



NASA Procedural Requirements

NPR 1600.4Effective Date: August 01,
2012Expiration Date: August 01,
2017**COMPLIANCE IS MANDATORY**[Printable Format \(PDF\)](#)

Request Notification of Change (NASA Only)

Subject: Identity and Credential Management

Responsible Office: Office of Protective Services[| TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) | [Chapter5](#) | [Chapter6](#) | [AppendixA](#)
| [AppendixB](#) | [AppendixC](#) | [AppendixD](#) | [ALL](#) |

Chapter 2. Roles and Responsibilities

2.1 Overview

All NASA employees and contractor employees, as well as NASA tenants and contractors for NASA tenants, shall comply with this directive. Commercial or private entities and their contractors (all tiers) and their employees needing physical or logical access per the Economy Act, Space Act, Commercial Space Competitiveness Act (CSCA), or Commercial Space Launch Act (CSLA) agreements will also comply with this directive. The AA for OPS is the system owner of all systems used to manage identities and to issue NASA PIV credentials. The AA for OPS has overall responsibility for ensuring uniformity of credential issuance policies and procedures throughout the Agency. All NASA organizational components must adhere to the policies and procedures herein and promulgate implementing regulations, as required, consistent with the policies and procedures set forth herein. Center Directors, through their Center OPS, supported by the Center Office of the Chief Information Officer (OCIO), Center Human Resources Office (HRO), Procurement Office, and other offices as necessary will ensure that local operating procedures and execution conform to the policies and procedures herein. The following roles and responsibilities are established to conform to the guidelines prescribed in NIST Special Publication 800-79-1 "Guidelines for the Accreditation of Personal Identity Verification Card Issuers."

2.2 Agency Roles and Responsibilities

2.2.1 Personal Identity Verification Card Issuer (PCI) Senior Authorizing Official (SAO) - The AA for OPS shall be the PCI SAO for Identity and Credential Management. The PCI SAO establishes budgets and provides oversight for the identity management and credential management functions and services of NASA. The PCI SAO documents all identity management and credential management responsibilities, roles, and procedures to be followed by NASA. The PCI SAO identifies and designates qualified individuals to the roles of PCI Designated Accreditation Authority (PCI DAA), PCI Assessor, PCI Agency Identity Management Official (AIMO), and other NASA officials that are involved with Agency identity management. The PCI SAO establishes appropriate attributes and assessment methods for a certification and accreditation, per NIST Special Publication (SP) 800-79-1, of the programs and procedures established in this document for the issuance of credentials. The PCI SAO ensures consistent application of this policy across NASA.

2.2.2 PCI AIMO - The PCI AIMO shall be a Federal employee. The PCI AIMO manages the identity management program at NASA and documents the policies and operations of the identity management program in this and other supporting documentation. The PCI AIMO ensures that all personnel, services, facilities, and/or equipment necessary to carry out the policies in this document are procured, updated, and provided reliably. The PCI AIMO ensures that credentials are produced and issued in accordance with the requirements in this document. The PCI AIMO approves all authorizer and investigation reviewer designations. The PCI AIMO recommends and executes an action plan to reduce or eliminate deficiencies and discrepancies identified by the assessor during the certification and accreditation (C&A).

2.2.3 PCI Designated Accreditation Authority (DAA) - The Deputy AA for OPS shall be the PCI DAA. The PCI DAA

reviews the certification documentation and the recommendation prepared by the PCI assessor and accredits the PCI as required by HSPD-12. Through accreditation, the DAA accepts responsibility for the operation of the PCI at an acceptable level of risk to NASA. The SAO can also fulfill the role of the DAA.

2.2.4 PCI Assessor - The PCI assessor shall be a Federal employee. The PCI assessor will be organizationally separate from the persons and the office(s) directly responsible for the day-to-day operation of identity management for the Agency and correction of deficiencies and discrepancies identified during the certification. The PCI assessor will have the appropriate skills, resources, and competencies to perform certifications of the Agency. The PCI assessor conducts the PIV C&A, per NIST SP 800-79-1.

2.2.5 NASA Enterprise Applications Competency Center (NEACC) - The NEACC provides hosting and management for core ICAM services. The NEACC provides help desk support for the systems implemented for identity management and credential management including trouble ticket management and procedures for handling escalation. The NEACC formally interfaces with appropriate service, security, support groups, and organizations as required. The NEACC provides access to technical and user training computer based training and maintains records related to this training.

2.3 Center Roles and Responsibilities

2.3.1 The Center PIV Issuing Facility (PIF) Manager - The Center PIF manager shall be a Federal civil service employee serving as the CCS, Chief of the Protective Services Office (PSO), or equivalent role designation at a Center or a designee of the Chief. The PIF manager supports the PCI AIMO at the Center level. The PIF manager oversees the identity management and credential management program implementation at the Center and documents the operations and procedures of the Center's identity management and credential management programs. The PIF manager or designee validates the individuals at the Center who perform the roles of PIV requester and PIV sponsor. The PIF manager or designee monitors training status of all persons fulfilling PIV identity management and credential management roles at the Center. The PIF manager identifies and designates individuals to fill the roles of PIV authorizer, PIV enrollment official, and PIV issuance official. The PIF manager is responsible for ensuring that all personnel, services, facilities, and/or equipment necessary to carry out the policies in this document at the Center are procured, updated, and provided reliably. The PIF manager is responsible for ensuring that credentials are produced and issued in accordance with the requirements in this document. The PIF manager or designee reviews I-9 document discrepancies and provides determinations for the acceptance of the documents. The PIF manager or designee is responsible for issuance of all non-PIV credentials (i.e., visitor badges, temporary badges, and non-PIV Center-specific badges).

2.3.2 PIV and non-PIV Applicant - Per FIPS 201-1, the PIV applicant is the individual to whom a PIV credential needs to be issued. The PIV applicant is a prospective or current NASA worker (e.g., a civil servant or an employee of a Federal contractor), requiring access to NASA facilities and/or IT resources. The PIV applicant is responsible for providing identification documents and data for the PIV request, for being photographed and providing biometrics during enrollment, and providing valid identity documents during enrollment, and issuance. The PIV applicant signs for acceptance of the PIV credential and acknowledgement of related responsibilities for proper handling and use of the PIV credential once issued, as defined in Appendix D: Subscriber Agreement. PIV applicants will not perform any role in the creation of their identity and issuance of their credential with the exception of the role of requester for the purpose of renewal and reissuance.

2.3.3 PIV and non-PIV Requestor - The role of PIV requestor is not defined in FIPS 201-1. The PIV requestor is the individual who submits the necessary information on behalf of the PIV applicant to initiate the process of requesting a PIV credential. The non-PIV requestor is the individual who submits the necessary information on behalf of the non-PIV applicant to initiate the process of requesting a non-PIV credential.

2.3.4 PIV and non-PIV Sponsor - The PIV sponsor is defined in FIPS 201-1 as the individual who substantiates the need for a PIV credential to be issued to the PIV applicant and provides sponsorship to the PIV applicant. The PIV sponsor requests the issuance of a PIV credential to the applicant. The PIV sponsor shall be a NASA civil servant employee or a California Technical Institute Jet Propulsion Laboratory employee who establishes and endorses the need for a relationship between the applicant and NASA. The PIV sponsor designates and approves the position risk determination (PRD) in the NASA Identity Management System. The PIV sponsor provides, as necessary, incorrect or missing information in the credential issuance request. The PIV sponsor is responsible for tracking the status of persons and reporting where access should be modified or terminated. The PIV sponsor is an individual from the identified entity for the following applicant affiliation:

- a. HR specialist for NASA civil service employees;
- b. Contracting Officer's Technical Representatives (COTR) or other Federal civil service technical personnel responsible for work requirements for contractors;
- c. Grants technical official for grantees;
- d. Authorizing official or designee for Economy Act, Space Act, CSLA or CSCA agreements, or

e. The NASA civil servant program or project manager who requires the foreign national to access NASA facilities or IT systems.

2.3.5 PIV and non-PIV Enrollment Official - The PIV enrollment official covers a portion of the duties that are described in FIPS 201-1 for the PIV registrar. The PIV enrollment official is the entity responsible for identity proofing of the PIV applicant and ensuring the successful collection of the information necessary to confirm employer sponsorship, bind the applicant to their biometric, and validate the identity source documentation. The role of the PIV enrollment official shall be performed by personnel from the Center security office. The PIV enrollment official collects, establishes, and verifies identity information of an applicant. The PIV enrollment official captures the biometrics and photograph of the applicant. The PIV enrollment official checks USCIS Form I-9 identity source documents for authenticity, captures copies and/or scans of the USCIS Form I-9 documents, compares the name and demographic data in the PIV credential request and the USCIS Form I-9 documents, and determines whether any discrepancies exist on an applicant's USCIS Form I-9. The non-PIV enrollment official performs the equivalent functions for non-PIV credentials as the PIV enrollment official does for PIV credentials.

2.3.6 PIV and non-PIV Authorizer - The PIV authorizer covers the portions of the PIV approval duties described in FIPS 201-1 that are not done by the PIV enrollment official. The PIV authorizer provides the final approval for the issuance of the PIV credential to the applicant. The PIV authorizer and the non-PIV authorizer shall be a NASA civil servant. The PIV authorizer and the non-PIV authorizer will hold no other role in the identity management or credential issuance process for a given identity. The PIV authorizer will hold no role other than the role of applicant in the issuance of their credential. The PIV authorizer and the non-PIV authorizer will be trained in adjudication by an accredited provider of adjudication training. The PIV authorizer reviews the PIV credential request, reviews the PIV sponsor's endorsement, and confirms that USCIS Form I-9 validation and biometrics capture has occurred. The PIV authorizer coordinates checks for existing background investigations. The PIV authorizer coordinates requests for background investigations as necessary. The PIV authorizer coordinates background investigation submissions through the OPM Electronic Questionnaire for Investigation Processing (e-QIP), as required. The PIV authorizer adjudicates the results of the fingerprint check and adjudicates background investigation results. The PIV authorizer records the results of the fingerprint check and background investigation results and approves or denies NASA PIV credential issuance. The PIV authorizer records the final result of adjudicated investigations, and when the adjudicated investigations are favorable, authorizes continued use of an issued PIV credential as required in NM 1600-96 NASA Personnel Security.

2.3.7 PIV and non-PIV Investigation Reviewer - The PIV investigation reviewer is an optional role within NASA that is not described in FIPS 201-1. The PIV investigation reviewer may be a civil servant or a designated contractor. The PIV investigation reviewer shall not be allowed to authorize production or issuance of a NASA PIV credential. The PIV investigation reviewer assists the PIV authorizer with:

- a. Reviewing the PIV credential request, the PIV sponsor's endorsement, and confirming that USCIS Form I-9 document validation occurred and that biometrics capture has occurred;
- b. Coordinating checks for existing background investigation;
- c. Coordinating requests for background investigations as necessary;
- d. Coordinating background investigation submissions through the OPM e-QIP, as required;
- e. Reviewing the results of the fingerprint checks and background investigation as they are received;
- f. Recording results of the fingerprint check; and
- g. Updating PIV applicant information when necessary.

2.3.8 PIV and non-PIV Issuance Official - The PIV issuance official is defined in FIPS 201-1 as the PIV issuer. The PIV issuer is the entity that performs credential personalization operations and issues the identity credential to the applicant after all identity proofing, background checks, and related approvals have been completed. The PIV issuance official is also responsible for maintaining records and controls for PIV credential stock to ensure that stock is only used to issue valid credentials. The role of the PIV issuance official shall be performed by personnel authorized by the CCS. The PIV issuance official issues NASA PIV credentials to approved PIV applicants. The PIV issuance official is responsible for submitting the order for the PIV credential to be encoded and printed with the appropriate identity information. The PIV issuance official verifies the applicant's identity through visual and biometric verification prior to issuing the NASA PIV credential. The PIV issuance official ensures the applicant has selected a Personal Identification Number (PIN). The PIV issuance official secures, receives, accounts for, and handles un-issued NASA PIV credential stock and NASA PIV credentials that are no longer authorized for use due to termination of employment, badge expiration, contract or grant expiration, or expiration of need for the badge by a foreign national.

2.3.9 PIV Digital Signatory - The PIV digital signatory is the entity that digitally signs the PIV biometrics and Cardholder Unique Identifier (CHUID) as defined in FIPS 201-1.

2.3.10 PIV Authentication Certification Authority (CA) - The PIV Authentication CA is the entity that signs and issues

the PIV Authentication Certificate.

2.4 Separation of Duties for the PIV Role

2.4.1 Per the requirements specified in FIPS 201-1, the principle of separation of duties shall be enforced to ensure that no single individual has the capability to issue a PIV credential without the participation of at least one other authorized person.

2.4.2 Individuals and entities assigned to the PIV enrollment official, PIV authorizer, PIV investigation reviewer, PIV issuance official, and the PIV digital signatory roles shall complete training that is specific to their duties prior to being allowed to perform in their function.

2.5 Training

2.5.1 Overview training is required for each role identified in this document to ensure a general and uniform understanding of the NASA policies and procedures for identity management. Training is required for each of the following roles in the PIV issuance process: PIV enrollment officer, PIV authorizer, PIV investigation reviewer, and PIV issuance official. Recertification is required each year to ensure training is up-to-date and conducted with the most recent system updates. Failure to complete annual recertification will result in the individual's role being revoked. Training records are maintained by the SATERN computer-based training system or subsequent/succeeding system(s).

2.6 Privacy

2.6.1 NASA shall ensure that applicant information and systems which facilitate identity management processes are managed consistent with:

- a. NPD 1382.17, NASA Privacy Policy;
- b. NPR 1382.1, NASA Privacy Procedural Requirements;
- c. Homeland Security Presidential Directive 12 (HSPD-12);
- d. OMB Memorandum 05-24;
- e. Privacy Act of 1974, U.S. Public Law 93-579; and
- f. E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch. 36);

2.6.2 As prescribed in NPR 1382, NASA shall conduct and maintain a Privacy Impact Assessment (PIA) of the identity management program. NASA will conduct and maintain PIAs for all systems which are used in the identity management processes and include Personally Identifiable Information (PII) and Information in Identifiable Form (IIF) of the applicant. The NASA System of Records Notice (SORN) will be updated and maintained to reflect the disclosure of information to other Federal agencies.

2.6.3 Only individuals with a legitimate need to access the systems in which an applicant's IIF is stored and maintained shall be allowed to access those systems. It is the responsibility of each Center PIF manager to ensure that the access restrictions defined in the PIA are enforced. NASA will ensure privacy of applicant information is sustained through all steps of identity management including enrollment and issuance. PIV credential issuance facilities will provide an electromagnetically opaque sleeve that assists in protecting against unauthorized contactless access to information stored in the PIV credential.

2.6.4 The Privacy Act Statement shall be posted in every enrollment and issuance location on the applicable NASA Web site and provided in pre-enrollment packages to the applicant. The Privacy Act statement covers:

- a. Use of collected PII;
- b. Protections provided to ensure the security of PII; and
- c. Effects of partial disclosure and non-disclosure of information by the applicant.

2.6.5 The Subscriber Agreement (see Appendix D) shall be posted in every enrollment and issuance location on the applicable NASA Web site and provided in any pre-enrollment packages to the applicant. The Subscriber Agreement covers:

- a. Authorized uses of the PIV credential;
- b. Authorized uses of the PKI certificates and services provided with the PIV credential;
- c. Notification requirements for the applicant; and

d. Requirements to return the PIV credential at the end of use.

2.6.6 The following documentation shall be made available, at the request of the applicant:

- a. Complaint procedures;
- b. Appeals procedures as described in NM 1600-96 NASA Personnel Security for those denied a PIV credential or whose PIV credential is revoked; and
- c. Consequences for employees violating NASA privacy policies as described in NPR 1382.1.

2.6.7 All notifications provided during identity management processes shall be conducted in a secure manner, ensuring applicant information is secure at all times. Centers will establish procedures for notifying applicants when their PII is lost, damaged, becomes corrupt, or stolen.

2.6.8 Any individuals violating the privacy requirements established in this chapter may be disciplined and/or banned from physical or logical access in compliance with NASA guidelines established in NPR 1382.1.

2.6.9 NASA shall archive and safeguard all stored data pursuant to NPD 1440.6, NASA Records Management, and NPR 1441.1, NASA Records Retention Schedules. Identity files are maintained for a minimum of two years after an individual's relationship with the Agency has ended. NASA may, at its discretion, increase but not reduce the time that identity source documents are to be maintained. The data to be maintained in electronic or hard copy includes:

- a. Completed and signed PIV credential request;
- b. Information related to the applicant's identity source documents;
- c. Results of the applicant's background check;
- d. Copies of the applicant's photograph; and
- e. Any additional documents used in the enrollment and issuance process.

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) | [Chapter5](#) | [Chapter6](#) |
[AppendixA](#) | [AppendixB](#) | [AppendixC](#) | [AppendixD](#) | [ALL](#) |

| [NODIS Library](#) | [Organization and Administration\(1000s\)](#) | [Search](#) |

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.
Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>
