

National Archives and Records Administration

Transmittal Memo

DATE: May 26, 2011

TO: Executives, Staff Directors, NHPRC, and OIG

SUBJECT: NARA 204, Access Privilege Procedures at AI and AII

Purpose: This transmits a revised NARA 204 Access Privilege Procedures at AI and AII (formerly NARA 272).

Background/significant changes: This revised directive continues to enhance the security of the National Archives Building and the National Archives at College Park and the records, artifacts, and personal and Government property therein. It also helps ensure the safety of individuals in the facilities by improving control over the movement of people in the buildings.

This revision changes the title and numbering of NARA 272 and adds definitions for clarity purposes to align to definitions in NARA Directive 275, Background and Identity Verification Process for Access Privileges, which was issued May 9, 2008. This revision also corrects citations to 36 CFR 1254.48 as the correct paragraph for revocation of research room privileges. This revision provides clarity on Security Officer, Supervisor and Employee responsibilities in regard to the use of the ID card and managing access privileges. A new mandatory training course for new employees has been added and is titled, Security and Safety Awareness Course. The course is available through NARA's Learning Management System (LMS), on the NAS home page.

Canceled directive. This directive cancels NARA 272 dated March 17, 2004.

Effective date: This change is effective upon date of signature.

Whom can I contact for more information? For questions regarding this directive, please contact Kevin McCoy, Security Management, at 301-837-0298 or via Kevin.McCoy@nara.gov.

DAVID S. FERRIERO
Archivist of the United States

Attachment

National Archives and Records Administration

NARA204
May 26, 2011

SUBJECT: Access Privilege Procedures at AI and AII

204.1 What is the purpose of this directive?

This renamed, revised and updated directive enhances the security of the National Archives Buildings, AI and AII, and the records, artifacts, personal and Government property therein. Due to the different building configurations, not all the processes are the same at both buildings, and those differences are identified in this directive. It also continues to ensure the safety of individuals in the facilities by improving control over the movement of people in the buildings. It aligns terminology and processes outlined in [NARA 275](#), Background and Identity Verification Process for Access Privileges. For clarification this directive is specific to AI and AII with more detailed processes, particularly on how access permissions are granted on the access media. [NARA 1572](#), Preventing Theft and Vandalism of NARA Holdings in NARA Facilities, identifies who is authorized to allow personnel to receive permission to access holdings storage areas in para. 8.

204.2 What are the authorities for this directive?

U.S.C. 2104; 2108(a); 2111 note, Sec. 103; and 2903

204.3 Definitions

For this directive, the following definitions apply:

- a. **Facility access media** - An accountable document used to confirm that the holder has permission to enter restricted areas of AI and AII:
 - (1) for unescorted access to A1 staff restricted areas: NARA-issued PIV identification card with photograph (MSO PIV), NARA identification card with photograph (NA Form 6000), NARA Temporary Building Pass (a version of NA Form 6000) with photograph, NARA Temporary Employee Pass (NA Form 6002I) without photograph, which must be displayed in the restricted area at all times.
 - (2) for unescorted access to A1 researcher restricted areas: NARA-issued PIV identification card with photograph (MSO PIV), NARA identification card with photograph (NA Form 6000), NARA Temporary Building Pass (a version of NA Form 6000) with photograph, NARA Temporary Employee Pass (NA Form 6002I) without photograph or be signed in by a Security Officer who will issue you a Temporary Researcher Pass (NA Form 6002G), which must be displayed in the restricted area at all times.

- (3) for escorted access to AI restricted staff and researcher areas: You must be accompanied by a person with identification listed in para (1) above, and be signed in by a Security Officer who will issue you a Tour Group Pass (NA Form 6002F) or a Visitor Pass (NA Form 6002H) which must be displayed in the restricted area at all times. The escort must stay with the individual(s) and there is a required ratio of one NARA-issued PIV identification card with photograph (MSO PIV), NARA identification card with photograph (NA Form 6000), NARA Temporary Building Pass (a version of NA Form 6000) with photograph, NARA Temporary Employee Pass (NA Form 6002I) without photograph for each 10 visitors.
 - (4) for unescorted access to AII restricted areas: NARA-issued PIV identification card with photograph (MSO PIV), NARA identification card with photograph (NA Form 6000), NARA Temporary Building Pass (a version of NA Form 6000) with photograph, NARA Temporary Employee Pass (NA Form 6002I) without photograph, which must be displayed in the restricted area at all times.
 - (5) for escorted access to AII restricted areas: You must be accompanied by a person with identification listed in para (4) above, and be signed in by a Security Officer who will issue you a Tour Group Pass (NA Form 6002F) or a Visitor Pass (NA Form 6002H) which must be displayed in the restricted area at all times. The escort must stay with the individual(s) and there is a required ratio of one NARA-issued PIV identification card with photograph (MSO PIV), NARA identification card with photograph (NA Form 6000), NARA Temporary Building Pass (a version of NA Form 6000) with photograph, NARA Temporary Employee Pass (NA Form 6002I) without photograph for each 10 visitors.
- b. **Identification** - Documents that prove an individual's identity.
 - c. **Identification card (ID)** - a photo identification card issued to NARA employees, volunteers, agency reviewers, interns and contractor employees.
 - d. **Temporary employee pass** - issued at the lobby security desk to holders who do not have their ID on their person when entering the building, or when their ID is confiscated after verification they are still permitted access, due to expiration of the ID or mutilation of the ID to render it useless as an ID card or pass.
 - e. **Proximity cards** - electronically encoded cards that release door locks when held against wall-mounted, card-reading devices. For purposes of this directive, an ID issued at AI and AII is considered a proximity card.
 - f. **Researcher cards** - (with or without a photograph of the individual) - issued at all NARA facilities that allow the holder access to the Research Center and Central Research Room (Room 203) at AI and the Steny H. Hoyer Research Center at AII.

- g. **Restricted areas** - All parts of AI accessed from the Pennsylvania Avenue lobby are restricted areas, and further defined as staff or researcher restricted areas. At AII all areas other than the entrance lobby, cafeteria, Thomas auditorium, lecture rooms and adjoining hallways.
- h. **Temporary researcher passes** - issued and retrieved by security officers at the AI Pennsylvania Avenue entrance to researchers going to the Research Center to carry out research or register for a researcher card, or to the Central Research Room.
- i. **Tour group passes** – issued and retrieved by security officers to each individual that is part of a NARA sponsored guided tour by an authorized NARA representative and indicates the person displaying the pass requires escort.
- j. **Visitor passes** - issued and retrieved by security officers from guests, representatives of other Government agencies, and company representatives calling on NARA business offices, indicating the person displaying the pass requires escort.
- k. **Workshop passes** - name badges issued by the NARA sponsoring unit to individuals attending workshops, conferences, or other educational activities after approval is received by Security Management and are designed on an ad hoc basis.

204.4 Responsibilities

- a. **Chief, Security Management:** The Chief, through subordinates:
 - (1) Issues IDs and proximity cards to NARA employees, volunteers, agency reviewers, interns and contractor employees at AI and AII.
 - (2) Advises supervisors and others concerning administration of this directive to ensure that proper procedures are followed and that all employees are treated equitably.
 - (3) Inspects building exit and entry registers to identify pass holders who regularly fail to carry building passes or otherwise do not follow proper procedures and notify that individual's supervisor of this pattern.
 - (4) Responds to requests from security officers for assistance in dealing with uncooperative individuals.
 - (5) Conducts periodic reviews of the verification of IDs.
- b. **Chief of Security for Archives I and Physical Security Team Leader for Archives II.** Must:
 - (1) Semi-annually provide program offices of NW, NL and NR within AI and AII under their jurisdiction a consolidated list of all individuals that have access to the facilities to validate the access to specific areas, particularly

stacks to either correct access authority or purge those no longer needing access. The source of the information will be obtained from the Identification Card Request ([NA Form 6006](#)) or email notification. Program offices must obtain these reports in accordance with section 204.4(d)(3).

- (2) Conduct a review of NARA employee departures lists monthly to ensure the individual properly out-processed the "Security Items" of section 6 of the NARA Employee Exit Clearance Record ([NA Form 3009a](#)) in accordance with [NARA 279](#), Exit Clearance Procedures for Separating or Reassigned NARA Employees, Contractor Employees, Volunteers, Interns, and Foundation Employees.
- (3) Implement an internal security management process based on the capability of the buildings physical access control system software to ensure any access media that has not been used on the access control system within a 90 day window are identified and automatically disabled by the system, purged or a determination is made the access media is still valid for that individual.

c. **Contract security officers.** Security officers:

- (1) In response to requests from NARA staff, or from their observations, request identification from individuals in restricted areas who do not properly display identification.
- (2) Escort from restricted areas to the entrance lobby individuals who do not correctly display or have proper identification, or do not produce the necessary identification when requested and prepare incident reports to document the incident and provide a report to the Security Management unit.
- (3) Ensure that researchers entering the Research Center or Central Research Room in AI and the Steny H. Hoyer Research Center at AII have current researcher cards.
- (4) Issue a visitor pass after confirming with the sponsoring NARA individual the visitor is expected and ensuring the sponsor escorts the visitor at all times, to include turning in the visitor pass upon departure from the building.
- (5) At AI, inquire of the public of their research plans and direct them to the researcher registration office, the Research Center, or the Central Research Room, and issue the appropriate pass.

- (6) Inspect and touch the ID of an individual holder before admitting the individual to a restricted area, ensuring the ID is that of the person presenting it, and the ID has not expired.
- (7) Issue and retrieve pass holder temporary identification from employees who do not have their permanent ID on their person or who's permanent ID has been confiscated, each time they enter or leave the building and at the end of the duty day, do an audit of temporary passes to ensure they have all been turned in. (Before issuing a temporary identification badge, security officers must contact the employee's supervisor to verify the employment status of the individual.)
- (8) Confiscate an individual's proximity card that has expired or deteriorated to the degree that the photograph cannot be recognized as the person presenting the badge and turn into Security Management unit for corrective follow up action.
- (9) Contact Security Management unit when confronted with an uncooperative individual.

d. Program Offices having major holding storage areas (NW, NL and NR) within AI and AII must:

- (1) Identify, by position, the program office representative(s) responsible for receiving the consolidated list of all individuals that have access to the storage areas under their operational control, to validate the access to specific areas, particularly stacks, records holding and processing areas, to validate access authority or identify those no longer needing access and who will return the list with changes to the Security Management unit to be purged.
- (2) Semiannually provide the Chief of Security for Archives I and Physical Security Team Leader for Archives II a consolidated list of all areas under their operational control by room number and unit and identify the responsible custodian of each stack, records holding and processing area.
- (3) Provide a USB drive or burnable CD/DVD so digital copies of the report can be provided to the program office. NASS can provide a paper access permission report.
- (4) For computer readable extracts or hard copy reports that may contain personally identifiable information, the program office would have to sign a receipt for the report and comply with NARA 1608, Protection of Personally Identifiable Information (PII). The program office would have to define the duration of reports and duration of use, justification if longer

than 90 days, an alternate disposition date if longer than 90 days and notification to the Security Management unit of destruction.

- e. NARA supervisors, acting supervisors, team leaders and NARA sponsors of agency reviewers, foundation employees, interns and volunteers must:
- (1) Ensure those individuals under their authority properly display their ID when entering, leaving, and in restricted parts of the building.
 - (2) Reports to Security Management unit at Archives I or Archives II by e-mail to physical.security@nara.gov or submission of a newly completed Identification Card Request ([NA Form 6006](#)) to Security Management, any changes in access requirement to those individuals under their authority at AI and AII. This is to ensure access to areas no longer needed by the individual is deleted, particularly to stack areas within the buildings. See NARA 275, Background and Identity Verification Process for Access Privileges for instruction to properly complete the form and also place time restrictions on access to areas if necessary for temporary access privileges.
 - (3) Report to security desk in the lobby and vouch for the identity and the legitimacy of the need to enter by an individual under their authority who has lost or forgotten their facility access media.
 - (4) Propose disciplinary action or other administrative sanctions regarding individuals under their authority who fail to follow proper procedures or improperly use their ID or proximity card.
 - (a) for NARA employees see levels for each offense identified in Chapter 752, Part 2, and NARA Personnel Manual (PERSONNEL 300).
 - (b) for other personnel see subpar. 204.15b, c, d, or e as appropriate to the individual responsible for the policy infraction.
 - (5) Alert security officers if an individual unknown to them and without appropriate identification or properly displayed identification is reported in a restricted area.
 - (6) Inform other supervisors when an employee under that supervisor's authority is not properly displaying his or her ID.
 - (7) Respond to security officer inquiries concerning visitors requesting to visit their office. Ensure employees escort visitors to the entrance lobby when the visitor is departing the restricted areas.

- (8) Complete and forward a new [NA Form 6006](#), Identification Card Request, to Security Management unit to request a replacement ID for employees under their authority because the ID has expired, is near expiration, or was confiscated.
- (9) Ensure compliance with [NARA 279](#), Exit Clearance Procedures for Separating or Reassigned NARA Employees, Contractor Employees, Volunteers, Interns, and Foundation Employees, to ensure all access media in turned in to the Security Management unit. Supervisors will initiate the [NA Form 3009a](#), NARA Employee Exit Clearance Record, in accordance with [NARA 279](#).
- (10) Ensure all new employees complete the Security and Safety Awareness course available through NARA's Learning Management System on the NAS home page, and encourage all subordinates to review the course materials as the supervisor deems necessary.

f. **Employees.** Employees must:

- (1) Wear their ID as prescribed in par. 204.10 at all times while in restricted areas.
- (2) Renew their ID before it expires or when the photograph has deteriorated to the point it is no longer recognizable. A completed and signed [NA Form 6006](#), Identification Card Request, must be presented when renewing the ID.
- (3) Inform their supervisor or a security officer if an individual is seen in a restricted area without appropriate identification or an improperly displayed ID. If an unidentified individual appears to be lost and asks for directions, employees may, at their discretion, escort the individual to the nearest occupied office and request a security officer to escort the individual to a public area, or do so themselves. Under no circumstances should employees approach an unidentified individual in a provocative or confrontational manner.
- (4) Use their proximity card to enter areas protected by wall-mounted, card readers, and show their ID to the security officer when entering a restricted area individually or with a group.
- (5) Not use their proximity card to let individuals known to lack access privileges into restricted areas.
- (6) Attempt to prevent and report to security personnel or their supervisor instances of individuals known to lack access privileges and who attempt to or do following them through a proximity card-controlled door.

- (7) Immediately report the loss of their ID or proximity card to Security Management.
- (8) Show photo identification and sign in at the security desk in the lobby each time they enter the building without their ID and return the pass holder temporary identification to the security officer and sign out each time they leave the building.
- (9) Return their ID and proximity card to the Security Management unit when leaving NARA employment or when their duty station is changed from AI or AII if they will no longer need to access to restricted areas in that building in accordance with [NARA 279](#), Exit Clearance Procedures for Separating or Reassigned NARA Employees, Contractor Employees, Volunteers, Interns, and Foundation Employees.
- (10) At AI and AII, hold out their ID to the security officer at the entrance to the restricted area, to allow the security officer to verify the validity of the badge.
- (11) Present their ID or proximity card to Security Officers, supervisors, management for inspection upon request, regardless of their location within AI and AII.
- (12) When acting as an escort for a visitor, ensure the visitor is not left unescorted at any time in any restricted areas of the building and ensure the visitor is properly signed out, leaves the buildings and that the visitor badge was turned-in at the point of issue.
- (13) Ensure they complete the Security and Safety Awareness course available through NARA's Learning Management System on the NAS home page, upon appointment and consider reviewing the course material as refresher as they feel necessary.
- (14) It is important to record everyone who enters an area where NARA Holdings are stored. When entering a processing room or holdings storage area each person entering must present their proximity card to the card reader. The reader will beep to acknowledge a valid read.
- (15) Employees are required to make sure doors leading to secure areas are closed and locked behind them. This is especially true on doors equipped with automatic operators. Employees should pass through the door, move far enough away from the motion operated safety device and remain in the area assuring the door closes completely.

- (16) If an employee should observe an individual enter a processing room or a holdings storage area by tailgating, he/she should report the incident immediately to his/her supervisor.

g. **Contracting officers' representatives/NARA project managers**

- (1) Inform Security Management unit of the access requirements to be coded onto the proximity cards of their employees.
- (2) Reports to Security Management at Archives I or Archives II by an e-mail to physical.security@nara.gov or submission of a newly completed [NA Form 6006](#), Identification Card Request, any changes to the contractor's employee's access at those facilities. This is to ensure access to areas no longer needed by the contractor's employee is deleted particularly to stack areas within the facilities.
- (3) Complete and forward a new [NA Form 6006](#), Identification Card Request, to Security Management to request a replacement ID because the ID has expired, is near expiration, or was confiscated.
- (4) Inform the contractor's project manager of any non-compliance by their employees, monitor performance, inform the contractor's project manager if violations continue, and request removal of the offending individual from the work site.
- (5) Inform Security Management unit when to cancel a contractor employee's or agency reviewer's access to a NARA facility and comply with requirements of [NARA 279](#), Exit Clearance Procedures for Separating or Reassigned NARA Employees, Contractor Employees, Volunteers, Interns, and Foundation Employees.
- (6) Ensure all individuals they sponsor complete the Security and Safety Awareness course available through NARA's Learning Management System on the NAS home page and encourage all sponsored individuals to review the training as necessary to ensure compliance with this directive.

h. **Labor/Employee Relations and Benefits Branch (HTL):** HTL advises supervisors about possible disciplinary actions against employees who do not follow the requirements of this directive, and approves written notices of proposed actions. (See PERSONNEL 300, ch. 752.)

i. **Textual Archives Services Division (NWCC) personnel**

- (1) Division employees stationed in researcher registration offices at AI and AII issue researcher cards.

- (2) NWCC employees stationed in the researcher assistance area at AII issue and retrieve special access badges to enable researchers to enter restricted areas to consult with NARA staff.
- j. **NARA volunteers.** Volunteers must abide by the requirements of subpar. 204.4e.
- k. **NARA contractor employees and agency reviewers.** Contractor employees and agency reviewers must abide by the requirements of subpar. 204.4e.

204.5 Are the IDs issued at AI and AII interchangeable?

No. The proximity card function of identification issued at one building is inoperable in the other building. NARA contractor employees, volunteers, interns and agency reviewers who enter areas in AI and AII where access is controlled by wall-mounted card-readers are issued pass holder level identification for both buildings. If the individual will not enter proximity card-controlled areas, the NARA ID issued in either building is sufficient for access to the other building.

204.6 Can security officers or security management personnel confiscate my ID?

Yes. IDs will be confiscated that have expired or that have deteriorated to the degree that the photograph is unrecognizable. The security officer will issue the person a pass holder temporary identification, pending replacement of the permanent ID if the person is still authorized for access to AI and AII.

204.7 How do I replace my ID?

At AI, a new ID is issued by Security Management during posted hours in room B7. At AII, a new ID is issued by the Security Management unit during posted hours in room 2300. Pass holders can request a new ID at any time if they notice that the photograph is badly deteriorated or that their ID is within 4 weeks of an expiration date. A new [NA Form 6006](#), Identification Card Request, must be presented by any individual each time a new ID is to be issued.

204.8 Who must wear ID?

- a. **AI.** All persons in the restricted areas of AI, except the following must display the appropriate NARA-issued identification at all times.
 - (1) Individuals attending receptions and other by-invitation-only events.
 - (2) NARA and contractor employees, agency reviewers, interns and volunteers engaged in hazardous activities described in par. 204.10.
- b. **AII.** All persons in restricted areas of AII must display appropriate NARA-issued identification at all times, except as permitted by par. 204.10.

204.9 Where is it not necessary to display identification?

At AII, researchers do not have to display identification while in the Steny H. Hoyer Research Center, and no one is required to display identification while in unrestricted areas of the buildings. In AI, visible identification is not needed in areas accessed from the Constitution Avenue side of the building.

204.10 How must the identification be worn?

Unless it would create a hazard, identification must be visible from the front and be at or above the belt line. When a pass holder is actively engaged in an activity that would make wearing any of the NARA-supplied badge holders hazardous, the ID must be carried on his or her person and produced upon request.

204.11 What types of devices to hold identification does NARA provide?

- a. ID holders. NARA provides to pass holders armbands or plastic sleeves and spring-loaded clips, neck chains, and retractable holders that may be fastened on a wearer's belt.
- b. Non-ID holders. NARA provides neck chains or clips to non-pass holders entering restricted areas of AI and AII.

204.12 What devices can be used to hold an ID?

Individuals may use NARA-supplied devices or others of their choosing as long as the ID is displayed in accordance with par. 204.10.

204.13 Does NARA supply replacements for broken or lost display devices?

NARA replaces the devices listed in par. 204.11 if damaged by wear and tear and a reasonable number that are lost or misplaced. NARA does not pay for or replace devices other than those listed in par. 204.11.

204.14 Who enforces the requirement to display identification and the proper use of proximity cards?

- a. Supervisors enforce the requirements of this directive for individuals under their authority. Supervisors must consult with the Security Management unit and the Office of Human Capital (H) before proposing a penalty to ensure proper procedures are followed and that equitable treatment is afforded to all employees.
- b. Security officers inform the Security Management unit of violation(s) of policy by NARA employees, volunteers, interns, contractor employees, agency reviewers, researchers, and visitors. Security Management informs the appropriate NARA officials of the reported violation(s). Security Management enforces the requirements of this directive when visitors are involved.

- c. NARA contracting officers, contracting officers' representatives, and NARA project managers enforce the requirements of this directive when contractor employees and agency reviewers are involved.
- d. Director, Customer Services Division (NWCC), enforces the requirements of this directive when researchers are involved.

204.15 What penalties are imposed for failure to properly display identification or misuse of proximity cards?

- a. **NARA employees.** Employees who fail to properly display their ID, misuse proximity cards, or refuse to follow other requirements concerning use of identification without good cause, are subject to disciplinary action in accordance with [PERSONNEL 300, ch. 752, app. 752a, Penalty Guide](#). Supervisors warn the employee (verbal or in writing depending on the magnitude of the act) before disciplinary action is taken under the Penalty Guide. The recommended penalty under the Penalty Guide ranges from a letter of reprimand to removal for the first offense.
- b. **NARA volunteers.** Volunteers who regularly fail to properly display their ID or misuse proximity cards will be asked to resign by the Volunteer Coordinator that sponsored them.
- c. **NARA contractor employees and agency reviewers.** NARA contracting officers, contracting officers' representatives, and NARA project managers request removal of employees from work on NARA projects in accordance with contract provisions for repeated failure to properly display identification, for misuse of proximity cards, or for entering restricted areas without authorization by following pass holders.
- d. **Researchers.** Researchers are our guests and must be reminded of the need to display their identification where appropriate. Those who refuse to comply without good cause may have their research privileges revoked in accordance with 36 CFR 1254.48.
- e. **Visitors.** Visitors who refuse to properly display their visitor pass without good cause will be denied access to, or be escorted from, the building.

204.16 How is privacy protected when implementing this directive?

- a. All relevant Federal privacy laws, policies, and NARA directives apply to the handling and maintenance of the background investigation, identity verification, and access request records.
- b. Only Security Management is permitted to retain copies of the forms used to request access. Those individuals must maintain the personal information on the forms in accordance with the provisions of the Privacy Act and NARA Privacy Act Systems Notice 11: Credentials and Passes.

204.17 How are records created by this directive maintained under the NARA Records Schedule?

a. **Security Management -**

- (1) Issuance of access media for NARA facilities in the DC Area - Follow the disposition instructions for file nos. 649, "Credentials Files," and 650, "Visitor Control Files," as applicable.
- (2) Background investigations and access suitability process - Use file no. 312-1 for security folders for NARA employees and applicants for employment, contractors, volunteers, interns, and other individuals who require recurring access to non-public areas of NARA facilities and to IT resources. Follow the disposition instructions for file no. 312-2 for investigative reports and related documents that are provided to NARA by investigative organizations for use in making access suitability determinations. For tracking records, see the instruction for item 313.
- (3) Security Officers Security Officers: Use file no's. 647, "Investigative Files", and 652-2, "Police Function Files".

b. **Supervisors** - Keep records pertaining to employees in an unofficial personnel file (UPF) for each individual in accordance with file no. 303-1.

c. **Office of Human Capital** - File in OPF file no. 301.

d. **CORs/COTRs** - Maintain records pertaining to contractor employees in the contract case file (item 519-1).

e. **Volunteer coordinators** - Use file no. 1605-3, "Volunteer and Tour Program Files: Individual Volunteer Files."

f. **Employees** - For personal use, you may maintain paper copies of your investigative forms and other related documents. However, make sure to keep these personal copies separately from any records filed in the UPF or elsewhere in your unit.

g. **NARA interns/student interns** - Keep records with other records relating to the individual intern. As these records are currently unscheduled, they may not be destroyed at this time.

h. **Foundation employees and volunteers** selected by the Foundation for the National Archives, the Presidential library foundations, and any other NARA support organization - Foundations should file and retain these records in accordance with their own policies, procedures, and record keeping practices.