

# National Archives and Records Administration

---

May 9, 2008

NARA 275

**SUBJECT: Background and Identity Verification Process for Access Privileges**

**TO: Office Heads, Staff Directors, ISOO, NHPRC, OIG**

**Purpose of this transmittal memo.** This transmits a new directive providing policies and procedures for establishing and implementing the personal identity verification and access control program at NARA.

**Background.** Homeland Security Presidential Directive (HSPD)-12 requires implementation of Government-wide standards for secure and reliable forms of personal identification issued by Federal agencies to their employees, contractors, and all other individuals requiring recurring access to staff-only areas of Government facilities or IT systems. Each agency is required to establish a personal identity verification program that includes background investigations and identity verifications as a prerequisite for issuance of an identification card or electronic authentication media access that is compliant with HSPD-12.

**Types of employee identification cards.** As the HSPD-12-compliant card becomes available across the nation through the management services offices (MSO) operated by GSA, employees requiring recurring access to NARA facilities and non-public IT resources will, upon a satisfactory access and identity determination, be issued a personal identity verification (PIV) card. In the interim, NARA will continue to issue NARA identification cards (ID) (NA Form 6000) to employees. Upon issuance of a PIV card, the NARA ID will be revoked.

Further guidance regarding the issuance of the PIV identification card through GSA will be issued as their enrollment offices are opened across the nation.

NARA will continue to issue NARA ID (NA Form 6000) to contractors' employees, volunteers, and student interns as facility access media to NARA-occupied and -operated facilities.

**Significant changes.** This guidance specifies who requires a background investigation to obtain recurring access to NARA facilities and information technology (IT) systems. This guidance also describes the processes NASS follows to determine access suitability for purposes of acquiring a NARA or PIV identification card, or systems access, and the requirements relating to their use.

Please note that access suitability determinations differ from employment suitability determinations. This directive addresses access suitability for purposes of access to NARA facilities and systems, whether the person involved is an employee or not. The employment suitability process will be detailed in NARA 276.

Please also note that there are different procedures for NARA facilities in the Washington, D.C. (DC) area and outside the DC area.

The definitions in this directive for identity processor, issuer, registrar and sponsor are unique to NARA's internal control procedures.

# National Archives and Records Administration

---

**Available forms.** Use of the following forms is authorized by this guidance:

NA Form 6000, NARA Identification Card  
NA Form 6002F, Tour Group Pass  
NA Form 6002H, Visitor Pass  
NA Form 6002I, Temporary Employee Pass  
NA Form 6006, Identification Card Request  
NA Form 6014, Record of Time of Arrival and Departure from Building  
SF 85, Questionnaire for Non-Sensitive Positions  
SF 85P, Questionnaire for Public Trust Positions  
SF 86, Questionnaire for National Security Positions  
SF 87, Fingerprint Card for Federal Position (Federal Employees)  
OF 306, Declaration for Federal Employment  
NA Form 3016, Personnel Security Action Request and Certification  
FD 258, Applicant Fingerprint Card (for NARA contractor employees and volunteers)

**Canceled guidance.** The following guidance is superseded by this issuance: Interim Guidance 275-1, Application Process for NARA Federal Identity Cards (FIC).

**Canceled forms.** The following forms are cancelled by this issuance:

NA Form 6000A1, NARA Renovation Contractor ID Card  
NA Form 6000B, Contractor / Agency Reviewer Identification Badge  
NA Form 6002, Volunteer Pass.  
NA Form 6002J, Room 2400 Pass  
NA Form 6002K, Room 2600 Pass  
NA Form 6003, Contractor Employee's Identification  
NA Form 6004, Contract Employee Suitability Record  
NA Form 6014A through F, Record of Time of Arrival & Departure from Building.

**Contact information.** Questions about this directive may be directed to Paula Ayres (NASS) in room 2300, AII; on 301-837-1494; by fax on 301-837-3657 or by email.

ALLEN WEINSTEIN  
Archivist of the United States

Attachment

# National Archives and Records Administration

---

NARA 275  
May 9, 2008

**SUBJECT: Background and Identity Verification Process for Access Privileges**

## **PART 1 – General**

### **275.1 What is the purpose of this directive?**

This directive establishes NARA's personal identity verification and access control program for the issuance of the NARA identification cards and Personal Identity Verification (PIV) cards. This program complies with Homeland Security Presidential Directive (HSPD)-12, which requires implementation of Government-wide standards for secure and reliable forms of verified personal identification issued by Federal agencies to their employees, contractors, and other individuals who need recurring access to staff-only areas of Government facilities and IT resources.

### **275.2 Why is this directive necessary?**

New Government-wide requirements, referenced in the authorities cited in para. 275.4, mean that NARA must verify and certify personal identity and determine access suitability before issuance of any identification card.

### **275.3 To whom does this directive apply?**

- a. All NARA employees (full-time, part-time, and intermittent; permanent and temporary) including career interns;
- b. NARA volunteers;
- c. NARA student interns;
- d. Contractor employees working under NARA contract;
- e. Employees, volunteers, and contractors of the Foundation for the National Archives and Presidential library foundations;
- f. Employees of other Federal agencies who need recurring full-time or part-time unaccompanied access to staff-only areas of NARA facilities; and
- g. Any other individual who needs access to non-public areas of NARA facilities or NARA information systems for 15 consecutive days or more.

### **275.4 What is the authority for this directive?**

- a. 44 U.S.C. 2903

- b. Executive Order (E.O.) 10450, Security requirements for Government employment, as amended (April 27, 1953)
- c. HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors
- d. Federal Information Processing Standards Publication (FIPS) 201-1, March 2006, Personal Identity Verification (PIV) of Federal Employees and Contractors
- e. Office of Management and Budget Memorandum M-05-24, Implementation of Homeland Security Presidential Directive (HSPD)-12 – Policy for a Common Identification Standard for Federal Employees and Contractors (August 5, 2005)
- f. Memorandum from Linda M. Springer, Director, United States Office of Personnel Management to Heads of Departments and Agencies: Interim Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD-12 (December 18, 2007)

## **275.5 Definitions**

The following definitions include terms specific to this directive.

- a. **Access suitability determination** - A decision based on the character, reputation and trust-worthiness of an individual's fitness for issuance of an identification card, facility access media, or electronic authentication to access NARA facilities or IT systems. Access suitability is different from employment suitability, and, unlike employment suitability, applies to all candidates for access to NARA facilities or IT systems, whether or not they are employees.
- b. **Candidate** - All NARA employees (full-time, part-time, intermittent, or temporary) including career interns; contractor employees working under NARA contract; employees, volunteers, and contractors of the Foundation for the National Archives and Presidential library foundations; volunteers; student interns; other Federal Government agencies' employees with a need for recurring full-time or part-time unaccompanied access to staff-only areas of NARA facilities; and any other individual requiring repeated access to non-public areas of NARA facilities or NARA information systems for 15 consecutive days or more.
- c. **Electronic authentication** - User names and passwords for access to NARA IT Systems. See NARA IT Security Mechanisms, version 5.0, dated February 28, 2008, for further specific information.
- d. **Electronic Questionnaires for Investigations Processing (e-QIP)** - A secure web site that is designed to house all personnel investigation forms, including the SF-85, Questionnaire for Non-Sensitive Position; SF-85P, Questionnaire for Public Trust Positions; and SF-86, Questionnaire for National Security Positions. OPM requires the use of this data collection tool that allows a user to complete his or her investigative form on-line instead of using paper forms which are no longer accepted.

e. **Facility access media** - An accountable document used to confirm that the holder has permission to enter “staff only” areas of NARA facilities. Examples of media used at NARA for employees, contractors, and volunteers include: NARA-issued PIV identification card with photograph, NARA identification card with photograph, and Temporary Building Pass with photograph. Examples of media used for visitors include the Visitor Pass and Tour Group Pass.

f. **Identification** - Documents that prove an individual candidate’s identity. (See Appendix B for a list of acceptable forms of identification.)

g. **Identity processor** - A current NARA employee with the authority to review and verify the identification presented by a candidate and submit the SF-85 and appropriate fingerprint chart to the Office of Personnel Management (OPM) using e-QIP. Normally this is a Security Management Branch (NASS) employee in the Washington, DC (DC) area or an administrative officer or Human Resources specialist outside the DC area.

h. **Issuer** - A current NARA employee with the authority to issue an approved identification card or other facility access media.

i. **Material fact** - A fact, which, had it been known before an access suitability determination, would have substantially influenced the decision to allow access authority for a candidate.

j. **Material intentional false statement** - A purposeful, inaccurate statement capable of influencing, or having a natural tendency to effect, an official decision.

k. **NARA identification card** - The identity card issued to individuals (NA form 6000) that is appropriate to their affiliation (federal employee, contractor, volunteer, etc.), contains identifying information such as photograph, name, and identification number, and is used to grant access to all NARA facilities and visually authenticate that the individuals have at a minimum, a favorably adjudicated National Agency Check with Inquiries (NACI).

l. **National Agency Check with Inquiries (NACI)** - The basic and minimum background investigation required of all individuals requesting an identification card or electronic authentication for NARA facilities or IT systems.

m. **DC area** - The following NARA facilities or offices: the National Archives Building; the National Archives at College Park, MD; the Washington National Records Center (Suitland, MD); and the Office of the Federal Register.

n. **Outside the DC area** - All NARA-occupied or NARA-operated facilities across the nation that are not located in the Washington, DC, area.

o. **Personnel Security Officer (PSO)** - The individual in NAS who is responsible for all access suitability investigations and adjudication procedures to determine if a candidate should be permitted access or continued access to NARA facilities or systems nationwide.

p. **Personnel Investigation Processing System (PIPS)** - A central data base of background investigations conducted by the Office of Personnel Management (OPM) and the adjudication results for those individuals, determined by the various Federal agencies served by OPM.

q. **Personal identity verification (PIV)** - the program for verifying the identity and access suitability of candidates, and issuing NARA identification cards, PIV identification cards, or electronic authentication.

r. **PIV identification card** - The identity card issued to an individual containing identifying information (such as photograph, name, and identification number) that meets the requirements of FIPS 201-1.

s. **Reciprocity** - A policy that requires acceptance by other Executive branch agencies of the Federal Government of the results of a background investigation and access suitability determination initiated or completed by another Executive branch agency of the Federal Government.

t. **Registrar** - A current NASS employee with the authority to adjudicate access suitability determinations for candidates and authorize issuance of an identification card or electronic authentication.

u. **Student intern** - An unpaid student who is not a Federal employee but who has been approved by his or her school and by NARA to participate in an uncompensated occupational training experience that complements his or her formal academic training.

v. **Sponsor** - A current NARA employee, normally a supervisor, human resources specialist, contracting officer's representative, contracting officer's technical representative, quality assurance inspector, volunteer coordinator, or administrative officer who would request facility access media to enter "staff only" areas of NARA facilities or electronic authentication for access to a NARA IT System.

w. **Temporary Building Pass (TBP)** - A version of the NA Form 6000 stamped with "TEMPORARY NARA ONLY" by the issuer, which is issued to a candidate pending approval authority from the registrar to issue an identification card.

x. **Volunteer** - An unpaid individual who is not a Federal employee but whose services have been accepted by NARA to enhance NARA's mission and services to the public.

y. **Visitor** - Any individual who does not possess a valid NARA-authorized access-granting document, such as a TBP, NARA or PIV identification card, and requires access to non-public areas of NARA facilities for 14 days or less on a non-recurring basis.

## 275.6 Who is responsible for implementing this directive?

a. **Archivist of the United States** - Certifies in writing to the Office of Management and Budget (OMB) that NARA policies and procedures for establishing proof of identity and registration meet the control and security standards that Federal agencies must follow to verify the identity and access suitability of a candidate and authorize issuance of an identification card.

b. **NARA Senior Official for Privacy (NGC)** - Ensure that NARA implementation of this guidance complies with all legal and administrative privacy requirements.

c. **Director, Acquisition Services Division (NAA)** - Ensure that language implementing this guidance is included in NARA contracts.

d. **Director, Human Resources Services Division (NAH)** - Act as sponsor and identity processor for newly-hired NARA employees in the DC area, except the Washington National Records Center (NWMW).

e. **Director, Information Technology (IT) Services Division (NHT)** - Grant access to NARA IT infrastructure by assignment of electronic authentication upon submission of application by the sponsor.

f. **Director, Space and Security Management Division (NAS)** -

(1) Establish the NARA-wide process for verification of identity, determination of candidates' access suitability, and issuance of TBPs, identification cards, and electronic authentication;

(2) For Presidential libraries, regional records services facilities, and the National Personnel Records Center (NRP), ensure compliance with this directive and the processes used to verify identity, determine candidates' access requirements, and issue TBPs, identification cards, and other access media;

(3) Ensure the successful completion of background investigations and make access suitability determinations;

(4) Assign NASS personnel to serve as identity processors, issuers, and registrars for candidates in the Washington, DC, area; and

(5) Maintain the stock of the NARA Identification Card (NA Form 6000) and ensure that stock is provided to valid NARA issuers only.

g. **Chief, Security Management Branch (NASS)** -

(1) Ensure that different individuals serve as the identity processor and registrar for identification cards in the DC area;

(2) Monitor and track background investigations for all candidates;

(3) Notify Presidential library directors, regional administrators, and the Director, NRP, if a successfully adjudicated background investigation for a candidate is on file with another agency;

(4) Notify Presidential library directors, regional administrators, the Director, NRP, Director NAH, contracting officer's representatives, volunteer coordinators, and other officials as appropriate, of any adverse information that could result in adverse action regarding a candidate being unsuitable for issuance of facility access media or electronic authentication;

(5) Ensure all NASS personnel have the required training to perform assigned roles as described in this directive;

(6) Review, approve, or disapprove requests for 24-hour access to Archives I and Archives II, through the building Security Team Leaders, in conjunction with the appropriate office head/staff director;

(7) Ensure local procedures are established for visitors, temporary employees, and tour groups, making certain they are issued temporary access media appropriate to their status, signed in, escorted, and signed out on a daily basis using NA Form 6014, when access is required into non-public areas of NARA facilities. Deviations from using standard temporary access media and the NA Form 6014 must be approved in advance by NASS;

(8) Adjudicate access suitability of candidates;

(9) Ensure that required investigations are initiated in a timely manner and monitored through completion;

(10) Maintain records of background investigations in accordance with OPM regulations;

(11) Document the reasons for all access suitability decisions in each individual's security folder;

(12) Assist all offices in determining the level of investigation to be conducted on contractors' employees working in NARA facilities (must be at least a NACI); and

(13) Obtain the documents needed to conduct background investigations on candidates in the Washington, DC, area and submit the investigative requests to OPM.

h. **Director, IT Security Staff (NHI)** - Ensure that initial security awareness training is made available so that the individual's sponsor, supervisors, or Contracting Officer's Representative/Contracting Officer's Technical Representative (COR/COTR), can ensure that the individual receives an orientation before requesting access to any NARA IT system.

i. **Directors of Presidential Libraries, Regional Administrators, and Director, National Personnel Records Center (NRP)** -



- (1) Implement and oversee the access application process at facilities under their jurisdiction;
- (2) Ensure that different individuals serve as the identity processor and issuer at the facilities under their jurisdiction;
- (3) Ensure candidate documentation is provided to the PSO. (See para. A.1 in Appendix A for a description of the required documentation.);
- (4) Control the local stock of NA Form 6000 the issuer provides by accounting for the forms by serial number, ensuring the forms are kept in a secured container, and issuing them only to candidates:
  - (a) As temporary building passes upon submission of the background investigation package; and
  - (b) Whose eligibility for an identification card has been determined.
- (5) Ensure the issuer provides the identification card to the candidate only after approval of the registrar;
- (6) Serve as the sponsor, or delegate sponsorship, for newly-hired employees volunteers, contractors, student interns, Library foundation employees (Presidential library directors only) and also act as sponsor for replacement or renewals of facility access media or electronic authentication as needed;
- (7) Ensure all identity processors and issuers at their facilities have the required training to perform assigned roles as described in this directive;
- (8) Review, approve, or disapprove requests for 24-hour access to facilities under their authority;
- (9) Ensure local procedures are established for visitors, temporary employees, and tour groups, making certain they are issued temporary access media appropriate to their status, signed in, escorted, and signed out on a daily basis using NA Form 6014, when access is required into non-public areas of NARA facilities;
- (10) Ensure that their candidates complete the required documents and submit them to their local e-QIP processor (normally the administrative officer) within the required time frame; and
- (11) Take action to implement appropriate procedures to remove employees, contractor's employees, volunteers, or interns from access to their facilities and IT systems, as applicable, within 24 hours of any access unsuitability determination made by NASS.

j. **Director, Washington National Records Center (NWMW) -**

- (1) Serve as the sponsor, or delegate sponsorship, for newly-hired employees, volunteers, contractors, and student interns, and also act as sponsor for replacement or renewals of facility access media or electronic authentication as needed;
- (2) Ensure candidate documentation is provided to the PSO (See para. A.1 in Appendix A for a description of the required documentation);
- (3) Review, approve, or disapprove requests for 24-hour access to facilities under his or her authority;
- (4) Ensure local procedures are established for visitors, temporary employees, and tour groups, ensuring they are issued temporary access media appropriate to their status, signed in, escorted, and signed out on a daily basis using NA Form 6014, when access is required into non-public areas of NARA facilities;
- (5) Ensure that candidates complete the required documents and submit them to NASS within the required time frame; and
- (6) Take action to implement appropriate procedures to remove employees, contractor's employees, volunteers, or student interns from access to their facilities and IT systems, as applicable, within 24 hours of any access unsuitability determination made by NASS.

k. **Office heads/staff directors** - When applicable, serve as the sponsor for candidates who are student interns, employees of other Federal government agencies requiring recurring access to NARA staff-only areas, and any other individual (other than employees, contractors, and volunteers) requiring repeated access to non-public areas of NARA facilities or IT systems for 15 consecutive days or more.

- (1) Ensure that their candidates complete the required documents and submit them to NASS within the required time frame; and
- (2) Take action to implement appropriate procedures to remove employees, contractor's employees, volunteers, or student interns from access to NARA facilities and IT systems, as applicable, within 24 hours of any access unsuitability determination made by NASS.

l. **Director, Center for the National Archives Experience (NWE)** - Serve as the sponsor for candidates who are employees, contractors' employees, or volunteers of the Foundation for the National Archives.

- (1) Ensure that candidates complete the required documents and submit them to NASS within the required time frame; and
- (2) Take action to implement appropriate procedures to remove employees, contractor's employees, volunteers, or student interns from access to their facilities and IT systems, as applicable, within 24 hours of any access unsuitability determination made by NASS.

**m. Supervisors -**

- (1) Serve as the sponsor for employees under their jurisdiction;
- (2) Take the following actions for individuals requiring access to NARA IT

Systems:

(a) Ensure initial security awareness orientation has been accomplished for the individual as appropriate; and

(b) Complete NA Form 3053, New User Request.

(3) Ensure that their employees complete the required documents and submit them to NASS within the required time frame; and

(4) In conjunction with NAH, ensure procedures in accordance with Interim Guidance 300-1, NARA Personnel Manual, ch. 752, Disciplinary and Adverse Actions, July 13, 1999, are implemented upon notification of any employee who is determined unsuitable for issuance of facility access media or electronic authentication.

**n. Contracting Officer Representatives/Contracting Officer Technical Representatives (COR/COTR) -**

(1) In conjunction with the contractor's project manager or supervisor, serve as the sponsor for candidates who are contractors' employees;

(2) Delegate sponsor responsibilities to Assistant COR's or Quality Assurance personnel actively monitoring designated contract, as needed;

- (3) Take the following actions for individuals requiring access to NARA IT

Systems:

(a) Ensure initial security awareness orientation has been accomplished for the individual as appropriate; and

(b) Complete NA Form 3053, New User Request.

(4) Ensure contractor's employees complete the required documents and submit them to NASS within the required time frame, as referenced in para. A.1 in Appendix A; and

(5) Take action to remove contractor's employees from access to NARA facilities and IT systems, as applicable, within 24 hours of any access unsuitability determination made by NASS in conjunction with NAA and their director or office head.

**o. Volunteer coordinators -**

- (1) Serve as the sponsor for candidates who are volunteers;
- (2) Ensure that their volunteers complete the required documents and submit them to NASS in the DC area or their local e-QIP processor outside the DC area within the required time frame, as referenced in para. A.1 in Appendix A;
- (3) Take the following actions for individuals requiring access to NARA IT Systems:
  - (a) Ensure initial security awareness orientation has been accomplished for the individual as appropriate; and
  - (b) Complete NA Form 3053.
- (4) In conjunction with their director or office head/staff director and volunteer supervisors, take action to remove volunteers from access to NARA facilities and IT systems, as applicable, within 24 hours of any access unsuitability determination made by NASS.

**p. Candidates for an identification card -**

- (1) Complete the paperwork required for an identification card truthfully, accurately, and within the time constraints directed;
- (2) Personally appear before the sponsor, identity processor, and issuer with the required paperwork and forms of identification (See Appendices A and B for details.); and
- (3) Take initial security awareness orientation before receiving IT systems access to NARA IT Systems.

**q. Identification card holders -**

- (1) Display their identification card at all times when present on NARA property;
- (2) Complete the paperwork required for renewal of their identification card truthfully, accurately, and in a timely manner, but no earlier than two weeks before the expiration date of the identification card; and
- (3) Personally appear before the sponsor, identity processor, and issuer with the required paperwork and forms of identification needed for identification card renewal. (See Appendices A and B for details.)

**275.7 Can the identity processor or the registrar also be the issuer?**

Yes, however no individual can perform both of the roles of identity processor and registrar for a single request for an identification card. FIPS 201 mandates a separation of duties, so no single individual has the ability to validate personal identity without the participation of another authorized individual.

**275.8 How does a sponsor request an identification card or renewal of an identification card for a candidate?**

Follow guidance in Appendix A.

**275.9 How does NARA determine access suitability for contractor's employees, volunteers and student interns?**

NARA uses OPM guidance in HSPD-12 to determine access privileges for contractor's employees, volunteers, and student interns. See Appendix C for specific procedures.

**275.10 What happens if an individual needs an investigation higher than a NACI?**

The office heads/staff directors, Directors of Presidential libraries, regional administrators, the Director, National Personnel Records Center, and the Director, Washington National Records Center, prepare an NA Form 3016, Personnel Security Action Request and Certification, requesting the specific investigation, i.e., public trust, and submit it to the NARA Personnel Security Officer. If a national security clearance is required, follow the procedures in NARA 273, Collateral Security Clearances.

**PART 2 – Use of an identification card****275.11 How must visitor badges, temporary passes, and identification cards be displayed?**

Visitor badges, temporary passes, and identification cards must be visible from the front and be at or above the belt line while in the staff-only or restricted areas of any NARA-owned or NARA-operated facility. When an individual with an identification card is actively engaged in an activity that would make wearing the identification card hazardous, the identification card must be displayed on the person's arm in a NARA-provided arm band.

**275.12 Are there other rules regarding the display of identification cards?**

Yes. Regional administrators, Directors of Presidential libraries, and Directors of the National Personnel Records Center and the Washington National Records Center have the authority to issue additional rules regarding the use and display of identification cards for facilities under their jurisdiction.

**275.13 What happens if the identification card is left at home?**

The identification card holder follows the security policy and procedures for temporary building entry at his or her location.

**275.14 Is an identification card needed to obtain access to NARA IT systems?**

No, but the individual's supervisor or COR must request an IT account using NA Form 3053, IT New User Account Request, to create a network account for the candidate when the initial TBP is issued.

**PART 3 – Temporary access**

**275.15 Are visitors required to be escorted by a NARA TBP or identification card holder in non-public or staff-only areas of facilities operated or occupied by NARA?**

Yes. Visitors are required to be escorted at all times while in non-public or staff-only areas. If the visitors are part of a tour group, there is a required ratio of one NARA TBP or identification card holder for each 10 visitors in a tour group. (For example, if there are 11 to 20 visitors in a tour group, this would require two NARA TBP or identification holders to escort the group on the tour, and so forth.)

**275.16 What are the procedures for temporary access control?**

a. Temporary access control is governed by local standard operating procedures using the approved NARA forms listed below:

- (1) NA Form 6014, Record of Time of Arrival and Departure from Building
- (2) NA Form 6002F, Tour Group Pass
- (3) NA Form 6002H, Visitor Pass
- (4) NA Form 6002I, Temporary Employee Pass

b. To obtain these forms, see NARA Directive 207, NARA Editing and Design Services, Appendix C.

**275.17 Why is there a Temporary Employee Pass?**

On occasion, TBP or identification card holders may have left their access media at home or lost the access media and will need to be signed in for that business day. These individuals must be issued a NA Form 6002I, Temporary Employee Pass to have access to staff-only areas.

**275.18 How are the Temporary Employee Passes issued?**

When an individual arrives at the facility without his or her TBP or identification card, the supervisor, project manager, or individuals responsible for building security must be contacted to verify employment. No other identification card or TBP holder can verify employment of another individual for this purpose because they may not have current information in regard to the person's employment status. Once verified, the individual is issued the temporary employee pass for that business day. Individuals issued temporary employee passes do not require escort in staff-only areas, but the pass must be turned in when the individual leaves the building.

**PART 4 – 24-hour access****275.19 Who authorizes 24-hour access to NARA-owned and NARA-operated facilities?**

a. The Directors of Presidential Libraries, National Personnel Records Center, Federal Register, Washington National Records Center, and Regional Administrators are authorized to decide who may have 24-hour access to facilities under their control;

b. The Archives I and Archives II Physical Security team leaders are authorized to decide who may have 24-hour access for Archives I and Archives II, respectively, after receiving requests from responsible supervisors, staff directors, or office heads/staff directors; and

c. The NARA Inspector General (IG) is authorized to designate which IG personnel may have 24-hour access to NARA-owned or –operated facilities.

#### **275.20 How is 24-hour access designated on identification cards?**

a. In the DC area, the number “24” is printed on the face of the identification card before lamination. NASS does not authorize a sticker or writing on the face of the card to designate “24”-hour access and considers such actions as criminal alteration of the card.

b. Outside the DC area, a yellow NA Form 6000 is used to designate “24”-hour access. See appendix D for details.

c. On the PIV identification card, the number “24” is printed on the face of the identification card before lamination. NASS does not authorize a sticker or writing on the face of the card to designate “24”-hour access and considers such actions as criminal alteration of the card.

#### **275.21 Can I be issued a 24-hour access authorized identification card if I come to work earlier or stay later than normally posted building operational hours?**

a. No, 24-hour access is not for this purpose. See para. 275.22 for more information.

b. For occasional work that occurs outside normal building operations hours, your supervisor should coordinate with those individuals responsible for facility security to arrange access or occupancy outside of normal operating hours as soon as practical in advance to accommodate the access.

#### **275.22 Why can’t everyone be authorized 24-hour access?**

In order to ensure collections and building security, 24-hour access is granted on a case by case basis. Normally access to facilities on a 24-hour basis is only routinely issued to individuals in positions that support 24-hour operations at a facility, such as those personnel responsible for maintenance and security during non-operational hours. Individuals designated as emergency employees or mission-critical emergency employees in accordance with Interim Guidance 300-33, Assignment and Deployment of Emergency Employees and Mission Critical Emergency Employees, may be authorized 24-hour access to support emergency operations.

### **PART 5 – Administrative**

#### **275.23 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 the identity processor, issuer, and registrar are 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.

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

a. **NASS -**

(1) Issuance of identification cards, TBPs, and other access media for NARA facilities and IT systems access in the DC Area – Follow the disposition instructions for file nos. MACROBUTTON HtmlResAnchor 649, “Credentials Files,” and MACROBUTTON HtmlResAnchor 650, “Visitor Control Files,” as applicable.

(2) Background investigations and access suitability process – Use file no. MACROBUTTON HtmlResAnchor 312-1 for security folders for NARA employees and applicants for employment, contractors, volunteers, student 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. MACROBUTTON HtmlResAnchor 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 MACROBUTTON HtmlResAnchor 313.

b. **Directors of Presidential libraries, regional administrators, and Director, National Personnel Records Center** - For issuance of identification cards, TBPs, and other temporary access media at facilities outside the DC area, follow the disposition instructions for file nos. MACROBUTTON HtmlResAnchor 649 and MACROBUTTON HtmlResAnchor 650, as applicable.

c. **Director, Washington National Records Center** - For issuance of TBPs and other temporary access media, follow the disposition instructions for file nos. MACROBUTTON HtmlResAnchor 649 and MACROBUTTON HtmlResAnchor 650, as applicable.

d. **Supervisors** - Keep records pertaining to employees (e.g., copies of the SF-52 and NA Form 3016) in an unofficial personnel file (UPF) for each individual in accordance with file no. MACROBUTTON HtmlResAnchor 303-1.

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



f. **Volunteer coordinators** - Use file no. MACROBUTTON HtmlResAnchor 1605-3, “Volunteer and Tour Program Files: Individual Volunteer Files.”

g. **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. Please note that your supervisor does not have electronic access to your investigative forms in e-QIP, and does not receive any paper copies of these forms as part of the access suitability process.

**Appendix A - How to obtain an identification card or other access media****A.1 How does a sponsor request facility access media or renewal of facility access media for a candidate?**

The sponsor must do the following:

- a. Complete items 1-6 and 9-15 of NA Form 6006, Identification Card Request (see Appendix E for an example of the form);
- b. Ensure the candidate signs and dates the form in items 7 and 8; and
- c. Ensure the candidate completes and signs the OF 306, Declaration for Federal Employment.
- d. Forward to the identity processor via memorandum, e-mail, or orally, the candidate's full name (including middle name), social security number, place of birth, date of birth, and e-mail address, to permit OPM e-portals PIPS check and e-QIP initiation, if needed.
- e. Ensure the candidate completes the background questionnaire in e-QIP within five business days of being directed to do so by the identity processor or registrar.
- f. Take the candidate and all paperwork to the local NARA identity processor for a review by that individual of the accuracy and validity of the identity documents.

**A.2 Which background questionnaire is required for the issuance of access media?**

a. An appropriate background questionnaire (SF-85, SF-85P or SF-86) is required for all candidates for new and renewed identification cards or other access media when there is no current report of a successfully adjudicated background investigation on file. A current report is one that is:

(1) At the level appropriate for the candidate's current critical sensitive position;  
or

(2) A NACI that is less than 15 years old.

b. For a candidate needing a current report and in a position not involving national security or public trust, as determined by NAH, an SF-85 must be completed.

c. For a candidate needing a current report and in a position of public trust, as determined by NAH, an SF-85P must be completed.

d. For a candidate needing a current report and in a national security position that requires a security clearance, as determined by NAH, an SF-86 must be completed.

e. In keeping with HSPD-12, all current identification card or other access media holders must also undergo a background investigation in the following circumstances. NASS will schedule the investigations as needed and inform the supervisor:

(1) If there is no successfully adjudicated background investigation on file when their current identification card or access media expires.

(2) If there is a successfully adjudicated background investigation on file that is more than 15 years old or not at the level appropriate for their current position.

f. All current facility access media holders with a successfully adjudicated background investigation on file that is less than 15 years old at the time of expiration of their facility access media, and appropriate to their current position, will not be required to undergo a background investigation when their current facility access media expires.

**A.3 How does the identity processor in the DC area determine if the candidate has a previous successfully adjudicated background investigation that is acceptable for issuance of an identification card or electronic authentication?**

In the DC area, the identity processor checks the OPM e-portal PIPS to determine if a previously acceptable investigation was successfully adjudicated.

- a. If PIPS has no record on file, follow the procedures in para. A.5.
- b. If PIPS shows a closed appropriate investigation, follows the procedures in para. A.6.
- c. If PIPS shows an investigation that may have disqualifying issues,
  - (1) Requests the file from OPM for review.
  - (2) Issues the candidate a TBP, pending receipt and review of the file.
  - (3) Takes the following actions, as appropriate, once the file is reviewed and access suitability determined:
    - (a) For a favorably adjudicated background investigation, follows procedures in para. A.6.
    - (b) For an unfavorably adjudicated background investigation, follows procedures in para. C.10.

**A.4. How does an identity processor outside the DC area determine if the candidate has a previous successfully adjudicated background investigation that is acceptable for issuance of an identification card?**

a. Outside the DC area, the identity processor provides the full name, social security number, date of birth, and place of birth (city and state, or city and country if born outside the United States) to their NASS registrar.

b. The NASS registrar checks PIPS to determine if a previously acceptable investigation was successfully adjudicated and provides the results to the outside-the-DC-area identity processor who:

- (1) If PIPS has no record on file, follows the procedures in para. A.5.
- (2) If PIPS shows a closed appropriate investigation, follows the procedures outlined in para. A.6.
- (3) If PIPS shows an investigation that may have disqualifying issues:
  - (a) Asks the registrar to request the file from OPM for the registrar to review; and
  - (b) Issues a TBP to the candidate, pending receipt and review of the file by the registrar.
- (4) Then takes the following actions, as appropriate, once the file is reviewed and access suitability determined:
  - (a) For a favorably adjudicated background investigation, follows the procedures in para. A.6.
  - (b) For an unfavorably adjudicated background investigation, the NASS registrar follows procedures in para. C.10.

**A.5 What does the identity processor do if the candidate does not have a current NACI?**

The identity processor:

a. Reviews the candidate's NA 6006, OF-306, and the General Release Form and Certification page the candidate obtains from e-QIP.

b. Logs on to e-QIP to verify the accuracy of the document prepared by the candidate for their background investigation and prints out a copy of the document.

c. Retains a file copy of the NA 6006, the SF-85, SF-85P, or SF-86, as appropriate, and the OF-306.

d. Provides instructions to the candidate for obtaining fingerprints or take fingerprints of the candidate, as appropriate.

(1) An SF-87, Fingerprint Card for Federal Position, is used for Federal employees; and

(2) An FD-258, Applicant Fingerprint Card is used for volunteers, student interns, Foundation employees and contractors, and NARA contractor employees.

e. Verifies the identification presented by the candidate and makes a copy of each form for retention in the file of the candidate. (See Appendix B for a list of acceptable identification documents that may be used for this purpose.)

f. Completes items 19 through 21 of the candidate's NA Form 6006, checks the first and third items in the certification statement in section B of the form, and signs and dates the certification in items 22 and 23.

g. Issues the candidate a TBP valid for no longer than six months and have them sign for receipt in items 24 and 25.

(1) For outside the Washington, DC, area, see Appendix D for instructions on preparing a TBP.

(2) For the Washington, DC, area, NASS uses the facility access control system to issue the TBP, in accordance with NASS internal standard operating procedures.

**A.6 What does the identity processor do once a determination is made that the candidate's NACI is adjudicated favorably based on a check of PIPS or after the e-QIP submission?**

a. For the Washington, DC, area, the identity processor:

(1) Verifies the identification presented by the candidate and makes a copy of each form for retention in the file of the candidate. (See Appendix B for a list of acceptable identification documents that may be used for this purpose.);

(2) Completes items 19 through 21 of the candidate's NA Form 6006, checks the first and second items in the certification statement in section B of the form, and signs and dates the certification in items 22 and 23; and

(3) Forwards the candidate's file to the registrar for further processing.

b. For outside the Washington, DC, area, the identity processor:

- (1) Completes items 19 through 21 of the candidate's NA Form 6006, checks the first and second items in the certification statement in section B of the form, and signs and dates the certification in items 22 and 23;
- (2) Makes photocopies of the identification documents presented by the candidate and places all appropriate documentation in the candidate's file;
- (3) Annotates items 26 through 30 with the information received from the registrar, entering "/s/" with the registrar's name in item 31; and
- (4) Forwards the candidate's file to the issuer for issuance of an identification card or access media.

**A.7 What does the registrar do?**

- a. Ensures a separation of duties between identity processor functions and registrar functions.
- b. Determines the suitability of a candidate to receive an identification card.
- c. Ensures items 26 through 30 are completed on the candidate's NA Form 6006.
- d. Signs item 31 and completes item 32 on the Washington, DC, area candidate's NA Form 6006.
- e. Instructs the identity processor, outside the DC area, to enter the registrar's name in block 30 of NA Form 6006 and follow guidance in para.A.6b.
- f. Authorizes the DC area or outside-the-DC-area issuer to issue:
  - (1) A NARA identification card or
  - (2) A PIV Card.

**A.8 What does the Issuer do?**

- a. Issues additional TBPs until the results of the background investigation are returned for the candidate.
- b. When notified by the registrar that the NACI has been approved, issues an appropriate identification card or access media to the candidate, completes items 33 through 39, and ensures the candidate completes items 40 and 41 of the NA Form 6006.
- c. Re-issues replacement or renewal identification cards or access media as necessary when requested by the sponsor and processed by the identity processor.

**A.9 What is the purpose of the Temporary Building Pass?**

The results of the background investigation have to be received and adjudicated before the identification card can be issued. Since this may take several weeks or months, a TBP is issued. The TBP allows unaccompanied access, to the extent deemed appropriate by the sponsor, to non-public, non-classified areas of NARA facilities and information systems.

**A.10 When is a candidate issued his or her identification card or facility access media?**

Upon receipt of the background investigation results, the registrar determines the candidate's suitability for access to NARA facilities and IT systems, in accordance with OPM policy and guidance.

a. If the candidate is found suitable for access, the registrar notifies the issuer, who then issues the identification card.

b. If the candidate is found unsuitable for access, the registrar notifies the issuer and the sponsor. The sponsor, designated below by type of candidate, takes appropriate action in accordance with relevant rules, regulations, and contract language, when notified that a candidate has been found unsuitable for access:

(1) NARA employee - Supervisor and Human Resources Services Division (NAH);

(2) Contractor employee - contracting officer's representative;

(3) Employee, contractor, or volunteer of the Foundation for the National Archives or Presidential library foundations - Director, NWE, or director of the appropriate Presidential library;

(4) Volunteer - volunteer coordinators; and

(5) Student intern, employee of another Federal Government agency, or other individual requiring repeated access to non-public areas of NARA facilities for 15 or more consecutive days - division or staff director.

**A.11 How long is the NARA identification card or PIV identification card valid?**

a. The initial and renewal identification card are valid for no more than five years.

b. Upon separation of the candidate, or revocation by the sponsor or registrar, the identification card is no longer valid and must be returned to the issuer.

**A.12 What happens if the NARA identification card or PIV identification card is lost?**

If an identification card is lost, the candidate follows the card renewal process described below.

a. The candidate immediately reports the loss to his or her supervisor if a NARA employee or sponsor for all others and the office that issued the identification card or TBP.

b. The supervisor or sponsor then:

- (1) Completes items 1-6 and 9-18 of an NA Form 6006;
- (2) Ensures that the candidate signs and dates the form in items 7 and 8;
- (3) Forwards via memorandum, e-mail, or orally, the applicant's full name, social security number, place of birth, date of birth, and e-mail address to the identity processor; and
- (4) Ensures the incident report has been filed.

c. The candidate reports to the local identity processor with the NA Form 6006 and forms identified in NA Form 6006 Part B, including a copy of the incident report.

d. The identity processor requests verification from the registrar that the candidate has a current background investigation.

(1) If the candidate has a current background investigation, the identity processor annotates information in items 26-30, noting the re-issuance of a lost identification card in item 28, and forwards the application to the issuer.

(2) If the candidate does not have a current background investigation, the identity processor advises the candidate to prepare the appropriate forms (SF-85, SF-86, SF-85P, OF-306 and either SF-87 or FD-258) and returns the completed forms to the identity processor for follow-up in accordance with para. A.5.

**A.13 How is an identification card renewed?**

The sponsor and candidate follow procedures described in para. A.1.

**A.14 How are records created by this appendix maintained under the NARA Records Schedule?**

Records are maintained according to the procedures in para. 275.24.



### Appendix B - List of acceptable forms of identification

**Note: The candidate must present two forms of identification, at least one form of identification must be the type described in column 1.**

<b>1. Government-Issued Identity Document Containing a Photograph (Photo ID)</b>	<b>2. Other Identity Document Issued by Approved Government Entities</b>
Identification card issued by Federal, state or local government agencies or entities in the USA or outlying possessions, provided it contains a photograph	Identification card issued by Federal, state or local government agencies or entities in the USA or outlying possessions, provided it contains information such as name, date of birth, gender, height, eye color, and address
Driver's license issued by a state or outlying possession of the US provided it contains a photograph and other identifying information such as name, date of birth, gender, height, eye color, and address	Driver's license issued by a state or outlying possession of the US provided it contains information such as name, date of birth, gender, height, eye color, and address
United States passport (unexpired or expired)	Voter's registration card
Certificate of United States Citizenship (N-560 or N-561)	U.S. Coast Guard Merchant Mariner card
Certificate of Naturalization (N-550 or N-570)	Native American tribal document
Unexpired foreign passport, with I-551 stamp or attached Form I-94 indicating unexpired employment authorization	Driver's license issued by a Canadian government authority
Permanent Resident Card or Alien Registration Receipt Card w/photograph (Form I-151 or I-551)	U.S. social security card issued by the U.S. Social Security Administration
Unexpired Temporary Resident Card (Form I-688)	Certification of Birth Abroad issued by the U.S. Department of State
Unexpired Employment Authorization Card (Form I-688A)	Original or certified copy of a birth certificate issued by a state, county, municipal authority or outlying possession of the United States and bearing an official seal
Unexpired Re-Entry Permit (I-327)	School based in the United States ID provided it contains a photograph of the candidate
Unexpired Refugee Travel Document (I-571)	Unexpired Employment Authorization Document issued by U.S. Department of Homeland Security that contains a photograph (I-688B)
Unexpired U.S. Military identification card	
Unexpired U.S. Military dependent's ID card	

## **Appendix C – Investigative requirements and access suitability process**

### **C.1 What are the investigative requirements for NARA employees, contractor's employees, student interns, and volunteers?**

For employees, the type of appointment and position sensitivity determines the type of investigation required for an access suitability determination. For contractor's employees, student interns, and volunteers, the work to be performed determines the type of investigation required.

- a. Employees, at a minimum, are subject to a successfully adjudicated (SA) NACI. Some employees may require a more thorough investigation (e.g., those working with classified documents).
- b. Contractors' employees working in the non-public areas of a NARA site, at a minimum, are subject to a SA NACI. Some contractors' employees may require a more thorough investigation (e.g., IT contractors' employees). For certain types of contracts, such as those for childcare workers, the investigative requirements may be determined in whole or part by applicable state or Federal laws. Contact NASS for guidance on required background investigations.
- c. All volunteers and student interns working in the non-public areas of a NARA site or with non-public services such as NARANET are subject to a SA NACI. Individuals working with children under the age of 18 are subject to a SA Child Care National Agency Check with Inquiries (CNACI) background investigation. See NARA 1606, Volunteer Programs, for further information.

### **C.2 Who has authority to conduct access suitability reviews for NARA?**

NASS is the sole branch responsible for making initial and final decisions on access suitability determinations for all individuals requiring access to NARA-operated or -owned facilities or IT systems.

### **C.3 How is an initial and final access suitability review conducted for candidates?**

#### **a. For employees**

(1) Human Resources Operation Branch (NAHO) and Employee Relations and Benefits Branch (NAHW) must obtain approval of an initial access suitability review determination before making a final commitment and establishing an effective date for placing an individual in a non-sensitive or sensitive position. NAHO/NAHW provides the following information to NASS when an applicant from outside of NARA has been selected for appointment to a non-sensitive or sensitive position:

- (a) Full name;
- (b) Social security number;
- (c) Date of birth (DOB);

(d) Place of birth (POB) - city and state if born in the United States or City and Country if born outside the United States;

(e) E-mail address;

(f) Position title, series, and grade;

(g) Organization code;

(h) Sensitivity level; and

(i) Copy of the individual's resume or application.

(2) Upon receipt of this information, NASS determines whether the individual has had the necessary investigation and successful adjudication of the investigation for access to NARA facilities or IT systems. For sensitive positions, NASS also has the individual sign a release under the Fair Credit Reporting Act of 1970, as amended, and conducts a credit check.

(3) NASS notifies the staffing specialist in NAHO or NAHW as soon as the individual has been initially successfully adjudicated for access to NARA facilities or IT systems. NAHO and NAHW do not make a final commitment to the selectee until NASS has provided the successful initial adjudication decision.

(4) NASS will conduct a final access suitability review after OPM completes the appropriate investigation and it is received at NARA. If the final results of the review and adjudication reveal any derogatory information which would result in an unfavorable access suitability determination, NASS notifies the employee's supervisor and NAHO and NAHW for appropriate action. However, if access is required for the employee to perform the job, an access unsuitability determination may require removal from employment. Such action is taken in accordance with Interim Guidance 300-1, NARA Personnel Manual, Ch. 752, Disciplinary and Adverse Actions, or other appropriate authority, as coordinated with NAH.

(5) For critical sensitive positions with access to national security information, NARA Directive 273, Collateral Security Clearances, is followed.

b. **For all other candidates for access** - There is no pre-screening process for all other candidates. They follow procedures outlined in Appendix A to obtain facility access media. If non-employee candidates are adjudicated unsuitable for access during the Appendix A facility access media process, para C.12 below outlines what actions may result.

#### **C.4 What circumstances require a reinvestigation of an employee's background?**

a. When an individual moves to a more sensitive position than the one previously occupied, the individual must meet the investigative requirements of the new position's sensitivity.

b. When the sensitivity of the position is changed for any reason (e.g., a change in position duties), the incumbent may remain in the position, but the investigation required by the

higher level sensitivity is initiated within 14 working days after the re-designation is final. Whenever such re-designation occurs, the responsible office immediately advises NASS.

c. When an individual's reinvestigation is required for a 5-year update or 10-year update, depending on the type of investigation, NASS schedules the updates and informs the affected individual(s).

d. In keeping with HSPD-12, all current identification card holders must also undergo a background investigation if there is:

(1) No successfully adjudicated background investigation on file when current identification cards expire; or

(2) A successfully adjudicated background investigation on file that is more than 15 years old or not at the level appropriate for the current position.

**C.5 What factors may disqualify a candidate from access to NARA facilities or IT systems?**

a. **Minimum access standards** - The following conduct factors apply to a determination of access unsuitability for all candidates:

(1) The candidate is known to be or reasonably suspected of being a terrorist;

(2) NARA is unable to verify the candidate's claimed identity;

(3) There is a reasonable basis to believe the candidate has submitted fraudulent information concerning his or her identity;

(4) There is a reasonable basis to believe the candidate will attempt to gain unauthorized access to classified documents, information protected by the Privacy Act, information that is proprietary in nature, or other sensitive or protected information;

(5) There is a reasonable basis to believe the candidate will use an identity credential outside the workplace unlawfully or inappropriately; or

(6) There is a reasonable basis to believe the candidate will use Federally-controlled information systems unlawfully, make unauthorized modifications to such systems, corrupt or destroy such systems, or engage in inappropriate uses of such systems.

**b. Additional access standards**

(1) **Employee candidates** - The following additional conduct factors, as applicable, are relevant to a determination of access unsuitability for employee candidates only:

(a) An employment suitability determination under 5 CFR part 731 that the candidate is unsuitable for the competitive civil service;

(b) Disqualification from appointment in the excepted service under 5 CFR part 302;

(c) Ineligibility for access to classified information under E.O. 12968; or

(d) Disqualification for employment under a similar authority.

(2) **Non-employee candidates** - The following additional conduct factors are relevant to a determination of access unsuitability for contractor, contractor employee, volunteer, student interns, and other non-employee candidates:

(a) There is a reasonable basis to believe, based on the candidate's misconduct or negligence in employment, that issuance of facility access media poses an unacceptable risk;

(b) There is a reasonable basis to believe, based on the candidate's criminal or dishonest conduct, that issuance of facility access media poses an unacceptable risk;

(c) There is a reasonable basis to believe, based on the candidate's material, intentional false statement, deception, or fraud in connection with federal or contract employment, that issuance of facility access media poses an unacceptable risk;

(d) There is a reasonable basis to believe, based on the nature or duration of the individual's alcohol abuse without evidence of substantial rehabilitation, that issuance of facility access media poses an unacceptable risk;

(e) There is a reasonable basis to believe, based on the nature or duration of the candidate's illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation, that issuance of facility access media poses an unacceptable risk;

(f) A statutory or regulatory bar prevents the candidate's contract employment, volunteer or intern work, or would prevent federal employment under circumstances that furnish a reasonable basis to believe that issuance of facility access media poses an unacceptable risk; or

(g) The candidate has knowingly and willfully engaged in acts or activities designed to overthrow the U.S. Government by force.

**C.6 What constitutes a reasonable basis to believe?**

A reasonable basis to believe occurs when a disinterested observer, with knowledge of the same facts and circumstances, would reasonably reach the same conclusion.

**C.7 Does unacceptable risk refer only to peoples' safety?**

An unacceptable risk refers to an unacceptable risk to the life, safety, or health of employees, contractors, vendors, or visitors; to the Government's physical assets or information systems; to personal property; to records, including classified, privileged, proprietary, financial, or medical records; or to the privacy of data subjects.

**C.8 Are there any additional factors that could be considered?**

Yes. The following special circumstances may be considered as part of the access suitability determination when assessing the standards and level of risk set forth in C.5 above:

- a. The nature of the position applied for or employed in;
- b. The nature and seriousness of the conduct;
- c. Circumstances surrounding the conduct;
- d. How recently the conduct occurred;
- e. The age of the individual at the time of the conduct;
- f. Contributing societal conditions; and
- g. The absence or presence of rehabilitation or clear evidence of efforts toward rehabilitation.

**C.9 Do access suitability decisions consider the candidate's qualifications for a position?**

No. Access suitability decisions consider only the character, reputation, and trustworthiness, not the competencies of the individual. Access suitability determinations are not the same as employment suitability determinations, although some of the factors may be similar.

**C.10 What happens if adverse information concerning a candidate is found?**

When, as a result of any background investigation, NARA discovers adverse information that impacts the subject's suitability for access or continued access, the NASS adjudicator writes a summary of the information. The summary may be shown to, and discussed with, NAH and the responsible NARA official to determine whether access should be removed or denied.

**C.11 What happens after an access unsuitability determination is made about a candidate?**

A candidate may be denied access to NARA facilities or IT systems, depending on the nature of the adverse information involved and the candidate's affiliation, duties, or position. For NARA employees, see C.3, subpara a (4) above. For all other candidates, see the next paragraph.

**C.12 What is the adverse action process for contractors' employees, volunteers, student interns, and other non-employee candidates?**

a. NASS adjudicates the access suitability of contractors' employees, volunteers, student interns, and other non-employee candidates based on the factors in C.5, subparas. a and b (2) above.

b. When the adjudicator finds that adverse information in a background investigation report is sufficiently serious to impact the candidate's suitability for access, the candidate is granted an opportunity to make an oral or written statement concerning the specific information in question. The statement or a summary of an oral presentation becomes a part of the candidate's file. The adjudicator, before making a final determination of access suitability, considers all information provided by the candidate. The provisions of para. C.14 concerning the administrative due process file are applicable to files of volunteers, student interns, and contractors' employees.

c. When the adjudicator determines an individual is unsuitable for access, NASS notifies the responsible NARA official.

(1) Contractors' employee - The Contract Officer Representative/Contract Officer Technical Representative (COR/COTR) is notified in writing. The COR/COTR notifies the contracting officer and the contractor's project manager that the candidate must be removed from the work site. Any government property (i.e., ID badge, access card, keys, parking permit, laptop, cell phone, pager, etc.) must be immediately surrendered to the COR/COTR. The COR/COTR returns all government property collected from the candidate to NASS and appropriate property custodian in the DC area, and to the appropriate official outside the DC area.

(2) Volunteer - The volunteer coordinator is informed in writing of the decision and that the candidate must be removed from the NARA worksite. The coordinator informs the appropriate supervisor or director. The supervisor or director must make arrangements to remove the volunteer from the work site. Any government property (i.e., ID badge, access card, keys, parking permit, laptop, cell phone, pager, etc.) must be immediately surrendered to the coordinator. The coordinator returns all government property collected from the candidate to NASS and appropriate property custodian in the DC area, and to the appropriate official in all other regions.

(3) Student intern - The supervisor is informed in writing of the decision and that the candidate must be removed from the NARA worksite. The supervisor informs the intern. Any government property (i.e., ID badge, access card, keys, parking permit, laptop, cell phone, pager, etc.) must be immediately surrendered to the supervisor. The supervisor returns all government property collected from the candidate to NASS and appropriate property custodian in the DC area, and to the appropriate official outside the DC area.

(4) Other non-employee candidates – The sponsoring or supervising official is informed in writing of the decision and that the candidate must be removed from NARA facilities or systems. The sponsor or supervisor informs the candidate. Any government property issued by NARA (e.g., ID badge, access card, keys, parking permit, laptop, cell phone, pager, etc.) must be immediately surrendered to the sponsor or supervisor. That person returns all government property collected from the candidate to NASS and appropriate property custodian in the DC area, and to the appropriate official outside the DC area. If the candidate is an employee with another federal agency, the candidate will not return to NARA government property issued by another federal agency. However, the candidate's supervisor at the other agency will be informed in writing of the decision and that the candidate was removed from access to NARA facilities or systems.

### **C.13 What rights does a candidate have to appeal a determination of access unsuitability?**

There are no appeal rights for candidates who are determined to be unsuitable for access based on the factors set forth in subpara. C.5. The NASS access suitability determinations are final. However, an employee candidate may have employment appeal rights if an adverse employment action is subsequently taken against them based upon an access unsuitability determination. Adverse employment actions do not come under the purview of this directive. Employees should refer to Interim Guidance 300-1, NARA Personnel Manual, Ch. 752, Disciplinary and Adverse Actions, or other appropriate authority, and consult with NAH, for more information on adverse employment actions and appeal rights from them.

### **C.14 What records must be created by the adjudicative process?**

The "Administrative Due Process File" must contain

- a. A copy of the OPM investigative report;
- b. A copy of any written summary to inform a supervisor or official of the adjudication;
- c. A copy of all written challenges, replies, and documentation supplied by the subject of the investigation;
- d. A written summary of any oral response;
- e. A record of all disclosures and access to the file; and



f. All other documents directly related to the issue. Include information provided by non-corroborated confidential sources. It may be used as a basis for further investigation or for questioning of the candidate, but cannot be the basis for an access suitability determination.

**C.15 Can investigative material be disclosed or released?**

NASS maintains investigative files and other source documents gathered in the access suitability determination process. Determinations regarding the disclosure of investigative materials are made in accordance with the provisions of the Privacy Act (5 U.S.C. 552a) and NARA 24, Personnel Security Files. NASS coordinates all requests for access with the NARA Privacy Act Officer (NGC).

**C.16 How are records created by this appendix maintained under the NARA Records Schedule?**

Records are maintained according to the procedures in para. 275.24.

**Appendix D - Instructions for preparing an outside the DC area Temporary Building Pass (TBP)**

There are 4 colors of TBP paper card stock. The choice of color depends on the status and access requirements listed below.

- |         |  |
|---------|--|
| BLUE:   | For NARA employees requiring less than 24-hour-a-day, 7-day-a-week access.   |
| YELLOW: | For NARA employees requiring 24-hour-a-day, 7-day-a-week access.   |
| GREEN:  | For NARA-affiliated foundation employees, volunteers and contractors; and NARA volunteers and unpaid interns.  |
| WHITE:  | For NARA contract employees, other Federal Government employees, and any other individual needing repeated access for more than 15 consecutive days to non-public areas of NARA facilities. For those requiring 24-hours-a-day, 7-day-a-week access to the building, type "24/7 Access" in |

the "Building" space to the left of name of the building on the back of the TBP.

Fill out the form using a typewriter with black ink.

The expiration date must not exceed six months from date of issuance, in the first instance of issuance. On expiration of the initial six-month period, TBPs may be reissued at six-month intervals until the results of the background investigation are returned and adjudicated.

The authorizing signature is the signature of the issuer.

Enter all signatures using black ink.

Once completed and signed by the FIC candidate, "TEMPORARY NARA ONLY" should be stamped or written in red ink below the candidate's photograph on the front of the card, as shown in the example below.

Laminate the completed card.

### Front View

### Back View

### Appendix E - NA Form 6006, Request for Personal Identity Verification

This form is available online at [http://\[e-forms web page\]](http://[e-forms web page]) in a fillable format. Do not use the version reproduced on this page of the directive, which is for your information only.

	<p style="text-align: center;"><b>National Archives and Records Administration</b></p> <p style="text-align: center;"><b>Identification Card Request</b></p>
--	--

**A. Identification Card Request and Source Document Confirmation** (To be completed by Sponsor)

1. Replacement Card: ☐ Yes ☐ No      1a. Reason for Replacement: ☐ Defaced ☐ Lost ☐ Expired
2. Background investigation completed: ☐ Yes ☐ No      2a. If Yes, type and date completed:
3. Background investigation package completed? ☐ Yes ☐ No

**Candidate Affiliation (check all that apply):**

4. Type: ☐ Foreign National ☐ NARA employee ☐ Contractor ☐ Volunteer ☐ Foundation  
☐ Student Intern ☐ Other

5. Name (Last, First, MI)      DOB      Hair Color      Eye Color      Height Weight  
 Last First MI      [mm/dd/yyyy]

6. Agency:      Firm:      24 Hour Access? ☐ Yes ☐ No

*I, the candidate, certify that the Candidate Affiliation entered above is accurate to the best of my knowledge.*

**7. Candidate Signature:****8. Date:** [mm/dd/yyyy]

9. Candidate's Position/Title:
10. Candidate's NARA Office Code:
11. Candidate's Work Phone:
12. Candidate Access [e.g., buildings, rooms]:

**14. Sponsor Information:**

Name:

Office Code:

Phone No: (    )    -

13. Identification Card to be valid until: [mm/dd/yyyy]      15. Parking Permit: ☐ Yes ☐ No

16. Brass Keys to Room #'s

*I agree to sponsor the above candidate for an Identification Card and certify that the information in Section A is accurate to the best of my knowledge.*

**17. Sponsor Signature:****18. Date:** [mm/dd/yyyy]**B. Identity Proofing (to be completed by Identity Processor)**

19. Requires two forms of identification attached (one of which is a photo ID issued to the candidate by a state or the Federal Government)

**21. Identity Processor Information:**

Name:

Office Code:

Phone No: (    )    -

**20. Identity (ID) Source Documents Details**

Document One:            Type:            Issuing Authority:    Document Number:  
Expiration Date:

Document Two:            Type:            Issuing Authority:    Document Number:  
Expiration Date:

*I, the Identity Processor, certify that:*

☐ *the above Candidate appeared before me and presented two ID source documents that appeared to be genuine.*

☐ *a current NACI is on file for the above Candidate.*

**OR**

☐ *I have issued a Temporary Building Pass to the above Candidate pending completion of a current NACI.*

**22. ID Processor signature:**

**23. Date:** [mm/dd/yyyy]

I, \_\_\_\_\_ acknowledge receipt of a temporary building pass, pending completion of a background investigation.

**24.** \_\_\_\_\_

**25. Date:** [mm/dd/yyyy]

**Candidate signature**

**C. Card Approval (To be completed by registrar)**

**26. Based on:** ☐ *NACI*                      ☐ *Other*

**27. Date completed:** [mm/dd/yyyy]

**28. Favorable?** ☐ Yes ☐ No

**29. Clearances/Access:**

☐ General ☐ SEC ☐ SEC/L ☐ TS ☐ Q ☐ SCI ☐ SI ☐ TK ☐ G ☐ HCS ☐ NATO

**30. Registrar Information**

Name:

Office Code:

Phone No. (    )    -

*I hereby ☐ Approve ☐ Disapprove issuance of an Identification Card to the above-named Candidate.*

**31. Registrar Signature:**

**32. Date:** [mm/dd/yyyy]

**D. Card Details (To be completed by Issuer after Section C has been completed)**

33. Name on Card:

34. Date Issued: [mm/dd/yyyy]

35. Card Expiration Date: [mm/dd/yyyy]

36. Parking Permit #:

**37. Issuer Information**

Issuer Name:

Office Code:

Phone No.: (    )    -

*I acknowledge issuance of an Identification Card to the Candidate identified above based on verification of the Candidate's identity and the above Registrar's issuance approval.*

**38. Issuer Signature:**

**39. Date:** [mm/dd/yyyy]

**E. Candidate Acknowledgement (To be completed by Candidate after Section D is completed)**

*I, the Candidate, confirm receipt of the Identification card identified above, verify that the information is accurate to the best of my knowledge, and agree to abide by all rules and responsibilities associated with the card.*

**40. Candidate Signature:**

**41. Date:** [mm/dd/yyyy]

*Upon completion, return this form to the Registrar*

See the back of this form for the **Privacy Act Statement** and **Paperwork Reduction Act Public Burden Statement** that applies to the information you are providing.

### **Privacy Act Statement**

In compliance with the Privacy Act of 1974, the following information is provided: Solicitation of the information is authorized by 44.U.S.C. 2104. Disclosure of the information is voluntary. The information provided will be used to prepare and issue an identification card or pass. Additionally, the information may be provided to an expert, consultant, or contractor or NARA to assist NARA in the performance of its duties. If some or any of the information is not provided by the candidate, the effect will be that the identification card or pass may not be issued, resulting in the candidate being denied access to NARA facilities and IT systems.

### **Paperwork Reduction Act Public Burden Statement**

**May 9, 2008**

**NARA 275**

You are not required to provide the information requested on a form that is subject to the Paperwork Reduction Act unless the form displays a valid OMB control number. Public burden reporting for this collection of information is estimated to be 3 minutes per response. Send comments regarding the burden statement or any other aspect of the collection of information, including suggestions for reducing this burden to the National Archives and Records Administration (NHP), 8601 Adelphi Road, College Park, MD 20740-6001. DO NOT SEND COMPLETED FORMS TO THIS ADDRESS.

