreed	None