



NATIONAL
ARCHIVES

NATIONAL ARCHIVES
OFFICE *of* INSPECTOR GENERAL

**ANNUAL AUDIT
WORK PLAN**

FISCAL YEAR 2013

FOREWORD

I am pleased to present the Fiscal Year (FY) 2013 Audit Work Plan for the National Archives and Records Administration (NARA) Office of Inspector General (OIG). This document describes how the OIG Office of Audits will achieve its mission of helping the agency effectively carry out its responsibilities by promoting economy, efficiency, and effectiveness in the administration of, and to prevent and detect fraud, waste, and abuse in NARA programs and operations. According to the Archivist of the United States:

NARA's role in our democracy is clear and simple—we are the nation's record keeper. We safeguard and preserve the records of our national government so our citizens can use them and learn from them now and many years from now.

The OIG prepared this Work Plan with the agency's mission in mind, and aligned our Work Plan with both NARA's Strategic Plan, and NARA's six defined Transformational Outcomes.

This plan reflects priority work the OIG believes is necessary to provide effective oversight of the broad spectrum of NARA programs and operations. Our planning efforts reflect direct outreach and solicitation of topics and assignment suggestions from NARA's leadership, external stakeholders, and our staff while including our oversight requirements. Successful execution will reflect our demonstrated ongoing commitment to provide high-quality service to our customers while assisting NARA in meeting its strategic mission and objectives.

Overall this plan is a projection of what we would like to accomplish in FY 2013. It is ambitious, and we realize it may not be fully completed or may be modified. Further, it should not be viewed as limiting our office to these specific topics, as other issues may certainly rise in importance and require our resources.

I wish to thank each member of NARA's leadership, as well as external stakeholders and our staff for their direct participation in this process. I look forward to a successful year of providing high quality audit and investigative support and service to NARA and our stakeholders.



James Springs
Acting Inspector General

TABLE OF CONTENTS

Foreword	1
2013 Listing of Audit Assignments	3
Audit Summaries	4
Additional Activities for FY 2013	19
Attestation Engagements.....	19
Non-audit Services	19
Peer Review	19
Background	20
Glossary	22

2013 LISTING OF AUDIT ASSIGNMENTS

FINANCIAL AUDIT

Consolidated Audit of NARA’s Financial Statements	4
---	---

COMPLIANCE/REGULATORY AUDITS

Evaluation of NARA’s Compliance with the Federal Information Security	4
Management Act (FISMA)	
Audit of NARA’s Compliance with HSPD-12 Policy for a Common Identification	5
Standard for Federal Employees and Contractors	
Audit of NARA’s Compliance with Improper Payments Elimination and Recovery Act...	5

IT AUDITS

Audit of the Electronic Records Archive Program	6
Audit of NARA’s Cloud Computing Efforts	7
Assessment of NARA’s Backup Operations	8
Audit of NARA’s Wireless Network	9
Audit of NARA’s Monitoring of Computer Security Incidents.....	9
Audit of Controls over Mobile Devices	10

PROGRAM AUDITS

Audit of NARA’s Preservation Program	10
Audit of NARA’s Processing Program.....	11
Audit of Management Controls Over the Declassification and Reclassification.....	12
of Holdings	
Evaluation of Original Classification Actions	13
Audit of Selected Aspects of NARA’s Digitization Program.....	13
Audit of Management Controls over Specially Protected Records	14
Audit of NARA’s Continuity of Operations Plan (COOP).....	14
Audit of Contractor Access to NARA’s Network and Facilities	15
Audit of NARA’s Social Media Program	15
Audit of Controls Associated with Review and Certification of Records Storage.....	16
Facilities	
Audit of the NARA’s Exit Clearance Process	16
Audit of Rental Payments to Federal Agencies (Other than GSA).....	17
Audit of Selected Procurement and Contract Management Practices and Functions	18

AUDITS

Consolidated Audit of NARA's Financial Statements

Background: The Accountability of Tax Dollars Act of 2002 requires all executive agencies with a budget authority in excess of \$25 million to prepare financial statements, subject them to an independent audit, and send them to the Congress and the Office of Management and Budget (OMB). This improves the ability of the Congress to monitor how tax dollars are spent and ensure resources are allocated in the most efficient manner. The OIG, in concert with management, contracts for this requirement with the OIG serving as the Contracting Officer's Technical Representative (COTR). The contract requires the contractor to conduct an audit of, and report on, NARA's consolidated financial statements for FY 2013 in accordance with the *Generally Accepted Government Auditing Standards* (GAGAS) and OMB Bulletin 07-04, "Audit Requirements for Federal Financial Statements."

Objective: To render an opinion on whether NARA's consolidated financial statements are presented fairly in all material respects. The contractor will issue reports on its conclusion based on the testing of internal controls and compliance with laws and regulation.

Scope: The OIG will monitor and review the contractor's effort, to determine whether the contractor complied with GAGAS and OMB Bulletin 07-04.

Estimated Staff Days: 90

Locations: Chief Financial Officer (BC), Financial Reports (BCF) and Information Services (I) at Archives II. Bureau of Public Debt, Parkersburg, WV

Evaluation of NARA Compliance with the Federal Information Security Management Act of 2002 (FISMA)

Background: FISMA requires Federal agencies to establish agency-wide risk-based information security programs including periodic risk assessments, use of controls and techniques to comply with information security standards, training requirements, periodic testing and evaluation, reporting, plans for remedial action, security incident response, and continuity of operations. The Act also requires annual independent evaluation of Federal agency information security programs and practices. Agency information security activities are guided by OMB policy and information security standards developed by the National Institute of Standards and Technology (NIST).

Objective: To assess the adequacy of controls over information security and compliance with information security policies, procedures, standards, and guidelines. The project will include tests of the effectiveness of information security control techniques.

Scope: The OIG will use the Department of Homeland Security "Inspector General FISMA Reporting Metrics," in addition to OMB and NIST guidelines, in conducting this evaluation.

Estimated Staff Days: 90

Locations: Archives II, Office of Information Services (I).

Audit of NARA's Compliance with Homeland Security Presidential Directive (HSPD) -12 Policy for a Common Identification Standard for Federal Employees and Contractors

Background: The Cyberspace Policy Review, directed by the President and referenced in the President's Budget for Fiscal Year 2011, highlighted the importance of identity management in protecting the nation's infrastructure. HSPD-12 is a strategic initiative intended to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. HSPD-12 requires agencies to follow specific technical standards and business processes for the issuance and routine use of Federal Personal Identity Verification (PIV) smartcard credentials including a standardized background investigation to verify employees' and contractors' identities. Specific benefits of the standardized credentials required by HSPD-12 include secure access to federal facilities and disaster response sites, as well as multi-factor authentication, digital signature, and encryption capabilities. Additionally, standardization leads to reduced overall costs and better ability to leverage the Federal Government's buying power with industry.

Objective: To determine whether NARA has effectively complied with HSPD-12 and has implemented appropriate management controls.

Scope: The OIG will evaluate the agency's effort in implementing HSPD-12 against OMB and NIST requirements.

Staff Days: 90

Locations: Archives II, Office of Information Services (I)

Audit of NARA's Compliance with the Improper Payments Elimination and Recovery Act

Background: The Improper Payments Eliminations and Recovery Act (IPERA), P.L. 111-204, amended the Improper Payments Information Act of 2002 (IPIA). Agencies are now required to determine whether the risk of improper payments is significant, provide valid annual estimates of improper payments, and implement a plan to reduce improper payments. Further, agencies must report estimates of the annual amount of improper payments in programs and activities and progress in reducing them.

Agencies shall report to the President and the Congress through their annual Performance and Accountability Report (PAR) in the format required by OMB Circular A-136, Financial Reporting Requirements, for IPIA reporting. The report should include an estimate of the annual amount of improper payments for all programs and activities determined to be susceptible to significant improper payments.

To determine compliance we will review the agency's PAR (and any accompanying information) for FY 2013. Compliance with IPIA means the agency has:

- Published a PAR for the most recent fiscal year and posted that report and any accompanying materials required by OMB on the agency website;
- Conducted a program specific risk assessment for each program or activity that conforms with Section 3321 of Title 31 U.S.C. (if required);
- Published improper payment estimates for all programs and activities identified as susceptible to significant improper payments under its risk assessment (if required);
- Published programmatic corrective action plans in the PAR;
- Published, and has met, annual reduction targets for each program assessed to be at risk and measured for improper payments;
- Reported a gross improper payment rate of less than 10 percent for each program and activity for which an improper payment estimate was obtained and published in the PAR or APR; and
- Reported information on its efforts to recapture improper payments.

Objective: To determine NARA's compliance with IPIA as amended by IPERA.

Scope: The implementing guidance for IPERA is OMB Memorandum 11-16, Issuance of Revised Parts I and II of Appendix C of OMB Circular A-123 titled Management's Responsibility for Internal Control. The audit will be conducted at Archives II; will cover improper payments report in the FY 2012 annual Performance and Accountability Report.

Estimated Staff Days: 60

Mandated Due Date: 120 days after the applicable PAR, approximately March 15, 2013.

Locations: Budget and Finance (BCB) and other Archives II offices to be determined.

Audits of NARA's Electronic Records Archives (ERA) Program

Background: Increasingly, government records are created and maintained in electronic formats. These digital records pose a critical challenge for NARA. The agency views success in facing this challenge as entailing nothing less than building the archives of the future. According to NARA officials, unless the agency succeeds in surmounting this challenge, there will not be a National Archives of the United States for the digital era.

NARA is developing an ERA to respond effectively to the challenge posed by the diverse, complex, and enormous volume of electronic records being created today, and the rapidly changing nature of the systems used to create them. ERA will authentically preserve and provide access to any kind of electronic record, free from dependency on any specific hardware or software, thus enabling NARA to carry out its mission into the future.

As directed by OMB, ERA completed its development phase September 30, 2011 and is now in the Operations and Maintenance (O&M) phase. The volume of data, as well as the number of ERA users, is increasing. As of the end of FY 2012, all agencies are required to use the ERA System to submit permanent electronic records for transfer to NARA's legal custody. NARA plans on issuing Technical Direction Letters (TDL) to the O&M contractor to perform corrective and adaptive software maintenance in FY 2013. The TDLs will be used to address shortcomings and provide enhancements identified by customer Federal agencies, ensuring the long-term usability of the system. Of particular importance will be the system's ability to handle the increased volume of data and users in an efficient and effective manner. If the system is unable to ensure the continued existence, accessibility, and authenticity of records over time, NARA will have failed in meeting its mission regarding electronic records.

Objective: The OIG plans to monitor this program on an ongoing basis. Our objectives will be to evaluate ERA's ability to meet user needs, NARA's oversight of the ERA program, and to provide the Archivist with an independent assessment of this critical and highly-visible program. Due to our limited resources, we cannot audit all aspects of the ERA program. Therefore our efforts will concentrate on reviewing various more limited aspects of the ERA program as they are identified and prioritized.

Scope: Our objective will be accomplished by evaluating ERA system documentation, and conducting interviews with ERA Program Management Office staff, as well as ERA System users.

Estimated Staff Days: 200

Locations: These efforts will be primarily performed at the ERA Program Management Office at Archives II.

Audit of NARA's Cloud Computing Efforts

Background: In December 2010, OMB announced its 25-Point Implementation Plan to Reform Federal Information Technology Management. This plan focused on reforms to eliminate barriers and more effectively manage IT programs throughout the Federal government. As part of this plan, agencies were required to immediately shift towards a "Cloud First" policy and identify at least three cloud computing capable services within their organizations. One of these services was required to move to the cloud by December 2011 and the other two by June 2012. Cloud computing is a means of outsourcing software, server, storage, and other IT needs to Web service companies.

Cloud computing brings a wide range of benefits, such as economies of scale, flexibility, and speed. As a pay-as-you-go approach to IT, cloud computing allows for low initial investments and additional investments are only needed as system use increases. Also, with cloud computing, IT departments can add or subtract capacity quickly and easily without scrambling for additional hardware or software. Finally, cloud computing can eliminate the long procurement and certification processes often required for in-house systems.

Objective: To determine whether NARA is adequately managing the use and implementation of cloud computing services and meeting OMB’s goals of a “Cloud First” policy.

Scope: The OIG will interview management and review NARA’s progress of migrating to cloud technologies. We will also review NARA’s policies and strategies for identifying shared services and opportunities for cloud computing.

Estimated Staff Days: 90

Location: Archives II and selected NARA field sites.

Assessment of NARA’s Data Backup Operations

Background: Backing up software and data is critical because, inevitably, there will be service interruptions. Agency plans should ensure there is an ability to recover and provide service sufficient to meet the minimal needs of users of the system. Normally, the primary contingency strategy for applications and data is regular backup and secure offsite storage.

Agency policies should (a) specify the frequency of backups (e.g., daily or weekly, incremental or full), based on how often the data changes and how important those changes are; and (b) designate the location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite.

Backup operations should include the following: (a) system data should be backed up regularly; (b) backup copies should be tested to ensure they are usable; (c) backup media and software should be stored offsite in a secure, environmentally controlled facility; and (d) the storage facility should be located far enough away from the original site to reduce the likelihood that both sites would be affected by the same event.

Objective: To determine if NARA has a systematic, accountable, and documented process for restoring original data after a data loss event. Specifically, we will determine if (a) there are documented plans and procedures for backing up data; (b) successful backups are accomplished on a regular basis; (c) backups are tested to verify media reliability and information integrity; and (d) backup copies of the operating system and other critical information system software are stored in a separate facility or in a fire-rated container that is not collocated with the operational software.

Scope: The assessment will include a review of the (a) agency’s backup policies and procedures, (b) roles and responsibilities of those individuals assigned to perform the backup functions, and (c) results of recent backups.

Estimated Staff Days: 120

Location: Archives II and selected NARA field sites.

Audit of NARA's Wireless Network

Background: Wireless networking enables computing devices with wireless capabilities to use computing resources without being physically connected to a network. Wireless local area networks (WLANs) are typically less secure than the wired network for several reasons, including the ease of access to the WLAN and the weak security configurations often used for WLANs (to favor convenience over security). According to NARA's Chief Information Officer, wireless access to the Internet is a necessary element of NARA's technical infrastructure for allowing the public to access government information and to conduct business in Federal facilities. In order to meet this need, NARA began providing unregistered access to the Internet on a dedicated public use segment of its wireless network in September 2012. Employee access to NARA's network via a wireless connection and the addition of other enhancements are under consideration.

Objective: To evaluate the implementation, configuration, and monitoring of NARA's wireless networks. Specifically, we will determine: 1.) whether adequate policies and procedures exist; 2.) whether effective security controls were implemented; 3.) whether the wireless network was properly configured; and 4.) whether NARA employed active monitoring of its wireless network.

Scope: The OIG will review policies and procedures, test security controls in place to ensure they are adequate, effective, and appropriate, review the configuration settings of the wireless networks, and review monitoring systems or processes in place.

Estimated Staff Days: 100

Location: Agency-wide, travel to field sites with wireless networks may be required.

Audit of NARA's Monitoring of Computer Security Incidents

Background: Attacks on computers and networks have become more numerous and more severe in recent years. Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents. Intrusion detection and prevention systems are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. They have become a necessary addition to the security infrastructure of nearly every organization.

Objective: To evaluate the intrusion detection technologies in use at NARA. Specifically, we will determine whether the intrusion detection capability is effective in monitoring computer security incidents.

Scope: The OIG will review the major components of the intrusion detection and prevention systems (IDPS), information collected and recorded by the IDPS, and security of the IDPS components.

Estimated Staff Days: 90

Location: Archives II, Office of Information Services (I).

Audit of Controls over NARA's Mobile Devices

Background: Mobile devices, such as Universal Serial Bus (USB) thumb drives, personal digital assistants (PDAs), smart phones, and tablet computers with wireless Internet access have become increasingly popular with today's highly mobile workforce. These devices allow employees to perform tasks at any time and from any place, as well as transport large volumes of data efficiently. Additionally, employees use these devices to send and receive electronic mail, browse the Internet, edit documents, deliver presentations, and access data remotely. Although portable devices may improve productivity, they also expose NARA to new security risks, such as downloading viruses or inadvertently exposing sensitive information or personally identifiable information. Security threats to portable devices include loss or theft, unauthorized access to networks or data, electronic eavesdropping, and electronic tracking of users.

Objective: To evaluate NARA's efforts to secure and deploy mobile devices on the NARA network, and to maintain and dispose of these devices. Specifically, we will determine whether (1) adequate policies and procedures have been implemented, (2) NARA maintains an accurate inventory of its mobile devices, and (3) effective controls have been implemented to protect the information stored or processed on the mobile devices.

Scope: The OIG will review the overall management and security of mobile devices deployed in the NARA environment. This review will not include laptops because the security controls available for laptops are quite different than those available for smart phones, tablets, and other mobile device types. In addition, mobile devices with minimal computing capability, such as basic cell phones, are also out of scope because of the limited security options available and the limited threats they face.

Estimated Staff Days: 90

Locations: Agency-wide, travel to field sites with wireless networks may be required.

Audit of NARA's Preservation Program

Background: Chapter 21 of Title 44 of the United States Code states the Archivist of the United States shall provide for the preservation, repair, and rehabilitation of records or other documentary material transferred to him as may be needful or appropriate. NARA's Strategic Plan (revised in FY 2009) identifies appropriate preservation of NARA holdings as a goal necessary for ensuring NARA achieves its mission. In June 2005, the OIG issued an audit report identifying resource and reporting deficiencies associated with NARA's Preservation program and declaring them a Material Weakness. Specifically, the audit identified: (a) items needing

preservation had not been identified; (b) inadequate staffing necessary for addressing preservation needs in a timely manner; (c) lack of criteria for assessing preservation needs/item condition; (d) NARA facilities that did not meet minimum environmental standards for the preservation of records, and; (e) inaccurate preservation performance data. NARA declared Preservation a Material Weakness in its FY 2005 FMFIA statement.

Objective: To assess the effectiveness of NARA's Preservation Program. Specifically, we will (1) identify program goals and objectives and how they support the agency's mission; (2) determine if program controls are adequate and properly functioning; and (3) determine if information concerning the condition of records is captured and reported in a standard format across the agency, used to formulate adequate risk rankings of records based on preservation needs, and used to guide resource allocations at the agency wide level (as opposed to the program office level). Furthermore, we will review recommendations contained in our prior report on preservation, to determine if they were adequately implemented and are achieving their intended effect.

Scope: This evaluation will include (a) a review of NARA guidance on preservation; (b) a review of internal controls related to the program with a specific focus on their ability to reasonably ensure information on record condition is being captured in a timely and consistent manner, conveyed to management, and used to guide agency wide preservation decisions; (c) evaluation of the means/methods used to capture and convey information on record condition; (d) a review of the resources associated with the preservation program; and (e) a review of the status of recommendations made in OIG Report No. 05-13, Evaluation in NARA's Preservation Program.

Estimated Staff Days: 120

Location: Archives I, Archives II, and NARA field sites, as necessary.

Audit of NARA's Processing Program

Background: In February 2007, OIG Report No. 07-06, "Audit of the Processing of Records Accessioned into NARA" found NARA was constrained in its ability to provide efficient and effective access to, and information about, textual records in NARA's custody as the result of large backlogs of inadequately processed records. At the time of our audit nearly 65 percent of NARA's textual records were not adequately processed, and the cost associated with fully processing these records was estimated to be \$1.5 billion, approximately three times NARA's annual budget. Because these backlogs impeded NARA's ability to perform its mission of providing access to records as soon as legally possible, and our audit revealed the need for additional controls, our report identified processing as a Material Weakness. An agency-initiated study agreed with our assessment of the impact of backlogs on NARA's ability to perform its mission. This study stated less than half of the holdings at Archives I and II (where the majority of NARA records reside and which draw the heaviest researcher use) were controlled at a level of detail enabling researchers to quickly identify records relevant to their interests. Further, more than one third were controlled at such a basic level that even experienced NARA staff had

difficulty determining whether they contained information which may be responsive to a researcher's request. While the processing backlog has been reduced from 50 percent to 48 percent of NARA's textual holdings, it still represents a significant obstacle to NARA's mission.

Objective: To assess NARA's efforts in implementing recommendations contained in OIG Report No. 07-06, and to determine whether effective controls have been put in place for ensuring records are being made available to the public in a timely manner.

Scope: This evaluation will include a review of the adequacy of efforts under-taken by management, and controls put in place to make records available to the public as quickly as possible.

Estimated Staff Days: 180

Location: Archives I and II.

Audit of Management Controls over the Declassification and Reclassification of Records

Background: In EO 13526 the President stated "[t]hroughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation's security and demonstrating our commitment to open Government through accurate and accountable application of classification standards and routine, secure, and effective declassification are equally important priorities." EO 13526 also established the National Declassification Center within NARA to streamline declassification processes, facilitate quality-assurance measures, and implement standardized training regarding the declassification of records determined to have permanent historical value.

Opposite of declassification, NARA may also be involved in reclassification issues whereby classification activity results in records being withdrawn from the open shelves at NARA. In 2006, the former Archivist tasked the Information Security Oversight Office with performing a review of withdrawals from NARA's open shelves which identified several weaknesses in NARA's process and made recommendations.

Objective: To determine whether adequate controls exist to provide assurance classified information is appropriately declassified and/or records are appropriately reclassified.

Scope: The OIG will assess the controls over this process and the control environment to ascertain if classified records are appropriately declassified and/or reclassified.

Estimated Staff Days: 90

Location: Archives II, Archives I and other NARA facilities to be determined.

Evaluation of a Original Classification Actions

Background: The Reducing Over-Classification Act , P.L. 11-258, requires "the inspector general of each department or agency of the United States with an officer or employee who is authorized to make original classifications, in consultation with the Information Security Oversight Office, shall carry out no less than two evaluations of that department or agency or a component of the department or agency" by 2016, with the first evaluation due in 2013. The Director of the Information Security Oversight Office has original classification authority under EO 13526.

Objective: According to the Act, the required evaluations are “(A) to assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within such department, agency, or component; and (B) to identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within such department, agency or component.”

Scope: This evaluation will include a review of the policies, procedures, rules, regulations, and management practices relating to original classification actions, and interviews of staff within the Information Security Oversight Office.

Estimated Staff Days: 30

Location: Archives I.

Audit of Selected Aspects of NARA’s Digitization Program

Background: According to NARA Directive 816, “Digitizing Activities for Enhanced Access,” digitization involves the creation of digital surrogates, digital images or copy of a textual or non-textual record for dissemination by a variety of means, including the Internet and CD-ROM. The primary purpose of digitizing is to improve and increase access to NARA archival holdings. A second purpose is to preserve rare, fragile, or high-use items by providing digital surrogates, for either online use or production of high-quality publications or reproductions for users. Producing a digital surrogate is not considered a preservation action, except in so far as it relieves wear and tear on original materials by allowing researchers to use digital surrogates instead of originals.

NARA does not aim to digitize its entire holdings. Rather, NARA aims to digitize only those holdings sharing the following characteristics: are highly significant, of considerable interest to the public, and in high demand; generally comprise whole, organic bodies of material; document the rights of American citizens, the actions of Federal officials, and the national experience; or have broad geographic, chronological, cultural, or topical appeal.

Objective: To determine whether management controls are adequate to address agency and customer needs and ensure greater access to NARA holdings.

Scope: The OIG will assess controls over this process and assess how challenges are addressed and managed.

Estimated Staff Days: 90

Location: NARA facilities to be determined.

Audit of Management Controls over Specially Protected Records (SPRs)

Background: NARA Directive 1572, “Preventing Theft and Vandalism of NARA Holdings in NARA Facilities” outlines the policy on security for NARA holdings in NARA facilities, including those needing special protection, and procedures staff must use to implement the policy. This directive informs staff, particularly in the Office of Record Services, Office of Regional Records Services, and Office of Presidential Libraries, of measures NARA must take to prevent theft and vandalism of NARA holdings.

Objective: To determine whether offices/work units are protecting, controlling, handling, and accounting for SPRs in accordance with NARA guidance.

Scope: Our objective will be accomplished by reviewing and determining the adequacy of controls over SPRs at various NARA locations.

Estimated Staff Days: 90

Location: Various NARA locations to be determined.

Audit of NARA’s Continuity of Operations Plan (COOP)

Background: Presidential Decision Directive 67 established the Federal Emergency Management Agency (FEMA) as the lead agency for COOP planning across the Executive branch. FEMA’s Federal Preparedness Circular (FPC) 65 provides guidance to federal agencies on development of COOP plans and carrying out testing, training, and exercise programs to ensure their effectiveness. The guidance states agencies are to test and exercise plans and procedures, personnel, and resources at specific frequencies during each year. FPC 65 also requires all Executive agencies to have in place a viable COOP capability which ensures the performance of their essential functions during any emergency or situation that may disrupt normal operations. To comply with this directive, a working group was chartered by NARA in November 2006 to develop the COOP.

Objective: To determine whether the COOP is adequate, and planning and testing efforts are efficient and effective to appropriately prepare NARA employees to address emergency situations.

Scope: The audit will assess the current COOP document to determine whether it is up-to-date, assigns appropriate roles and responsibilities, and addresses pertinent emergency situations. Additionally, we will determine whether testing is occurring on a frequent basis, and review results to ascertain adequacy and effectiveness.

Estimated Staff Days: 60

Location: Archives I, Archives II and the NARA COOP site at Allegany Ballistics Laboratory.

Audit of Contractor Access to NARA's Network and Facilities

Background: NARA relies on contract support for a range of IT and agency functions. Such support often requires contractors to be granted access to NARA's network systems and facilities. Federal guidance requires agencies to develop account management controls and procedures to ensure the identification and authorization of contractors and the specification of access privileges. Further, these controls must include a process for establishing, activating, modifying, disabling, removing, and reviewing access privileges.

Objective: To determine whether NARA has adequate controls in place to identify and manage contractor access to its network and facilities. This includes whether contractor accounts and access privileges are appropriately terminated when no longer required.

Scope: The audit will include a review of the overall management of contractor access to NARA's network and facilities. This will include a review of 1) Federal and agency policies and procedures, 2) NARA contracts and memorandums of agreement, and 3) access and user control lists of NARA's network and systems.

Staff Days: 90

Location: Archives II.

Audit of NARA's Social Media Program

Background: Organizations today are jumping on the social media bandwagon in record numbers. In the US, more than 80 percent of companies have a presence on Facebook and 45 percent are active on Twitter. Globally, approximately 16 percent of companies are using social media to interact and engage with their customers according to a 2012 IBM Global CEO Study, and that number is expected to triple in three to five years. To safeguard brand reputation, protect information and intellectual property, and mitigate legal actions, organizations need to be more proactive about managing social media risks. To set up an effective social media risk management process, organizations need to focus on 1) identifying social media risks, 2) assessing and prioritizing those risks against limited resources, 3) mitigating and managing those risks to reduce the impact on the organization and 4) evaluating emerging risks against mitigation efforts. Federal agencies have additional issues with social media, including such

topics as potential applications of the Federal Records Act, increased security issues, and others.

Objective: To determine whether management controls over the use of social media at NARA are effective.

Scope: The OIG will assess the agency's social media policies, review social media training and assess monitoring and enforcement protocols.

Estimated Staff Days: 60

Location: NARA facilities to be determined.

Audit of Controls Associated with Review and Certification of Records Storage Facilities

Background: NARA is authorized to (1) establish, maintain, and operate records centers for Federal agencies; (2) approve agency records centers; and (3) promulgate standards, procedures, and guidelines to Federal agencies with respect to the storage of their records in commercial records storage facilities. NARA regulations in 36 CFR 1234 specify the facility standards and approval processes applicable to all records storage facilities Federal agencies use to store, service, and dispose of their records. If not stored in appropriate facilities, records which document our history may be at risk of loss.

Objective: To evaluate the adequacy and effectiveness with which NARA carries out its responsibilities for inspecting and approving Federal agency and private records storage facilities used to store Federal records.

Scope: Our objective will be accomplished by sampling facilities and reviewing NARA's compliance with facility standards.

Estimated Staff Days: 90

Location: Various locations to be determined.

Audit of NARA's Exit Clearance Process

Background: NARA must, in accordance with Federal law and regulation, ensure all individuals ending their work or volunteer relationship with NARA, or relocating to a different office or facility within NARA, account for any outstanding financial responsibilities and accountable items for which the individual is responsible. In addition, NARA must terminate the individual's access to IT systems in compliance with OMB Circular A-130, "*Management of Federal Information Resources*" which states agencies are to protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to, or modification of, such information.

NARA Directive 215, “*Exit Clearance Procedures for Separating or Reassigned Individuals*” provides a process for employees, volunteers, student interns, foundation employees, and contractor employees to return accountable items and clear duties and financial responsibilities when they leave NARA or are reassigned to a different office or facility within NARA. It also provides procedures for terminating an individual's access to NARA IT systems when the individual leaves.

Objective: To determine the adequacy and effectiveness of NARA controls over the exit clearance process.

Scope: We will review the agency's separation records, exit clearance forms, and IT system access reports. We will also interview supervisors responsible for processing the exit clearance forms.

Estimated Staff Days: 60

Location: Office of Human Capital (H), Information Systems (I) and other offices to be determined.

Audit of Rental Payments to Federal Agencies (Other than GSA)

Background: Federal agencies are faced with a constant challenge to meet their missions expediently, oftentimes with limited resources. To meet their missions, agencies may require services outside their current capacities. Frequently these needs are met by contracting with private sector vendors through a complicated, costly and time-consuming contracting process that can detract from efforts to achieve mission objectives.

Other Federal agencies can provide specific services through an alternate procurement mechanism known as an “Interagency Agreement” or IAA. Quick, simple, flexible and easy to prepare, an IAA is the convenient and easy way for federal organizations to procure services from other federal agencies.

In 2011 NARA spent \$7.5 million on rental payments to Federal agencies, other than to GSA, using IAAs and other vehicles. The OIG will review these costs to understand these payments to other Federal agencies. Like contracts, interagency agreements or other payment vehicles need to be managed and monitored to ensure adequate performance is received from the vendor.

Objective: To evaluate the rental payments to federal agencies, other than GSA to ensure obligations are appropriate, the agreements are in NARA’s best interest and NARA is receiving services in accordance with the agreement.

Scope: Our objective will be accomplished by: (a) reviewing NARA’s guidance on interagency agreements, (b) evaluating interagency agreements and any other methods used, and (c) conducting staff interviews, including contracting officers and contracting officer representatives.

Estimated Staff Days: 45

Location: Business Support Services (B) located at Archives II.

Audit of Selected Procurement and Contract Management Practices and Functions

Background: In the past the OIG has partnered with the Acquisitions Services Division to perform proactive efforts aimed at addressing contracting issues facing NARA, and ensure contractors perform in accordance with contract terms and bill appropriately. Our efforts resulted in questioned costs and strengthened management controls. In FY 2013, we will try to reinstate these efforts with a focus on IT-related contracts. Specifically, we will continue to: (1) review contractor billings; (2) review contracts and procurement processes for compliance with the Federal Acquisition Regulation (FAR); (3) perform pre-award surveys, contract closeouts, and other contract audit services requested by management; and (4) monitor contractor performance.

Objective: To ensure that (1) procurement activities and contracts comply with the FAR; (2) contractors effectively perform contractual requirements and bill appropriately; and (3) NARA gets the best service or products possible for the contract funds expended.

Scope: Our objective will be accomplished by: (a) reviewing legal, regulatory and NARA based requirements, (b) evaluating procurement and contracting documents, and (c) conducting interviews, including contracting officers, contracting officer representatives, contractors, and NARA staff.

Estimated Staff Days: 60

Location: Assessments will be conducted at Archives II and, possibly, at field sites to be determined.

ADDITIONAL AUDIT STAFF ACTIVITIES PLANNED FOR FY 2013

Attestation Engagements

In addition to audits, the Audit Staff provides management assistance services to NARA program and administrative managers in the form of attestation engagements. These engagements concern examining, reviewing, or performing agreed-upon procedures on a subject matter or an assertion about a subject matter, and reporting on the results. The subject matter of an attestation engagement may take many forms, including historical or prospective performance or condition, physical characteristics, historical events, analyses, system and processes, or behavior. Attestation engagements can cover a broad range of financial or non-financial subjects and can be part of a financial audit or performance audit.

Nonaudit Services

In very limited circumstances OIG audit staff may perform nonaudit services in accordance with GAGAS. Such work does not usually provide a basis for conclusion, recommendations, or opinions on the information or data. In the case of non-government auditors who conduct audits under GAGAS, the term nonaudit service is typically synonymous with consulting services.

Peer Review

The Council of the Inspectors General on Integrity and Efficiency (CIGIE) Peer Review Committee schedules external quality control reviews, or peer reviews, of OIG audit functions once every three years. The NARA OIG Audit Division is scheduled to be peer reviewed in September 2013. The Investigative Committee of the President's Council on Efficiency schedules external quality reviews of the IG investigation function. The NARA OIG Investigative Division is scheduled to be reviewed in FY 2013.

BACKGROUND

In fiscal year 2012 NARA continued to implement a complete transformation of the agency. A staff-driven transformation of the agency to better align NARA with its customers, this five-year process is intended to modernize the agency and increase NARA efficiency and effectiveness in a time of increasingly austere budgets. A new organizational structure attempts to eliminate stovepipes and duplicative processes, and make NARA more nimble and responsive to its stakeholders. Six new transformation goals, listed below, provide NARA a new lens through which to view its strategic goals, and fosterer innovative, creative ways to approach work projects and assignments.

- One NARA
- A Great Place to Work
- Out in Front
- A Customer-Focused Organization
- An Agency of Leaders
- An Open NARA

To achieve NARA's six Transformational Outcomes, the agency has committed to the following set of values:

1. We are a diverse staff unified by our strong commitment to protect records, help people use them, and support an open and responsive government;
2. We want to do our personal best and make our agency the world's best archives; and
3. We believe in an open, inclusive work environment, encouraging creativity and investing in innovation and pursuit of excellence through continuous learning.

Additionally, NARA has defined six strategic goals and the strategies to achieve them in its strategic plan titled, "Preserving the Past to Protect the Future: The Strategic Plan of the National Archives and Records Administration, 2006 – 2016," issued January 11, 2007, revised and re-issued October 1, 2009. The NARA Strategic Plan sets out six primary goals:

1. As the nation's record keeper, we will ensure the continuity and effective operation of Federal programs by expanding our leadership and services in managing the Government's records.
2. We will preserve and process records to ensure access by the public as soon as legally possible.
3. We will address the challenges of electronic records in Government to ensure success in fulfilling NARA's mission in the digital era.
4. We will provide prompt, easy, and secure access to our holdings anywhere, anytime.
5. We will increase access to our records in ways that further civic literacy in America through our museum, public outreach, education and grants programs.
6. We will equip NARA to meet the changing needs of our customers.

The OIG has linked its work processes to align with NARA's six Transformational Outcomes and strategic plan to focus on critical issues that have a major impact on NARA's ability to effectively carry out its mission. The projects described in this work plan are designed to address the challenges faced by NARA and, more specifically, for evaluating (1) internal management and management systems to recommend improved and more effective, efficient, and economical means for achieving results, and (2) internal management controls to identify unnecessary spending, to recover funds used inappropriately, and to detect and prevent waste, fraud, and abuse.

To accomplish the projects listed in this plan, we may use various audit services such as audits, attestation engagements, and nonaudit services. "Audits" address the management and financial operations of NARA, the economy and efficiency with which NARA's programs and functions are managed, and the results achieved. The overall objective is to identify management and operational weaknesses and to recommend improvements in the management and operation of programs and activities. Audits assess the extent to which NARA complies with laws, regulations, and policies in implementing programs; the extent to which programs are managed effectively and efficiently; and the accuracy and reliability of financial statements. Program effectiveness is defined by statute and NARA's mission and program objectives.

"Financial Audits" are utilized for (1) financial statement work where the objective is to provide reasonable assurance about whether financial statements present fairly the financial position, results of operations, and cash flows in conformity with generally accepted accounting principles, and (2) financial-related work where the objective is to determine whether (a) financial information is presented in accordance with established or stated criteria, (b) the agency has adhered to specific financial compliance requirements, and (c) the agency's internal control structure over financial reporting and/or safeguarding assets is suitably designed and implemented for achieving the control objectives.

"Program Audits" are systematic studies conducted periodically to assess how well a program or operation is working. Program audits include (1) determining the extent to which a program is operating as it was intended, (2) assessing the extent to which a program achieves its outcome-oriented objectives, (3) assessing the net effect of a program by comparing program outcomes with an estimate of what would have happened in the absence of the program, and (4) comparing a program's outputs or outcomes with the costs to produce them.

In the interests of improving program effectiveness, public accountability, and service delivery, the Government Performance and Results Act (GPRA) demands Federal agencies focus on results. The OIG will direct its efforts toward helping NARA meet the demands of the GPRA. The planned FY 2013 audits are designed to aid NARA in accomplishing its strategic goals and statutory or other requirements.

GLOSSARY

Audits - Objective and systematic examinations of evidence for the purpose of providing an independent assessment of the performance of a government organization, program, activity, or function in order to provide information to improve public accountability and facilitate decision-making.

Financial Audits – Financial audits are primarily concerned with providing reasonable assurance about whether financial statements are presented fairly in all material respects in conformity with generally accepted accounting principles (GAAP) or with a comprehensive basis of accounting other than GAAP. Other objectives of financial audits, which provide for different levels of assurance and entail various scopes of work, may include providing special reports for specified elements accounts, or items of a financial statement, reviewing interim financial information, issuing letters for underwriters and certain requesting parties, reporting on the processing of transactions by service organizations and auditing compliance with regulations relating to federal award expenditures and other governmental financial assistance in conjunction with or as a by product of a financial audit.

Performance Audits – Performance audits entail an objective and systematic examination of evidence to provide an independent assessment of the performance and management of a program against objective criteria as well as assessments that provide a prospective focus or that synthesize information on best practices or cross-cutting issues. Performance audits provide information to improve program operations and facilitate decision making by parties with responsibility to oversee or initiate corrective action, and improve public accountability. As used in this plan, program audits are a type of performance audit. Performance audits encompass a wide variety of objectives, including objectives related to assessing program effectiveness and results; economy and efficiency; internal control; compliance with legal or other requirements; and objectives related to providing prospective analyses, guidance, or summary information.