

ATTACHMENT J-15

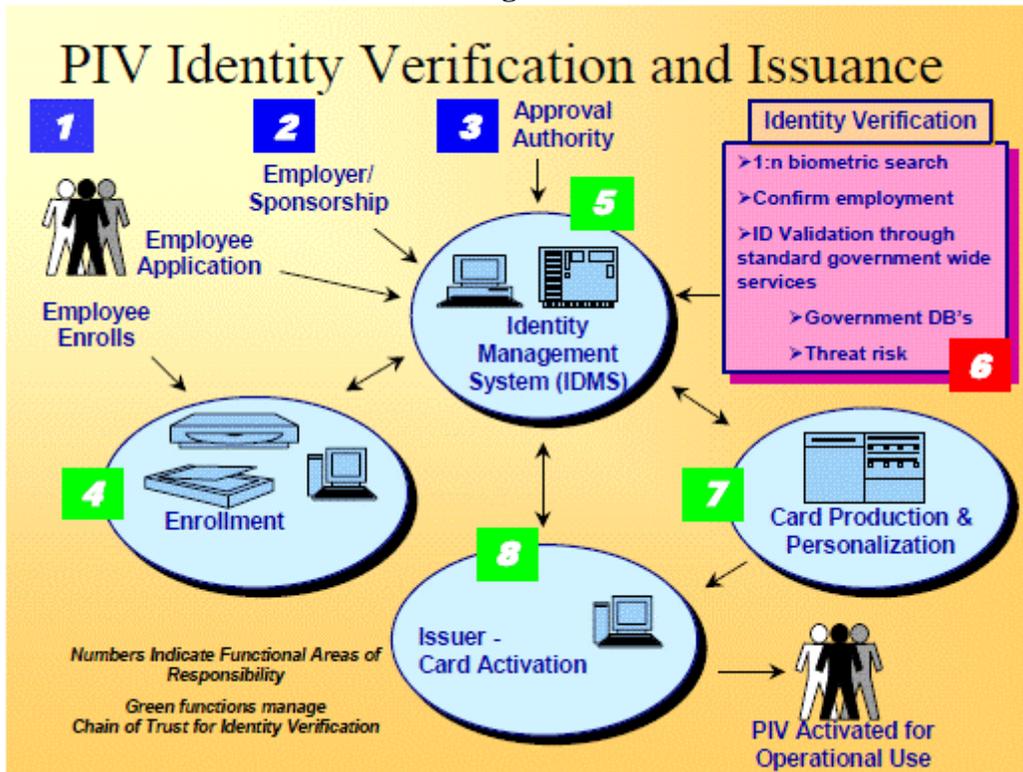
PERSONAL IDENTITY VERIFICATION (PIV) PROCEDURES

PIV Card Issuance Procedures (in accordance with FAR Clause 52.204-9, *Personal Identity Verification of Contractor Personnel*):

Overview

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 201-1 and is represented diagrammatically in that document via Figure J-15.1:

Figure J-15.1



Chain of Trust

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.

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.

NASA Credential Types

NASA uses both PIV credentials and non-PIV credentials. Access is granted via NASA PIV Credentials. NASA PIV Credentials allow physical only, logical only, and both physical and logical access to resources at NASA. Each NASA credential is linked to an established identity

ATTACHMENT J-15**PERSONAL IDENTITY VERIFICATION (PIV) PROCEDURES**

and shall go through the appropriate issuance steps as outlined in this chapter. See NPR 2810.1, Security of Information Technology for policy and procedures regarding NASA non-PIV credentials that allow access to only logical systems. NASA visitor badges are NASA non-PIV badges which allow only physical access to NASA Centers. For short-term visitors, Centers are authorized to issue Center-specific badges (i.e. NASA non-PIV badges) for physical access to that Center based on a risk-based determination documented as part of the permanent record.

NASA PIV credentials shall be issued to all persons who have been deemed as needing access to NASA Centers, Facilities, and IT systems and resources for a period exceeding 179 days in a 365-day period. These persons include all NASA employees, all NASA contractors, agreement partners, as well as non-NASA tenants in NASA facilities. NASA PIV credentials will be issued to both U.S. citizens and foreign nationals. NASA PIV credentials will be issued following the complete 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. 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 National Agency Check with inquiries (NACI) background investigation at a minimum. NASA PIV credentials will have an expiration date set for a period not to exceed 5 years from the Card Production Request (CPR) generation date. NASA PIV credentials will not be issued to individuals holding a federal PIV credential issued by another federal entity or to individuals holding a PIV-I credential issued by an organization whose PIV-I credentials conform to the federal PIV-I standard. Exceptions to this policy may be made only when the exception has been formally documented and approved. The exception request will specifically explain why a non-NASA credential is not usable in the NASA Identity Credential and Access Management (ICAM) services.

Any person (i.e., NASA employee, NASA contract personnel, non-NASA tenant, or other category of individuals such as volunteers, guest researchers, interns, grantees, etc.) who will be affiliated with NASA and its Centers or Facilities for a period of less than 180 days shall be issued a NASA non-PIV badge (i.e., a NASA temporary badge). The 180-day period begins the first day of affiliation and ends 180 calendar days later regardless of the work schedule. If an individual's affiliation extends for 180 days in a 365-day period, the individual will be issued a NASA PIV credential if the individual is a NASA employee (either a civil servant or a federal contractor employee). All other individuals (volunteers, construction workers, guest researchers, interns, grantees, etc.) determined to need intermittent access with no IT access may be exempted from the 180-day limit on use of a NASA non-PIV badge consistent with risk-based assessments by Center Chief of Security/Center Protective Services (CCS/CPS). Issuance of NASA non-PIV badges requires at minimum a favorable adjudication of a National Crime Information Center (NCIC) name query and completion of steps 1-4: On-Site Enrollment and Issuance Procedures. Escort requirements for individuals with a NASA non-PIV badge will be based on risk-determination by the CCS.

NASA visitor badges shall be issued to individuals requiring access to a NASA Center for a period less than 30 days in any single visit and not more than a cumulative total of 29 days in a

ATTACHMENT J-15**PERSONAL IDENTITY VERIFICATION (PIV) PROCEDURES**

365-day period. Individuals needing access for 30 days or more will be issued a NASA Non-PIV Temporary badge. Issuance of NASA visitor badges requires completion of below steps 1-3: Enrollment and Issuance, and will include capture of the visitor's photograph below Step 4: Enrollment Process. Visitors requiring access to a NASA Center for more than 5 days will undergo a minimum of a National Crime Information Center name query prior to receiving a visitor badge. Escort requirements for individuals with visitor badges will be based on risk-determination by the Center Chief of Security.

NASA Center-specific badges shall be issued to accommodate unique situations of the Center not otherwise accommodated by NASA PIV credentials, and NASA visitor badges. All NASA Center-specific badge templates will have the approval of the Agency Identity Management Official prior to their creation and utilization. NASA Center-specific badges will be issued upon completion of a favorable adjudication of a National Crime Information Center (NCIC) name query. This is a minimum requirement and additional security measures may be employed at the discretion of the CCS/CPS. Issuance of these badges will be based on a risk-based access determination by the Center Chief of Security. NASA Center-specific badges 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 need to be on the NASA Center is not available at a point of entry. Issuance of NASA Center-specific badges requires completion of below steps 1-3: On-Site Enrollment and Issuance Procedures, verification of a favorably adjudicated investigation, and capture of the individual's photograph, below Step 4: Enrollment Process.

Logical access credentials and their usage are addressed by NPR 2810.1, *Security of Information Technology*, and include but are not limited to username and password, RSA tokens, digital certificates.

Applicant Types

NASA employees are Federal civil servants employed and paid by NASA. NASA Employees also includes individuals employed and paid by another entity 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.

NASA contractors are individuals working under contract with the responsibility to perform activities for NASA. NASA grantees are individuals who are working under grant and performing activities for and/or at NASA Centers and Facilities. Detailees are either Federal employees from other-Federal Agencies, or U. S. military personnel, or non-Federal employees working at NASA through an Intergovernmental Personnel Act (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 Human Resources Office (HRO) to validate investigative and suitability results for detailees from other-agency partners. Government employees from other departments and agencies who do not have

ATTACHMENT J-15**PERSONAL IDENTITY VERIFICATION (PIV) PROCEDURES**

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 temporary badge by NASA.

International Partners are individuals, working for agencies or organizations of foreign governments, foreign education institutions, foreign companies, or international organizations, 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.

Tenants are individuals who require physical access to a NASA facility but do not work directly for NASA. There may or may not be a "Formal" agreement associated with a tenant (example: 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 this other agency. Tenants include those entities and their contractors and employees under Economy Act, Space Act, Commercial Space Competitiveness Act (CSCA) or Commercial Space Launch Act (CSLA) agreements are those individuals needing physical or logical access based on the above authorities. The tenant may work for a company that is leasing space on a NASA facility but does not work on a NASA-related project.

Transients are individuals (i.e., construction workers, club members, childcare drop off/pickup, delivery drivers, retirees, Center transits, and others approved by Center Chiefs of Protective Services/Security) who requires intermittent access for 180 days or more. Transients shall be issued Center-specific badge.

On-Site Enrollment and Issuance Procedures for NASA Credentials**Step 1:**

Credential Request - A requester completes a credential request within IdMAX for an applicant. The requester submits the request to the sponsor via IdMAX. The information submitted includes the following:

- a. Name of the applicant;
- b. Date of Birth of the applicant;
- c. Position of the applicant;
- d. Contact information for the applicant;
- e. Name of the requester;

ATTACHMENT J-15**PERSONAL IDENTITY VERIFICATION (PIV) PROCEDURES**

- f. Organization of the requester; and
- g. Contact information for the requester.

Step 2:

Sponsorship - The sponsor validates the receipt of the request from the requester. The sponsor reviews the data in the request. The sponsor reviews the Position Risk Determination. The sponsor 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

Step 3:

Check for Background Investigation or database checks - The authorizer or Investigation Reviewer validates the receipt of the request from the sponsor. The authorizer and supporting staff review the Office of Personnel Management (OPM) and other federal databases and take appropriate steps to validate the applicant's investigation status with regard to a current investigation.

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, Step 4: Enrollment Process, for capture of enrollment data with flat fingerprints.

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, I-9 documents, and photograph.

If the applicant is requesting a non-PIV badge then the authorizer or designee conducts the appropriate database check.

Step 4:

Enrollment Process - 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 appears in-person before the authorized Enrollment Official and presents two forms of identity source documents in original form per Form I-9, 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.

ATTACHMENT J-15**PERSONAL IDENTITY VERIFICATION (PIV) PROCEDURES**

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 to be captured. If no background investigation is on file or in progress, both flat and rolled fingerprints are required to be captured. In cases where there is difficulty in collecting fingerprints due to damage, injury or deformity, NASA shall perform authentication using asymmetric cryptography for authentication. 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.

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, coverings, etc. The facial expression shall 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 as the patch is no longer necessary and an un-obscured full-facial photograph can be captured. Waivers for religious reasons may be obtained by written application to the AA for Protective Services who may refer the matter for a recommendation to a NASA Headquarters Access Appeals Panel.

Enrollment I-9 Documentation - The Enrollment Official obtains and maintains a legible photocopy or scan copy of the original I-9 documentation. Any document that appears 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.) is 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. I-9 documents that do not pass electronic examination, if available, are rejected and another approved I-9 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.

Enrollment Subscriber Agreement - The Enrollment Official shall provide the applicant with the Subscriber Agreement and obtains an electronic signature of the applicant attesting to their reading and acceptance of the Subscriber Agreement.

Step 5:

Adjudication Process - If no investigation is on file or in progress, the fingerprints captured during enrollment shall 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 NCIC 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 in Step 3: Check for Background Investigation, if the applicant is eligible to receive a PIV credential. If the adjudication of the available background investigation is favorable, the authorizer submits a PIV

ATTACHMENT J-15**PERSONAL IDENTITY VERIFICATION (PIV) PROCEDURES**

credential issuance request to authorize the creation and issuance of a PIV credential. In instances where a badge is to be issued, the authorizer notifies the sponsor and requester that the badge issuance has been authorized. Final adjudication of the record is performed in compliance with NASA personnel security policies.

Step 6:

Badge Production Process - 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 prints the identity information onto the card and compares 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. The applicant will be notified when the badge has been successfully encoded.

Step 7:

Issuance Process - 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 printed in a batch job or previously printed on-site, the Issuance Official obtains the card stock from storage. If the badge is to be printed on-site, the Issuance Official obtains a blank badge from storage, verifies the identity of the applicant against the database, and prints 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 shall be offered to the applicant in order to protect the badge and the privacy of information on the badge.