NASA Procedural Requirements

NPR 1600.4A
Effective Date: April 08, 2016
Expiration Date: August 08, 2029

COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES

Printable Format (PDF)

Subject: Identity and Credential Management with Change 1, August 8, 2024

Responsible Office: Office of Protective Services

Chapter 3. Enrollment and Credential Issuance

3.1 Overview

3.1.1 The NASA Identity Management and Credential Management Processes are designed to conform to the system-based model for identity proofing, registration, and issuance process that is described in NIST FIPS 201-2.

3.1.2 The NASA Identity Management and Account Exchange (IdMAX) system shall be the sole and authoritative source for the enrollment and processing of NASA identity data, as recognized by the Office of Management and Budget (OMB), per the Paperwork Reduction Act (OMB control number 2700-0158), and for the processing of access requests and for the issuance of credentials.

3.2 Chain of Trust

3.2.1 A chain of trust is followed which simultaneously captures the biometrics, photograph, identity source documents, and background investigation of the applicant and can be tied to the identity of that applicant at any point in the identity management process.

3.2.2 The credential is released to the applicant only after completion of the chain of trust by verifying that the biometric information contained on the credential matches the applicant.

3.3 NASA Credential Types

3.3.1 NASA uses both PIV credentials and non-PIV credentials. Each NASA credential is linked to an established identity and shall go through the appropriate issuance steps as outlined in this chapter. See NPR 2841.1, for policy and procedures regarding NASA non-PIV credentials that allow access to only logical systems. Requirements for the characteristics of these credentials, including printing elements and technology capabilities are detailed in Chapter 5, Characteristics of NASA Badges.

3.3.2 NASA PIV Credentials

3.3.2.1 NASA PIV credentials shall be required for all persons who have been deemed as needing routine and regular physical only, logical only, and/or both physical and logical access to NASA Centers, facilities, and IT systems and resources for a period exceeding 179 calendar days in a 365-day period. These persons include all NASA employees, all NASA contractors, agreement partners, and non-NASA tenants in NASA facilities. NASA PIV credentials will be issued to both United States (U.S.) citizens and foreign nationals.

3.3.2.2 NASA PIV credentials will be issued following the identity proofing, registration, and issuance processes defined in this document for the management of identities of all new and current employees, contractors, and affiliates including foreign nationals.

3.3.2.3 NASA PIV credentials will be issued only after completion of a Federal Bureau of Investigation (FBI)

fingerprint check and submission of a background investigation, which will be a Tier I background investigation, at a minimum.

3.3.2.4 NASA PIV credentials will have an expiration date set for a period not to exceed five years from the Card Production Request (CPR) generation date.

3.3.2.5 NASA PIV credentials shall not be issued to individuals holding a Federal PIV credential issued by another Federal entity. Reserve military personnel who are full-time NASA employees or contractors are exempt from this restriction and may be issued a NASA PIV credential in addition to their DoD CAC. Exceptions to this policy may be made only when the exception has been documented and approved via the process described in section 1.3, Waivers and Exceptions, of this document. The exception request will specifically explain why a non-NASA credential is not usable in the NASA ICAM services.

3.3.3 NASA Non-PIV Credentials

3.3.3.1 All NASA non-PIV physical access credentials shall be created utilizing the Agency Enterprise Physical Access Control System (EPACS) and in compliance with NPR 2810.1.

3.3.3.2 NASA non-PIV temporary credentials will be issued to any person (e.g., NASA employee, NASA contract personnel, non-NASA tenant, or other category of individuals; such as volunteers, guest researchers, interns, grantees, etc.) who needs access to a NASA facility or NASA IT system and who will be affiliated with NASA and its Centers or facilities for a period of less than 180 calendar days (up to 179 calendar days) in a 365-day period. The 180-day period begins the first day of affiliation and ends 179 calendar days later regardless of the work schedule. If an individual's affiliation extends for 180 calendar days in a 365-day period from the first day of affiliation regardless of the work schedule, the individual will be issued a NASA PIV credential. The following categories of affiliates with no logical access may, at the discretion of the CCS/CCPS, be exempted from the requirement to receive a NASA PIV credential at the 180 calendar day point: seasonal student interns, volunteers, construction workers, and others as approved by the AIMO.

3.3.3.3 Issuance of NASA non-PIV badges requires a minimum favorable adjudication of a National Crime Information Center (NCIC) name query and completion of steps 1-4 of section 3.5, On-Site Enrollment and Issuance Procedures for NASA Credentials, of this NPR. Escort requirements for individuals with a NASA non-PIV badge will be based on risk-determination by the CCS/CCPS, in compliance with the requirements in this document.

3.3.3.4 NASA non-PIV visitor badges allow physical-only access to the issuing NASA Center. For visitors, Centers are authorized to issue alternate agency credentials (i.e., NASA non-PIV credentials) for physical access to that Center based on a risk-based determination documented as part of the permanent record. NASA visitor badges shall be issued to individuals requiring access to a NASA Center for a period less than 30 calendar days in any single visit and not more than a cumulative total of 29 calendar days in a 365-day period. Escort requirements for individuals with visitor badges will be based on risk-determination by the CCS/CCPS, in compliance with the requirements in this document.

3.3.3.5 NASA non-PIV alternate Agency credentials shall be issued to accommodate unique situations of the Center not otherwise accommodated by NASA PIV credentials and NASA visitor badges. All NASA alternate Agency credential templates will have the approval of the Agency Identity Management Official prior to their creation and utilization. NASA alternate Agency credentials will be issued upon completion of a favorable adjudication of an NCIC name query. This is a minimum requirement, and additional security measures may be employed at the discretion of the CCS/CCPS. Issuance of these credentials will be based on a risk-based access determination by the CCS/CCPS. NASA alternate Agency credentials may be issued to individuals who hold a PIV credential issued by another Federal Government agency or department if their current non-NASA PIV credential does not work at the NASA Center. This may include contractors from another NASA Center in the event that electronic verification of a requirement to access the NASA Center is not available at a point of entry. Issuance of alternate Agency credentials requires completion of steps 1-3 of section 3.5, On-Site Enrollment and Issuance Procedures for NASA Credentials, verification of a favorably adjudicated investigation, and capture of the individual's photograph.

3.3.4 Logical-only access credentials and their usage are addressed by NPR 2810.1 and include, but are not limited to, username and password, RSA tokens, and digital certificates.

3.4 Applicant Categories

3.4.1 NASA employees are Federal civil servants employed and paid by NASA and also includes individuals employed and paid by other entities but working for NASA under an Intergovernmental Personnel Act (IPA) agreement. NASA employees include all Non-Appropriated Funds Instrumentality (NAFI) employees; these employees shall be issued a civil servant badge with the affiliation of NAFI.

3.4.2 NASA contractor employees are individuals working for a contracting organization or entity with the responsibility to perform activities for NASA.

3.4.3 NASA grantees are individuals who are working under a grant or cooperative agreement and performing grant-funded activities at NASA Centers and facilities.

3.4.4 Detailees, for the purposes of this NPR, are either Federal employees from other-Federal agencies, U.S. military personnel, or non-Federal employees working at NASA through an IPA assignment. Any badges issued to a detailee shall be designated with an affiliation of NASA and will appear as a Federal employee badge. The Center PIF manager will coordinate with the Center HRO to validate investigative and suitability results for detailees from other-agency partners. Government employees from other departments and agencies who do not have a PIV credential issued by their agency or department and require identity verification and access at NASA may be issued a NASA PIV credential or NASA alternate Agency credential.

3.4.5 International partners are individuals working for agencies or organizations of foreign governments, foreign education institutions, foreign companies, or international organizations who are engaged in a program of international cooperation in work done pursuant to a Space Act Agreement, as defined by NPD 1050.1, Authority to Enter into Space Act Agreements. A signed international agreement shall first be in effect for international partners to receive a foreign national NASA PIV credential.

3.4.6 Tenants are individuals who require physical access to a NASA facility but may not work directly for NASA, including individuals requiring access under any property agreement (e.g., Enhanced Use Lease) with NASA. There may or may not be a "formal" agreement associated with a tenant (e.g., Credit Union). The tenant may require logical access to certain NASA applications. A tenant may work for another Government agency as either a civil servant or contractor and may have a PIV badge from their agency. Tenants shall be issued alternate Agency credentials. Tenants without a PIV badge from another Government agency may, at the discretion of the CCS/CCPS, be issued NASA PIV badges following the processes and requirements for a NASA PIV badge. Tenants with a PIV credential from another Government agency which cannot be registered in IdMAX may be issued alternate Agency credentials (non-PIV), at the discretion of the CCS/CCPS.

3.4.7 Transients are individuals (i.e., construction workers, club members, childcare drop off/pickup, delivery drivers, retirees, Center transits, and others requested by CCS/CCPS and approved by the AIMO) who requires intermittent access for 180 calendar days or more. Transients shall be issued alternate Agency credentials.

3.4.8 Interns are students from educational institutions participating in NASA internship/research programs and programs or projects which benefit and/or further the goals, objectives, and efforts of NASA.

3.5 On-Site Enrollment and Issuance Procedures for NASA Credentials

3.5.1 Step 1: Credential Request

3.5.1.1 A requester completes a credential request within the NASA Identity Management System for an applicant. The requester submits the request to the sponsor via the NASA Identity Management System. For civil servants, this information is submitted by the HRO via Workforce Transformation Tracking System (WTTS). The information submitted includes the following:

a. Name of the applicant.

b. Date of birth of the applicant.

c. Home address.

d. Social Security Number (SSN).

e. Position of the applicant.

f. Contact information for the applicant.

g. Name of the requester.

h. Organization of the requester.

i. Contact information for the requester.

3.5.2 Step 2: Sponsorship.

3.5.2.1 The sponsor validates the receipt of the request from the requester and reviews the data in the request. The sponsor reviews the Position Risk Determination in the NASA Identity Management System and approves or denies

the request, establishing the need for a relationship between the applicant and NASA and the applicant's need for a PIV credential.

3.5.3 Step 3: Check for Background Investigation or Database Checks.

3.5.3.1 The authorizer or investigation reviewer validates the receipt of the request from the sponsor. The authorizer and supporting staff review OPM and other Federal databases and take appropriate steps to validate the applicant's investigation status with regard to a current investigation.

3.5.3.2 If the applicant has an investigation on file or in progress that meets the investigative and reciprocity requirements, the authorizer submits the request to the enrollment official and the applicant proceeds to enrollment, section 3.5.4, Step 4: Enrollment Process for capture of enrollment data with flat fingerprints.

3.5.3.3 If no investigation is on file or in progress, the authorizer coordinates initiation of an invitation in the OPM e-QIP for the applicant to complete the appropriate background investigation form and authorizes the enrollment official to obtain the applicant's flat and rolled fingerprints, identity source documents, and photograph.

3.5.3.4 If the applicant is requesting a non-PIV alternate Agency credential then the authorizer or designee conducts the appropriate database checks and approves the credential if the database checks are favorable. The submission of the captured fingerprints to OPM is optional, as determined by the CCS/CCPS.

3.5.4 Step 4: Enrollment Process.

3.5.4.1 The enrollment official validates the receipt of the request from the authorizer. The sponsor advises the applicant that they will appear in person before the enrollment official and present two forms of identity source documents in original form. The applicant then appears in person before the authorized enrollment official and presents two forms of NASA-approved identity source documents in original form, one of which will be a Federal or state issued picture identification. The enrollment official inspects the source document for authenticity and validates the source document through visual or electronic scrutiny and, when necessary, with the authority or entity which issued it.

3.5.4.2 Enrollment Fingerprints — The applicant's fingerprints are captured. If the applicant currently has a favorable background investigation on file or in progress, only flat fingerprints are required. If no background investigation is on file or in progress, both flat and rolled fingerprints are required. In cases where there is difficulty in collecting fingerprints due to damage, injury, or deformity, NASA will process the credential with a designation of fingerprints as non-classifiable. The facial image collected from the applicant during enrollment can also be used for authenticating badge recipients covered under Section 508 of the Rehabilitation Act.

3.5.4.2.1 When fingerprints are captured at a location other than the Center Protective Services Office, the transmission of those fingerprints to the Center Protective Services Office shall be from a valid law enforcement agency or other accredited fingerprint provider. To ensure a chain of trust, the fingerprint cards will be delivered to the Center Protective Services Office by the entity that took the fingerprints.

3.5.4.3 Enrollment Photograph — The applicant's photograph is captured which will include the entire face, from natural hairline to the chin, and may not be obscured by dark glasses, hats, etc. The facial expression will be neutral (non-smiling) with a closed mouth. Eye patches that do not obscure an excessive portion of the face need not be removed. Individuals with temporary eye patches should be issued a temporary badge until such time when the patch is no longer necessary and an unobscured, full-facial photograph can be captured. Waivers for religious reasons may be obtained by written application to the AA for OPS.

3.5.4.4 NASA-Approved Identity Source Documents — The enrollment official obtains and maintains legible photocopies or scanned copies of the original identity source documents. Any documents that appear invalid (e.g., absence of security hologram or other known security features on a state issued driver's license, security features on a birth certificate or passport, smeared ink, etc.) are to be rejected by the enrollment official and reported to the proper authority for review. Photocopies of rejected documents are to be made and retained for a period not to exceed one year or until any appeal process is completed. Identity source documents that do not pass electronic examination are rejected and another approved identity source document will be obtained and subjected to electronic scrutiny. In the event the applicant is required to provide documentation to resolve discrepancies or omissions in data collected, the enrollment official shall review the information with the applicant as necessary. The information submitted by the applicant will be used to update the applicant identity record.

3.5.4.5 Enrollment Subscriber Agreement — For applicants requesting PIV credentials, the enrollment official shall provide the applicant with the Subscriber Agreement, (See Appendix D: Subscriber Agreement), and obtain an electronic signature of the applicant attesting to their reading and acceptance of the Subscriber Agreement.

3.5.5 Step 5: Adjudication Process.

3.5.5.1 If no investigation is on file or in progress, the fingerprints captured during enrollment will be submitted to OPM with a request for a background investigation. The authorizer receives the results of the fingerprint check. If the fingerprint check comes back with a status of unclassifiable, the Center will use the results of a name check to process the PIV credential request. The authorizer makes a determination based upon receipt of the fingerprint check results or evidence of an acceptable existing background investigation (as found in section 3.5.3, Step 3: Check for Background Investigation or Database Checks), if the applicant is eligible to receive a PIV credential. If the adjudication of the available background investigation is favorable, the authorizer will submit a PIV credential issuance request to authorize the creation and issuance of a PIV credential. Final adjudication of the record is performed in compliance with NASA personnel security policies.

3.5.6 Step 6: Badge Production Process.

3.5.6.1 The PIV authorizer submits a request for badge printing if the badge is to be printed remotely at a commercial facility or a shared service provider. The necessary information is included in a batch card creation request. The initialized and printed badges are returned to NASA and forwarded to the appropriate issuance officials where the credentials shall be held in a secure location. If the badge is to be produced locally, the issuance official will print the identity information onto the card and compare the photo to the identity database. The badge will be encoded with the identity and biometric data of the applicant. The encoded badge will be tested, and the applicant will be notified when the badge has been successfully encoded.

3.5.7 Step 7: Issuance Process.

3.5.7.1 The applicant appears before the issuance official, who establishes whether the badge was printed in a batch job, previously printed on-site, or is to be printed on-site. If the badge is printed in a batch job or previously printed on-site, the issuance official will obtain the card stock from storage. If the badge is to be printed on-site, the issuance official will obtain a blank badge from storage, verify the identity of the applicant against the database, and print the badge. The issuance official checks the printed badge to verify the identity of the applicant, conducts a biometric match, and encodes the badge with an applicant entered PIN number. Upon completion of the badge printing and encoding, the badge is officially released to the applicant. An approved electronically shielded badge holder will be offered to the applicant in order to protect the badge and the privacy of information on the badge.

3.5.7.2 For any badge issued without a biometric check, facial recognition shall be performed by comparing the photograph stored in IdMAX to the photograph on the badge and the face of the applicant. When the facial recognition is verified, the badge can be released to the applicant.

| TOC | ChangeLog | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | ALL |

| NODIS Library | Organization and Administration(1000s) | Search |

DISTRIBUTION:
NODIS