 **NASA NPR 1600.4B**

**Procedural**Effective Date: August 3, 2025

**Requirements** Expiration Date: August 3, 2030

**Subject: Identity and Credential Management**

**Responsible Office: Office of Protective Services**

**Table of Contents**

[Preface](#_Toc198296205)

[P.1 Purpose](#_Toc198296206)

[P.2 Applicability](#_Toc198296207)

[P.3 Authority](#_Toc198296208)

[P.4 Applicable Documents and Forms](#_Toc198296209)

[P.5 Measurement/Verification](#_Toc198296210)

[P.6 Cancellation](#_Toc198296211)

[Chapter 1. Introduction](#_Toc198296212)

[1.1 Overview](#_Toc198296213)

[1.2 Scope](#_Toc198296214)

[1.3 Waivers and Exceptions](#_Toc198296215)

[Chapter 2. Roles and Responsibilities](#_Toc198296216)

[2.1 Overview](#_Toc198296217)

[2.2 Agency Roles and Responsibilities](#_Toc198296218)

[2.3 Credential Issuance Roles and Responsibilities](#_Toc198296219)

[2.4 Separation of Duties](#_Toc198296220)

[2.5 Training](#_Toc198296221)

[2.6 Privacy](#_Toc198296222)

[2.7 Events and Tours](#_Toc198296223)

[Chapter 3. Enrollment and Credential Issuance](#_Toc198296224)

[3.1 Overview](#_Toc198296225)

[3.2 Applicant Categories](#_Toc198296226)

[3.3 Enrollment and Issuance Procedures](#_Toc198296227)

[3.4 Visitor Enrollment and Issuance Procedures](#_Toc198296228)

[3.5 Remote Enrollment Procedures](#_Toc198296229)

[3.6 Remote Issuance Procedures](#_Toc198296230)

[3.7 Identity Proofing and Vetting Requirements](#_Toc198296231)

[3.8 Trusted Partnerships and Federation](#_Toc198296232)

[Chapter 4. Foreign Nationals](#_Toc198296233)

[4.1 Overview](#_Toc198296234)

[4.2 NASA Foreign National Access Policy and Related Requirements](#_Toc198296235)

[4.3 Enrollment and Issuance Procedures for Foreign Nationals](#_Toc198296236)

[4.4 Enrollment and Issuance Procedures for Foreign National Visitors](#_Toc198296237)

[4.5 Remote Enrollment and Issuance Procedures for Foreign Nationals](#_Toc198296238)

[4.6 Implementation](#_Toc198296239)

[4.7 Identity Proofing and Vetting Requirements for Foreign Nationals](#_Toc198296240)

[4.8 Foreign National Escort Requirements](#_Toc198296241)

[4.9 Requirements for Visas](#_Toc198296242)

[4.10 Requirements Based on Affiliation](#_Toc198296243)

[4.11 Requirements Based on Visitor Attributes](#_Toc198296244)

[4.12 Requirements Based on Credential Type](#_Toc198296245)

[4.13 Access Control Plans, Technology Transfer Control Plans, and Access Provisioning](#_Toc198296246)

[4.14 Onsite, Offsite, and Virtual Meetings](#_Toc198296247)

[4.15 Visiting Center Request](#_Toc198296248)

[4.16 Annual Review](#_Toc198296249)

[4.17 Requirements for Logical Access](#_Toc198296250)

[Chapter 5. NASA Credentials](#_Toc198296251)

[5.1 Types of NASA Credentials](#_Toc198296252)

[5.2 NASA PIV Smartcard](#_Toc198296253)

[5.3 Agency Smart Badge](#_Toc198296254)

[5.4 Center-Specific Badges](#_Toc198296255)

[5.5 Visitor Passes](#_Toc198296256)

[5.6 Derived PIV Credentials](#_Toc198296257)

[5.7 Additional Characteristics](#_Toc198296258)

[5.8 Digital Characteristics](#_Toc198296259)

[5.9 The Uniform Universal Personal Identification Code (UUPIC)](#_Toc198296260)

[Chapter 6. Credential Lifecycle Management](#_Toc198296261)

[6.1 General Credential Management](#_Toc198296262)

[6.2 Credential Inventory, Storage and Handling](#_Toc198296263)

[6.3 Credentialing Determinations](#_Toc198296264)

[6.4 Credential Usage: Display, Protection, and Proper Usage](#_Toc198296265)

[6.5 Credential Renewal](#_Toc198296266)

[6.6 Credential Re-issuance](#_Toc198296267)

[6.7 Credential PIN Reset](#_Toc198296268)

[6.8 Credential Revocation](#_Toc198296269)

[6.9 Lost and Stolen Credentials](#_Toc198296270)

[6.10 Forgotten Credentials](#_Toc198296271)

[6.11 Credential Suspension](#_Toc198296272)

[6.12 Credential Return](#_Toc198296273)

[6.13 Credential Termination](#_Toc198296274)

[6.14 Credential Destruction](#_Toc198296275)

[Appendix A: Definitions](#_Toc198296276)

[Appendix B: Acronyms](#_Toc198296277)

[Appendix C: References](#_Toc198296278)

Preface

P.1 Purpose

1. This National Aeronautics and Space Administration (NASA) directive establishes Agency-wide identity, credential, and access management policy and establishes high-level implementation requirements as set forth in NASA Policy Directive (NPD) 1600.2, NASA Security Policy. Identity, credential, and access management are the activities that deal with identifying individuals and controlling their access to resources (e.g., facilities and information technology (IT) systems) by associating user rights and restrictions with the established identity.
2. This NASA directive prescribes personnel responsibilities and procedural requirements for the creation, usage, and management of identities and the creation and issuance of identity credentials to assist NASA Centers and Component Facilities in executing the NASA security program to protect people, property, and information.

P.2 Applicability

1. This NASA directive applies to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers.
2. This directive is applicable to the Jet Propulsion Laboratory (JPL), a Federally Funded Research and Development Center (FFRDC), only to the extent specified in the NASA/Caltech Prime Contract.
3. This directive is applicable to other contractors, recipients of grants or cooperative agreements, or parties to other agreements only to the extent specified in contracts, grants or cooperative agreement, or other agreements.
4. This directive is applicable to all other personnel completing work through Space Act Agreements (SAA), Memorandums of Agreement/Understanding, or other applicable agreements, those assigned or detailed under the Intergovernmental Personnel Act, partners, tenants, and visitors.
5. In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms "may" denotes a discretionary privilege or permission, "can" denotes statements of possibility or capability, "should" denotes a good practice and is recommended, but not required, "will" denotes expected outcome, and "are/is" denotes descriptive material.
6. In this directive, all document citations are assumed to be the latest version unless otherwise noted.
7. This directive is applicable to NASA directives developed or revised after the effective date of this NASA Procedural Requirements (NPR).

P.3 Authority

National and Commercial Space Programs, 51 United States Code (U.S.C.) § 20132, Public Law (Pub.L.) 111-314, 124 Stat. 3328 (2010).

P.4 Applicable Documents and Forms

1. Children’s Online Privacy Protection Rule, 15 U.S.C. §§ 6501-6505
2. E-Government Act of 2002, 44 U.S.C. § 101.
3. Privacy Act of 1974, 5 U.S.C. § 552a.
4. Rehabilitation Act of 1973, 29 U.S.C. § 701.
5. Paperwork Reduction Act of 1980, 44 U.S.C. §§ 3501-3521.
6. Exchange Visitor Program, 22 CFR pt. 62.
7. Office of Management and Budget (OMB) Memo M-05-24, August 5, 2005, “Implementation of Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standards for Federal Employees and Contractors.”
8. NASA Procedural Directive (NPD) 1050.7, Authority to Enter into Partnership Agreements.
9. NPD 1382.17, NASA Privacy Policy.
10. NPD 1440.6, NASA Records Management.
11. NPD 1600.2, NASA Security Policy.
12. NPR 1382.1, NASA Privacy Procedural Requirements.
13. NPR 1441.1, NASA Records Management Program Requirements.
14. NPR 1600.1, NASA Security Program Procedural Requirement.
15. NPR 1600.3, Personnel Security.
16. NPR 1620.3, Physical Security Requirements for NASA Facilities and Property
17. NPR 1660.1, NASA Counterintelligence and Counterterrorism.
18. NPR 2190.1, NASA Export Control Program.
19. NPR 2200.2, Requirements for Documentation, Approval, and Dissemination of NASA Scientific and Technical Information.
20. NPR 2810.1, Security of Information and Information Systems.
21. NPR 2841.1, Identity, Credential, and Access Management Services.
22. NPR 8715.2, NASA Emergency Management Program Procedural Requirements.
23. NASA Advisory Implementing Instruction (NAII) 1600.4, Foreign National Access Management (FNAM) Operations Manual.
24. NAII 2190.1, NASA Export Control program Operations Manual.
25. NASA Identity Management and Account Exchange (IdMAX) System.
26. Department of Homeland Security, United States Customs and Border Protection, Form I-94, Arrival/Departure Record.
27. Federal Information Processing Standards Publication (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors.
28. FIPS 140, Security Requirements for Cryptographic Modules.
29. Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, April 27, 2004.
30. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-79, Guidelines for the Certification and Accreditation of Personal Identity Verification Card Issuers.

P.5 Measurement/Verification

To determine compliance with this NASA directive, the Office of Protective Services (OPS) will conduct program reviews and assessments to determine compliance with the procedural requirements of this NPR. Reviews and assessments will occur in such a timeframe to ensure all card issuance locations are reviewed and assessed every 6 years.

P.6 Cancellation

1. NPR 1600.4A, Identity and Credential Management, dated April 8, 2016.
2. Memorandum for Center Directors, dated August 18, 2017, “Agency Smart Badge”.
3. Memorandum for Center Directors, dated October 4, 2017, “Foreign National Personal Identity Verification (PIV) Credential Expiration and Escort Requirements for Foreign Nationals from Designated Countries with a PIV Credential”.
4. Memorandum for Center Directors, dated December 12, 2019, “Requirements for Investigations and Credentials”.
5. Memorandum for Office of Education and Office of International and Interagency Relations, dated March 27, 2017, “Response to Proposed Policy for Foreign National Students and Interns”
6. Memorandum for Center Chiefs of Protective Services, dated January 22, 2021, “Procedures for Appealing Foreign National Escort Requirements at NASA Facilities”.
7. Memorandum for Center Chiefs of Protective Services, dated May 24, 2022, “Update to the Requirements for Investigations and Credentials”.
8. Memorandum for Center Chiefs of Protective Services, dated November 29, 2022, “Clarification of Interim Agency Smart Badge Issuance for all NASA Badging Offices”.
9. Memorandum for Center Chiefs of Protective Services, dated March 15, 2024, “Personal Identity Verification Issuance Clarification”.

# Introduction

## Overview

* + 1. This NASA directive establishes the policies and high-level procedures that will be used throughout NASA to achieve consistency in Identity, Credential, and Access Management (ICAM). Strong ICAM business processes and practices which adhere to Federal requirements and guidance support a secure environment where trusted individuals are granted appropriate access to approved assets in order to conduct business.
    2. ICAM business processes include all the processes necessary to support proofing and vetting the identity of all individuals requiring access (physical, logical, or both) to NASA assets. ICAM business processes also include issuing credential and granting access based on favorable identity proofing and vetting. The governance structure that has been established for ICAM business processes is documented in NPR 2841.1, Identity, Credential, and Access Management Services.

## Scope

* + 1. The policies and procedures identified within this document define the approved processes for NASA to manage personal identities and their associated enrollment records, and the issuance of NASA Personal Identity Verification (PIV) credentials. This NPR also establishes the policy for the management of Agency Smart Badges (ASB), Center-specific badges, and visitor passes. Logical access tokens are not covered in this document. Use of vetted and bound identities for physical access is covered by NPR 1600.1 and NPR 1620.3, and logical access is covered by NPR 2810.1, Security of Information and Information Systems. The policies and procedures for granting remote only IT access to foreign nationals are described in this NPR. The policies and procedures necessary to properly manage ICAM services as an integrated end-to-end service to improve security, efficiency, and inter-Center collaboration are covered in NPR 2841.1.
    2. This policy covers the creation, issuance, and use of NASA PIV Smartcards, Agency Smart Badges, Center-specific badges, and visitor passes; collectively referred to as credentials. Credentials derived from the NASA PIV Smartcard or Agency Smart Badge are covered by this NPR. Other logical credentials or access tokens not bound to the enrollment record and or derived from a smartcard certificate are covered in NPR 2841.1.

## Waivers and Exceptions

* + 1. Situations may arise for which a deviation from specific requirements established by this NPR is required. Waiver/exception requests may be submitted for a deviation from the specific requirements for that specific situation and timeframe.
    2. Approval authority for all waivers/exceptions to this NPR resides with the Assistant Administrator (AA), Office of Protective Services (OPS) who may delegate this authority as necessary.
    3. Blanket waivers/exceptions to NPR requirements shall not be issued.
    4. Waiver/exception requests shall be processed in accordance with the requirements of NPR 1600.1, section 1.4, Exceptions and Waivers.

# Roles and Responsibilities

## Overview

* + 1. All NASA civil service employees and contractor employees (collective referred to as NASA employees), as well as NASA tenants and contractors for NASA tenants, shall comply with this directive. Government, commercial, educational, or private entities and their employees and contractors (all tiers) needing access to NASA assets will also comply with this directive.
    2. The Agency Identity Management Official (AIMO) is the authorizing official or data owner of all systems used to manage identities and to issue NASA credentials that allow physical and/or logical access. The AA, OPS has overall responsibility for ensuring uniformity of credential issuance policies and procedures throughout the Agency.
    3. All NASA organizational components shall adhere to the policies and procedures herein and promulgate implementing regulations, as required, consistent with the policies and procedures set forth herein. Center OPS, supported by the Center Director, Center Office of the Chief Information Officer (OCIO), Center Human Capital Office (HCO), Procurement Office, and other offices as necessary will ensure that local operating procedures and execution conform to the policies and procedures herein.
    4. The roles and responsibilities and procedures and requirements set forth in this policy conform to the guidelines prescribed in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-79, “Guidelines for the Accreditation of Personal Identity Verification Card Issuers.”
    5. Failure to comply with the policies and procedures set forth in this NPR and NPR 2841.1 shall be treated as a violation of security requirements, per NPR 1600.1, section 2.3, and will be reported as a security incident to the Center Chief of Protective Services (CCPS) and the AIMO.

## Agency Roles and Responsibilities

* + 1. The Assistant Administrator (AA), Office of Protective Services (OPS) shall:

1. Serve as the Senior Agency Official (SAO), also known as the Senior Authorizing Official, for identity, credential, and access management at NASA.
2. Establish budgets, provide oversight, develop policy, and have authority over all NASA identity management and credential management functions and services.
3. Document all identity management and credential management responsibilities, roles, and procedures to be followed by NASA.
4. Identifies and designates qualified individuals to the roles of Designated Authorizing Official (DAO), Assessor, AIMO, and other NASA officials that are involved with Agency identity, credential, and access management.
5. Ensures consistent application of this policy across NASA.
   * 1. The Deputy AA, OPS shall:
6. Serve as the Designated Authorizing Official (DAO) for identity, credential, and access management at NASA.
7. Review all assessments of the PIV Card Issuer (PCI) and PIV Issuing Facilities (PIF).
8. Authorize the PCI as required by Homeland Security Presidential Directive 12 (HSPD-12).
9. Accept responsibility for the operation of the PCI at an acceptable level of risk to NASA.
10. Not assume the role of AIMO.
    * 1. The Agency Identity Management Official (AIMO) shall:
11. Be a Federal employee.
12. Manage the identity, credential, and access management program at NASA.
13. Document the policies and operations of the identity, credential, and access management program in this and other supporting documentation, including the PCI Operations Plan.
14. Implement the policies and operations of the identity, credential, and access management program.
15. Provides guidance and assistance to PIF personnel and coordinate activities with PIF Managers.
16. Approve and designate, as appropriate, capable, trustworthy, knowledgeable, and trained personnel to fulfill Agency and Center roles in the identity, credential, and access management process.
17. Ensure all services, facilities, and/or equipment necessary to carry out the policies in this document are procured, updated, reliable, and meet the requirements of Federal Information Processing Standards (FIPS) 201.
18. Ensure that credentials are produced and issued in accordance with the requirements in this document.
19. Support the authorization process.
20. Recommend and execute an action plan to reduce or eliminate deficiencies and discrepancies identified by the assessor during the assessment and authorization.
    * 1. The Assessor shall:
21. Be a Federal employee who is organizationally separate from the persons and the office(s) directly responsible for the day-to-day operation of identity, credential, and access management for NASA and correction of deficiencies and discrepancies identified during the assessment and authorization.
22. Not perform any other role (i.e., SAO, DAO, or AIMO) in the assessment process.
23. Have the appropriate skills, resources, and competencies to perform an assessment of NASA’s PIV processes to verify compliance with the control objectives of FIPS 201.
24. Assess the NASA PCI, per NIST SP 800-79.
25. Provide recommendations for reducing or eliminating deficiencies and security weaknesses, describing the potential impact of those deficiencies if not corrected.
    * 1. The Chief Privacy Officer or designee shall:
26. Serve as the Privacy Official for identity, credential, and access management at NASA.
27. Issue policy guidelines with respect to collection and handling of personally identifiable information from applicants to ensure the issuer is compliant with all relevant directives of privacy laws.
28. Oversee privacy-related matters in the ICAM system and be responsible for implementing all privacy requirements.
29. Not perform any other operational role within the issuer organization with the exception of the roles of applicant for issuance of a credential or requester for the purpose of renewal and reissuance.
    * 1. The NASA OCIO shall:
30. Provide knowledge to the Enterprise Service Desk which provides trouble help desk support and ticket management and procedures for handling escalation.
31. Formally interface with appropriate service, security, and support groups and organizations as required.
32. Provide technical and user training materials as well as computer-based training modules through the NASA System for Administration, Training, and Educational Resources for NASA (SATERN).
33. Provides hosting of core ICAM infrastructure.

## Credential Issuance Roles and Responsibilities

* + 1. The PIV Issuing Facility (PIF) Manager shall:

1. Be a Federal civil service employee within the OPS organization serving as the CCPS or a designee of the CCPS.
2. Support the AIMO at the Center level.
3. Implement the requirements and guidance provided by the AIMO.
4. Oversee the identity management and credential management program implementation at the Center.
5. Document the operations and procedures of the Center’s identity management and credential management programs.
6. Validate the individuals at the Center who perform the roles of identity requester and affiliation sponsor.
7. Identify and recommend/designate capable, trustworthy, knowledgeable, and trained personnel to fulfill Center roles in the identity, credential, and access management process.
8. Ensure 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 and timely.
9. Ensure that credentials are produced and issued in accordance with the requirements in this document.
10. Review identity source document discrepancies and provide determinations for the acceptance of the documents.
11. Manage the issuance of Agency credentials (i.e., PIV, ASB, Center-specific badges, visitor passes).
12. Support the authorization process.
13. Recommend and execute an action plan to reduce or eliminate deficiencies and discrepancies identified by the assessor during the assessment and authorization for the Center.
14. Enforce the access restrictions defined in the Privacy Impact Assessment (PIA).
    * 1. The Applicant shall:
15. Be a prospective or current NASA worker or non-NASA worker requiring access to NASA facilities and/or IT resources and to whom a credential needs to be issued.
16. Provide all necessary identity source documentation and personal and biometric data required to process a credential request.
17. Sign for acceptance and acknowledgement of the NASA Public Key Infrastructure (PKI) Subscriber Agreement (henceforth referred to as the Subscriber Agreement), located in the Identity Management and Account Exchange (IdMAX) system.
18. Not perform any other role in the creation of their identity and issuance of their credential with the exception of the role of requester.
    * 1. The Requester shall:
19. Hold a valid credential that enables access to IdMAX to perform the functions of Requester.
20. Submit all necessary information on behalf of the applicant to initiate the process of requesting a credential.
21. Complete a position designation in IdMAX for all applicants holding a position.
22. For foreign nationals, initiate and coordinate the annual review process.
    * 1. The Sponsor shall:
23. Be a U.S. Citizen and an identified entity for the following applicant affiliations:
    1. Human Capital specialist for NASA civil service employees.
    2. Contracting Officer’s Representatives (COR) or other Federal civil service technical personnel responsible for work requirements for contractors.
    3. A Caltech employee working at JPL for Caltech employees, contractors, and affiliates at JPL.
    4. Grants technical official for grantees.
    5. Authorizing official or designee for any agreement between NASA and any outside entity.
    6. The NASA civil service employee program or project manager who requires a foreign national to access NASA facilities or IT systems.
    7. Tenant with a PIV or registered PIV/Common Access Card (CAC) and approved by the AIMO for tenant organizations.
    8. For all other affiliations, a NASA civil service employee designated to perform the role of sponsor for a given applicant’s affiliation.
24. Hold a valid credential that enables access to IdMAX to perform the functions of Sponsor.
25. Establish and endorse the need for a relationship between the applicant and NASA, affirm the applicant is in good standing, substantiate the need for a credential to be issued to the applicant, and provide sponsorship for the applicant.
26. Approve the position designation in IdMAX.
27. Correct or complete, as necessary, incorrect or missing information in the credential issuance request.
28. Track the status of persons and reports when access should be modified or terminated.
29. Ensure the applicant is advised to appear in person before the enrollment official and present the necessary identity source documents, as identified in the NASA-Approved Identity Source Documents, in original form.
30. Ensure the Applicant understands all requirements of the Applicant’s specific visit or assignment.
    * 1. The Enrollment Official shall:
31. Be a NASA worker within the OPS organization or designated by the AIMO or PIF Manager to perform the role of enrollment official.
32. Perform identity proofing of the applicant.
33. Check identity source documents for authenticity, capture copies and/or scans of the identity source documents, compare the name and demographic data in the credential request and the identity source documents, and determine whether any discrepancies exist.
34. Ensure the successful collection of the information necessary to confirm employer sponsorship, bind the applicant to their biometric data, and validate identity source documentation.
35. Collect, establish, and verify identity information of an applicant.
36. Capture the biometrics and photograph of the applicant.
    * 1. The Authorizer shall:
37. For PIV and ASB credentials, be a NASA civil servant within the OPS organization approved by the AIMO.
38. For Center-specific badges, be a NASA worker within the OPS organization and approved by the PCI Manager.
39. Provide the final approval for issuance of a credential to the applicant.
40. Hold no other role in the identity management or credential issuance process for a given identity.
41. Be personnel security specialists trained in accordance with Federal credentialing and adjudication guidelines and standards as specified in in NPR 1600.3.
42. Review the credential request, sponsor’s approval, and results of identity proofing and vetting.
43. Coordinate checks for existing background investigations and requests for background investigations, as necessary.
44. Adjudicate the results of all database checks and background investigations, in accordance with NPR 1600.3.
45. Record the adjudication determination and approve or deny credential issuance or continued use of an issued credential based on the determination.
    * 1. The Investigation Reviewer shall:
46. Be a NASA worker within the OPS organization.
47. Not authorize production or issuance of PIV or ASB credentials but may provide the final approval for issuance of Center-specific badges, as allowed by the PIF Manager.
48. Review and confirm the position designation with the requester and sponsor.
49. Assist the authorizer by:
    1. Reviewing the credential request and the sponsor’s endorsement.
    2. Confirming identity proofing and biometrics capture.
    3. Coordinating checks for existing background investigations.
    4. Coordinating requests for background investigations.
    5. Coordinating background investigation submissions.
    6. Recording results of database checks.
    7. Updating applicant information.
       1. The Issuance Official shall:
50. Be a NASA worker within the OPS organization or designated by the AIMO or PIF Manager to perform the role of issuance official.
51. Perform credential personalization operations and issue the identity credential to the applicant after all identity proofing, background checks, and related approvals have been completed.
52. Maintain records and controls for credential stock to ensure that stock is only used to issue valid credentials.
53. Issue credentials to authorized applicants.
54. Provide an electromagnetically opaque badge holder to all applicants receiving a smartcard and a badge sleeve to all other applicants.
55. Submit the order for the credential to be encoded and printed with the appropriate identity information.
56. Verify the applicant’s identity through visual and biometric verification prior to issuing the credential.
57. Advise the applicant to select a Personal Identification Number (PIN) that is 6-8 digits long and is not easily guessable or individually identifiable.
58. Order, receive, account for, secure, and handle unissued credential stock and 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 any individual.
    * 1. The PIV Digital Signatory shall digitally sign the PIV biometrics and Cardholder Unique Identifier (CHUID), as defined in FIPS 201.
      2. The PIV Authentication Certification Authority (CA) shall sign and issue the PIV Authentication Certificate.
      3. The International Visit Coordinator (IVC) shall:
59. Review, coordinate, process, and grant final authorization of all visits, assignments, access, and credential requests by and for foreign nationals at NASA.
60. Work with program managers and sponsors to determine access requirements, work description, dates of affiliation, length of assignment, citizenship, risk associated with the visit, and other pertinent information.
61. Work with the Center Protective Services Office, program managers, and sponsors to determine escort requirements while the foreign national is located at the Center.
62. Conduct and complete pre-visit identity proofing and vetting.
63. Coordinate and ensure access reviews are performed by the project office, sponsor, Center Protective Services Office, Center Counterintelligence Special Agent (CISA), and export control office.
64. When necessary, coordinate review and approval with the Center public affairs office for press or foreign space agency members, the Center protocol office for protocol visits, and the Center sponsor and the export control office for NASA Exchange Visitor Program visitors.
65. Inform the sponsor of the approval or denial of the access request and, in the case of approvals, report the terms and conditions of the visit to the sponsor.
66. Coordinate with request reviewers to ensure appropriate timeframes are followed for processing of the access request and escalates outstanding requests to the AIMO for resolution.
    * 1. The Center Export Control Administrator shall review all access requests for foreign nationals and provide the IVC an approval or denial recommendation.
      2. Agency Export Control Desk Officers shall review all access requests for foreign nationals from designated countries and provide the IVC an approval or denial recommendation.
      3. The Escort shall:
67. Be, for the following categories of escorted individuals:
    1. A U.S. citizen or Lawful Permanent Resident (LPR) holding a PIV, ASB, or registered PIV/CAC and have a favorably adjudicated Tier 1 or higher background investigation for any individual requiring escort including visitors, foreign nationals from nondesignated countries, and foreign nationals from designated countries.
    2. A nondesignated foreign national, approved by the CCPS holding a PIV, ASB, or registered PIV/CAC and have a favorably adjudicated Tier 1 or higher background investigation for other nondesignated foreign nationals within the same program/project (e.g., International Partners escorting other International Partners).
68. Foreign National Escorts will be required to complete annual Foreign National Escort Training and submit a NASA Access Management System (NAMS) request for a Foreign National Escort badge upon completion of training.
69. The escort shall display the Foreign National Escort badge when escorting foreign nationals.
70. Assume responsibility and accountability for the escorted individual.
71. Provide continuous physical supervision of those persons without sufficient access privileges, as determined by a risk-based determination, or need to be granted unsupervised access to the Center for the entire duration of the visit or assignment, beginning with entry through the Center perimeter and concluding with exit through the Center perimeter.
72. Maintain active certified escort status by completing annual escort training and possess a Foreign National Escort badge.
73. Permit access only to those areas the escort and the escorted person have been granted access.
74. Be assigned and clearly display at all times an additional, Agency-standard badge that identifies their certified status as an escort at that Center.
75. Ensure they understand and follow all escort requirements for the Center at which they are escorting and, when approved to escort at another Center, complete any Center-specific escort training and understand and follow all escort requirements at that Center.
    * 1. The Technical Point of Contact (also referred to as a technical representative or agent) shall:
76. Be able to provide detailed information about an applicant’s work requirements and responsibilities.
77. Understand the technical nature of the work to be performed.
78. Work with the sponsor, requester, and escort (when required) to process an applicant and ensure the applicant is aware of their responsibilities while at the Center.
79. Ensure the applicant is properly escorted at all times, when required.
    * 1. The Host shall:
80. Be the point of contact for a visitor to a NASA Center.
81. Understand the purpose of the visit, sponsor the visitor pass request, and support processing the visitor pass request.
82. Ensure the visitor is properly escorted and aware of their responsibilities while at the Center.
83. Assume responsibility and accountability for the visitor.
    * 1. The Trusted Partner Organization shall:
84. Work with NASA to develop a Trusted Partner Agreement that identifies all required actions of the Trusted Partner Organization and associated Trusted Partner Identity Requesters and Trusted Partner Affiliation Sponsors. The Trusted Partner Agreement may be appended to an existing agreement between NASA and the Trusted Partner Organization.
85. Be held accountable for all individuals associated with the Trusted Partner Organization and affiliated with NASA.
86. Appoint Trusted Partner Identity Requesters and Trusted Partner Affiliation Sponsors to support identity proofing, sponsoring and enrollment of Trusted Partner Organization personnel.
    * 1. The Trusted Partner Identity Requester shall:
87. Be appointed by a Trusted Partner Organization and approved by the AIMO.
88. Be a U.S. citizen or LPR holding a PIV, ASB, or registered PIV/CAC and have a favorably adjudicated Tier 1 or higher background investigation.
89. Perform the role of Identity Requester for the Trusted Partner Organization as part of the Trusted Partner Agreement.
    * 1. The Trusted Partner Affiliation Sponsor shall:
90. Be appointed by a Trusted Partner Organization and approved by the AIMO.
91. Be a U.S. citizen or LPR holding a PIV, ASB, or registered PIV/CAC and have a favorably adjudicated Tier 1 or higher background investigation.
92. Perform the role of Affiliation Sponsor for the Trusted Partner Organization as part of the Trusted Partner Agreement.
93. Adhere to all requirements defined in the Trusted Partner Agreement with NASA.
94. Ensure the applicant’s current good standing and affiliation with the Trusted Partner Organization.
95. Confirm the applicant’s identity using the established and agreed upon identity proofing process.
96. Review and confirm an applicant’s identity data and enrollment information.
97. Ensure the applicant has completed the proper identity proofing and vetting process defined in the Trusted Partner Agreement with NASA.
98. Ensure an applicant’s need for access.
99. Initiate the process to register a credential if required and as approved in the Trusted Partner Agreement.
100. Provide the applicant with information and instruction on all processes and requirements outlined in the Trusted Partner Agreement.

## Separation of Duties

* + 1. The principle of separation of duties shall be enforced to ensure that no single individual has the capability to issue a credential without the participation of at least one other authorized person.

## Training

* + 1. ICAM Overview training shall be required for each role in the IdMAX system.
    2. Annual role-based training shall be required for individuals performing the role of escort.
    3. Training records shall be maintained by the System for Administration, Training, and Educational Resources for NASA (SATERN) computer-based training system or subsequent/succeeding system(s).

## Privacy

* + 1. NASA shall ensure that applicant information and systems which facilitate identity management processes are managed consistent with:

1. NPD 1382.17, NASA Privacy Policy.
2. NPR 1382.1, NASA Privacy Procedural Requirements.
3. Homeland Security Presidential Directive 12 (HSPD-12).
4. OMB Memorandum 05-24.
5. Privacy Act of 1974 (Public Law 93-579, 5 U.S.C. § 552a).
6. OMB 03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.
7. E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. § 101).
8. Children’s Online Privacy Protection Rule, 15 U.S.C. § 6501-6505.
   * 1. Per the E-Government Act, 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 (SOR) (SOR) will be updated and maintained to reflect pertinent information regarding the SOR such as the disclosure of information to other Federal agencies.
     2. Only individuals with a legitimate need to access the systems in which an applicant’s PII or IIF is stored and maintained shall be allowed to access those systems. NASA will ensure privacy of applicant information is sustained through all steps of identity management including enrollment and issuance.
     3. PIFs shall provide an electromagnetically opaque badge holder that assists in protecting against unauthorized contactless access to information stored in the credential.
     4. A Privacy Act Statement shall be posted in every enrollment and issuance location, on the applicable NASA Web site, and made available to the applicant through other means as appropriate.
     5. The Subscriber Agreement shall be posted in every enrollment and issuance location, on the applicable NASA Web site, and made available to the applicant through other means as appropriate.
     6. The following documentation shall be made available, at the request of the applicant:
9. Complaint procedures.
10. Appeals procedures for those denied a PIV or ASB credential or whose PIV or ASB credential is revoked are described in NPR 1600.3. There are no appeals procedures for those who have been denied a Center-specific badge.
11. Consequences for individuals violating NASA privacy policies, as described in NPR 1382.1.
    * 1. 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. 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.
      3. NASA shall archive and safeguard all identity data and files pursuant to NPD 1440.6, NASA Records Management, and NPR 1441.1, NASA Records Management Program Requirements.
      4. PII will not be released to any entity external to NASA except as allowed by the NASA Privacy Act Systems of Records Notice (SORN), 10SECR, Security Records System.
      5. Minors, Children, and Infants
         1. NASA will collect, maintain, and protect the PII (including fingerprints) of minors, defined as individuals between the ages of 13 and 18, in accordance with the requirements of this NPR. Minors, or their parent or guardian, may provide and authorize use of the minor’s PII. Fingerprints of minors will be collected only in those situations where the minor will be working for NASA and in accordance with the requirements of this policy and in compliance with relevant Federal laws regarding the employment of minors.
         2. The PII of a minor will not be released to any entity external to NASA except when required for identity proofing and vetting as part of employment as a NASA worker in accordance with the requirements of this policy and in compliance with relevant Federal laws regarding the employment of minors.
         3. In situations requiring issuance of a Center-specific badge to a minor, no database checks will be performed.
         4. An ASB may be issued to a minor only as required for access under the aforementioned employment of a minor.
         5. NASA will collect, maintain, and protect the PII (excepting fingerprints which will not be collected) of children, defined as individuals between the ages of 2 and 13, in accordance with the requirements of this NPR and the requirements set forth in the Children’s Online Privacy Protection Rule (“COPPA”). Parents or guardians of children may provide and authorize use of a child’s PII. A child may provide their PII to NASA and NASA will attempt to identify the submission of PII by a child and contact the parent or guardian in order to obtain necessary consent prior to continued use of the PII. Failure to obtain consent from the parent or guardian of a child within 5 business days will result in permanent removal of the provided PII.
         6. In situations requiring issuance of a Center-specific badge to a child, no database checks will be performed.
         7. NASA will not collect, maintain, or release to any entity external to NASA the PII of infants, defined as individuals under the age of 2, except to support daycare operations at a Center or in such situations as benefits the health and/or safety of the infant or as otherwise required by Federal law.
         8. The PII of a minor not employed by NASA, child, or infant will be permanently removed when no longer required.
      6. The PII of a minor, child, or infant will not be released, except as otherwise stated in this policy, to any entity external to NASA except in such situations as benefits the health and/or safety of the minor, child, or infant or as otherwise required by Federal law.
         1. In all situations involving the release of PII of a minor, child, or infant, only the minimum necessary PII will be released.
         2. In situations where an individual other than a parent or guardian (e.g., teacher) submits the PII of a minor or child, it is the sole responsibility of that individual to obtain permission from a parent or guardian to submit PII for the minor or child.
         3. The PII of a minor or child shall only be used within NASA for the purposes of establishing an identity, verifying the identity, and/or granting access in accordance with the policies established in this NPR for those purposes.

## Events and Tours

* + 1. The CCPS may require additional credentialing (e.g., event/tour badge, wristband, vehicle placards, etc.) or vetting (e.g., visitor registration, fingerprint check, etc.) requirements for events and tours beyond those prescribed in this section.
    2. The host or organizer for an event or tour shall coordinate with the Center Office of Protective Services, Center Export Control, and the appropriate Facility Manager(s) to establish and approve an event or tour plan prior to the event or tour. Additional personnel may be included in the event or tour planning and approval as appropriate.
    3. The event or tour plan will include, at a minimum, the following: a description of the event; dates, times, and durations for the event; security presence; authorized access control points; security perimeter of the event; additional resources (e.g., guards/officers, moveable fencing/barriers, etc.); list, description, and reason for any facilities or areas involved; emergency action plan; and threat summary.
    4. Center Office of Protective Services, Center Export Control and the appropriate Facility Manager(s) may deny or place restrictions on any event or tour based on unacceptable risk, disruption, or proximity to controlled or sensitive facilities, technologies, operations, information, or other assets, or for any other reason.
    5. The IVC shall have final approval authority for any foreign national participation in an event or tour.
    6. Events and tours not formally approved by the Center Office of Protective Services, Center Export Control, and the Facility Manager(s) shall require all participants to adhere to all visitor requirements.
    7. Events and tours which require escort shall establish an escort-to-visitor ratio which ensures the escort is able to maintain operational control of participants.
    8. Deviations from an approved event or tour shall be approved by Center Office of Protective Services, Center Export Control, and the appropriate Facility Manager(s).
    9. Authorized Public Tours
       1. An authorized public tour is a guided excursion, generally offered to the general public, by which escorted access is granted to non-public areas of interest on a Center.
       2. Authorized public tours may be managed and/or operated directly by a NASA Center or through an affiliated visitor facility for which an agreement has been established to conduct such tours.
       3. Authorized public tours shall require no identity proofing and vetting except for foreign nationals at the discretion of the CCPS.
       4. Participants in an authorized public tour shall be escorted at all times.
    10. Special Tours
        1. A special tour is a guided excursion, offered to specific, vetted individuals, by which escorted access is granted to non-public areas of interest on a Center.
        2. Special tours may be managed and/or operated by specific NASA organizations for which such activities are recognized.
        3. Special tours shall require identity proofing and vetting and credentialing as a visitor, at a minimum.
        4. Participants in a special tour shall be escorted at all times.
    11. Public Events
        1. Public events are indoor and/or outdoor activities open to the public or offered to the general public during which the established security perimeter of the Center is temporarily modified to allow access to areas of the Center which are typically controlled. Examples of such events include open house days at a Center or a launch event at KSC. Public events may be paired with special events which designate certain areas as publicly accessible and other areas as limited public accessibility.
        2. Public events shall be approved by the Center Director, or designee, in addition to all previously mentioned approvals.
        3. The CCPS shall notify the AA/OPS of any approved public event.
        4. Public events shall require no identity proofing and vetting.
        5. Public events shall not require escort.
    12. Special Events
        1. Special Events are activities (retirement ceremony, awards ceremony, special launch viewing location, etc.) in support of NASA Missions, Center Operations, or by Special Request from a NASA Organization during which access to areas of the Center are made available to specific individuals.
        2. Special events may be requested by NASA civil servants with approval of their organizational management/supervisor or by contractors with approval of their COR. Such approvals are in additional to and performed prior to the reviews and approvals defined in this section.
        3. Special events should be approved by the Center Director, or designee, in addition to all previously mentioned approvals.
        4. The CCPS should notify the AA/OPS, or designee, of approved special events.
        5. Special events shall require identity proofing and vetting as a visitor, at a minimum.
        6. Participants in a special event shall be escorted when not in the special event location.
    13. Escorting Requirements for Authorized Public Tours and Special Events
        1. Escorts shall follow all requirements of section 2.3.14.
        2. When a foreign national is attending an Authorized Public Tour or Special Event, the escort shall be an authorized foreign national escort in accordance with section 2.3.14.
        3. The escort shall observe all safety and security policies, and the specific requirements of any facility to be visited.
        4. The escort shall maintain operational control of their assigned guests and remain with them at all times.
        5. Ensure guests being escorted wear the required, if any, visitor pass.
        6. Guests will only have access to authorized areas and public domain information.
        7. The escort shall have the proper access levels and approvals to enter facilities.

# Enrollment and Credential Issuance

## Overview

* + 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 FIPS 201.
    2. The NASA Identity Management and Account Exchange (IdMAX) system shall be the sole and authoritative source for the collection 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. No other forms or systems may be used to collect applicant identity data unless specifically approved by the AIMO.
    3. The IdMAX system shall operate as the authoritative system for the enforcement of and adherence to Federal policies and guidance for the purposes of identity, credential, and access management.
    4. Chain of Trust
       1. A chain of trust shall be followed which 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.
       2. The credential shall be 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. PIV enrollment records provided by an applicant’s previous Agency may be accepted when the biometric data contained in the PIV enrollment record is successfully matched to the applicant.

## Applicant Categories

* + 1. NASA interacts with both workers and non-NASA workers in the execution of its mission.
       1. Workers are persons who directly support the mission and goals of NASA and/or are compensated by NASA (e.g., Federal civil servants, contractors, Caltech Employees at JPL, interns, etc.). Workers may be associated with NASA for long-term (180 days or more in a 365-day period) or short-term (0-179 days in a 365-day period). Association with NASA begins the first day of affiliation, regardless of schedule.
    2. Non-NASA Workers are persons who use NASA resources and/or information to conduct independent work not directly for the benefit or consumption of NASA (e.g., tenants, researcher using computational hours on a NASA supercomputer) or persons participating in activities not directly benefiting NASA (e.g., members of the public on a public tour, members of a social club). Non-NASA workers may be associated with NASA for long-term (180 days or more in a 365-day period), short-term (0-179 days in a 365-day period), or as a visitor (0-29 days in a 365-day period). Association with NASA begins the first day of affiliation, regardless of work schedule.
    3. NASA Federal civil service employees are workers employed and paid by NASA and 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 and these employees will be issued a civil servant badge.
    4. NASA contractor employees are workers employed by a contracting organization or entity with the responsibility to perform activities for NASA.
    5. Grantees are workers and non-workers supporting NASA through a grant or cooperative agreement and performing grant-funded activities requiring physical or logical access to NASA resources. Recipients of grants who do not require physical or logical access to NASA resources shall not be processed or granted access as grantees.
    6. Detailees, for the purposes of this NPR, are workers who are either Federal employees from other Federal agencies, U.S. military personnel, or non-Federal employees working at NASA through an IPA assignment. Credentials issued to detailees shall be designated with an affiliation of NASA and appear as a Federal employee credential. Federal 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.
    7. International partners are workers 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 1050.7, Authority to Enter into Partnership Agreements. A signed international agreement shall first be in effect for international partners to receive a foreign national credential.
    8. Tenants are typically non-NASA workers 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 Federal Government agency as either a civil servant or contractor and may have a PIV credential from their agency which will be registered with NASA to permit physical and/or logical access. Tenants will be issued Agency Smart Badges. A tenant from another Federal Government agency without a PIV credential may, at the discretion of the CCPS, be issued a NASA PIV Smartcard following the processes and requirements for a NASA PIV Smartcard. Tenants with a PIV credential from another Federal Government agency which cannot be registered in IdMAX may be issued an Agency Smart Badge or Center-specific badge, at the discretion of the CCPS.
    9. Transients may be workers or non-NASA workers (i.e., construction workers, club members, childcare drop off/pickup, delivery drivers, retirees, Center transits, and others requested by the CCPS and approved by the AIMO) who require intermittent access to a NASA Center. Transients shall complete a Federal Bureau of Investigation (FBI) National Criminal History Check (NCHC) at the time of badge issuance and may be issued an Agency Smart Badge, or Center-specific badge at the decision of the CCPS.
    10. Logical Transients may be workers or non-NASA workers (e.g., ISS payload operator, vendor support, contractor requiring non-routine access from their own facility) who require intermittent, non-routine access to very low risk systems or roles in NASA IT systems from a non-NASA facility. Logical transients shall complete an approved trusted partner federation or individual proofing mechanism.
    11. Retirees are previous NASA civil servants who have favorably left the Agency and may retain access to services offered at their home Center. Retirees may be issued a NASA Retiree Souvenir/ID Card which grants no access or benefits to the Center. Retirees requiring access to a NASA Center will be treated as visitors or as another affiliation defined in this section.
    12. Emeritus are previous NASA civil servants who have favorably left the Agency and entered into an emeritus agreement to provide consulting and mentorship support at a NASA Center. Emeritus will be issued an Agency Smart Badge.
    13. Interns are workers participating in an internship sponsored by the NASA Office of Science, Technology, Engineering, and Math (OSTEM) which benefits and/or furthers the goals, objectives, and efforts of NASA. Individuals who are interns at another company working with NASA will not be treated as interns and will be treated as the affiliation for the company for which they work.
    14. Visitors are individuals requiring escorted or supervised physical-only 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. Visitors exceeding 29 days in a 365-day period may continue to be processed as a visitor at the discretion of the CCPS. Visitors will receive no access beyond Center guest wireless as permitted by the Center and upon approval.
    15. Customers are non-NASA workers who have requested and been approved for access to NASA assets which are considered publicly accessible but require authentication and/or identity proofing. Examples of such assets include but are not limited to patents and software through the NASA Technology Transfer Program, and NASA supercomputers.
    16. Digital worker identities are machines, programs, and artificial intelligences (often referred to as bots), owned by a NASA civil servant. All digital worker identities will be assigned to agreements that define their access and capabilities. Digital worker identities shall be requested and sponsored but do not require enrollment, investigation, or training. Digital worker identities will be authorized by the OCIO, or designee, for logical access and the CCPS for physical access. Non-humans may be issued an Agency Smart Badge or logical access credential.

## Enrollment and Issuance Procedures

* + 1. Identity proofing and vetting requirements will follow the requirements in section 3.7, Identity Proofing and Vetting Requirements.
    2. The enrollment and issuance procedures identified in this section shall be performed in-person at a NASA Center or Facility or a NASA-approved enrollment location. Specific procedures for visitors, remote-only, and foreign national enrollment and issuance procedures can be found in subsequent sections and chapters.
    3. Step 1: Identity Request
       1. The requester initiates an identity request within IdMAX for an applicant using the applicant’s full legal name. For civil servants, identity information is submitted by the HR specialist. For all other persons, identity information is entered by the requester or the applicant via invitation, as required in IdMAX.
    4. Step 2: Sponsorship
       1. The sponsor validates the applicant’s identity and assignment data in the identity request. The sponsor reviews the Position Designation in IdMAX and approves or denies the request, establishing the need for a relationship between the applicant and NASA and the applicant’s need for a credential.
       2. The sponsor advises the applicant to appear in person before the enrollment official and present the necessary identity source documents, as identified in the NASA-Approved Identity Source Documents, in original form.
    5. Step 3: Reciprocity and Vetting
       1. If the applicant is requesting a credential which does not require a background investigation then the authorizer or designee conducts the appropriate database checks, the authorizer submits the request to the enrollment official, and the applicant proceeds to enrollment, section 3.3.6, Step 4: Enrollment Process.
       2. The authorizer or investigation reviewer reviews Federal databases and takes appropriate steps to validate the applicant’s investigation status with regard to a current investigation.
       3. 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 3.3.6, Step 4: Enrollment Process.
       4. If no investigation is on file or in progress, the authorizer coordinates initiation of the appropriate background investigation. The authorizer submits the request to the enrollment official and the applicant proceeds to enrollment, section 3.3.6, Step 4: Enrollment Process.
    6. Step 4: Enrollment Process
       1. The applicant will appear in person before the authorized enrollment official and perform all required enrollment activities. The applicant will present the required NASA-approved identity source documents in original form, one of which will be a government issued picture identification. The applicant will allow capture of all required fingerprints, photographs, and signatures, in compliance with the following phases of the enrollment process.
       2. NASA-Approved Identity Source Documents – The enrollment official inspects the identity source document for authenticity and validates the identity source document through visual or electronic scrutiny and, when necessary, with the authority or entity which issued the document. The enrollment official obtains and maintains legible photocopies or scanned copies of the original identity source documents. Any documents which 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.) shall be rejected by the enrollment official and reported to the Office of Inspector General (OIG) and CCPS for review. Photocopies of rejected documents are to be made and retained in accordance with the NASA records retention schedule. Identity source documents which do not pass electronic examination are rejected and another NASA-approved identity source document will be provided and subjected to visual or electronic scrutiny. In the event the applicant is required to provide documentation to resolve discrepancies or omissions in data collected, the enrollment official will review the information with the applicant as necessary. The information submitted by the applicant will be used to update the applicant identity record.
       3. Fingerprints – The applicant will allow capture of all required flat and/or rolled fingerprints. A compatibility test will be performed to ensure two enrolled fingerprints can be used for biometric matching. 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. In situations where individual fingerprints cannot be captured due to damage, injury, deformity, or loss, the fingerprints will be labeled accordingly. When fingerprints are captured at a location other than an approved enrollment location, the transmission of those fingerprints to the Center Office of Protective Services will 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 Office of Protective Services by the entity that took the fingerprints.
       4. 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 glasses, hats, headphones, etc. The CCPS may allow head coverings worn for religious or medical reasons or eyeglasses worn for medical reasons and which do not hide any part of the face, from natural hairline to the chin. The facial expression shall be neutral (non-smiling) with a closed mouth. Permanent eye patches that do not obscure an excessive portion of the face need not be removed. Individuals with temporary eye patches or other temporary coverings should be issued an Agency Smart Badge until such time when the patch or covering 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 AIMO. The facial image collected from the applicant during enrollment may be used for authenticating badge recipients covered under section 508 of the Rehabilitation Act.
       5. Signature – An electronic signature of the applicant shall be obtained. For applicants requesting a credential, the enrollment official will provide the applicant with the Subscriber Agreement and the signature will attest to the applicant’s reading and acceptance of the Subscriber Agreement.
    7. Step 5: Authorization
       1. If a database check or investigation is required and no database check or investigation is on file or in progress, the fingerprints captured during enrollment shall be submitted to the appropriate authority with a request for a database check or background investigation. If a fingerprint check comes back with a status of unclassifiable, the results of a name check will be used to perform the access determination.
       2. The authorizer makes an access determination based upon favorable fingerprint check results, results of other database checks, or evidence of an acceptable existing background investigation (as found in section 3.3.5, Step 3: Reciprocity and Vetting). If the access determination is favorable, the authorizer will authorize access and creation and issuance of the credential.
       3. Access determinations shall be performed in accordance with section 6.3, Credentialing Determinations.
    8. Step 6: Credential Production
       1. If the credential is to be produced using central print, the necessary information is included in a batch card production request. The initialized and printed badges are delivered to NASA and forwarded to the appropriate issuance officials where the credentials shall be held in a secure location.
       2. If the credential is to be produced using local print, the issuance official shall print and inline encode the appropriate credential and validate the identity information on the credential with the identity information in the credential request.
       3. The applicant will be notified when the credential is ready for issuance.
    9. Step 7: Issuance Process
       1. The applicant shall appear before the issuance official, who obtains the credential from storage.
       2. The issuance official shall check the printed credential to verify the identity of the applicant and oversee a biometric match of the applicant to the identity record.
       3. If required, the applicant shall enter a PIN which finalizes encoding of the credential. The applicant is advised the PIN will be 6-8 digits long and not easily guessable or individually identifiable (e.g., phone number, Social Security Number). Upon completion of the credential encoding, the credential is officially released to the applicant.
       4. For any credential issued without a biometric verification, facial recognition shall be performed by comparing the photograph stored in IdMAX to the photograph on the badge and the face of the applicant. Two forms of identity source documentation shall be verified against the individual. When the facial verification is completed, the badge will be released to the applicant.
       5. An approved electronically shielded badge holder shall be offered to the applicant in order to protect the credential and the privacy of information on the credential.

## Visitor Enrollment and Issuance Procedures

* + 1. All visitor enrollment and issuance procedures shall occur at a NASA Center or Facility.
    2. U.S. citizens and Lawful Permanent Resident (LPR) visitors shall complete visitor invitation and registration in the Enterprise Visitor Access Management System (EVAMS). Visitors may require approvals based on specific NASA Center or Facility requirements.
    3. Foreign national visitors shall be processed through IdMAX in accordance with section 4.4, Enrollment and Issuance Procedures for Foreign National Visitors.
    4. Visitors who are minors, children, or infants shall not be required to register in EVAMS when accompanied by a parent or guardian but may elect to do so, following all appropriate requirements, when in possession of a NASA-approved identity source document.
    5. Logical access will not be granted to visitors.
    6. Visitors requiring subsequent routine physical access or logical access shall be processed in accordance with the requirements of section 3.3, Enrollment and Issuance Procedures.
    7. Identity proofing and vetting requirements shall follow the requirements in section 3.7, Identity Proofing and Vetting Requirements.
    8. Step 1: Visit Request
       1. A requester may submit a visit request within EVAMS for a US Citizen or LPR visitor. Identity information is entered by the requester or the applicant via invitation, as required in EVAMS.
       2. Visit requests will be reviewed based on the requirements of the visit and the specific accesses requested.
    9. Step 2: Enrollment and Check-In Process
       1. The visitor will appear in person at the Center and perform all required enrollment and check-in activities.
       2. NASA-Approved Identity Source Document – The visitor will present a primary NASA-approved identity source document in original form which shall be reviewed and processed in accordance with the requirements of section 3.3.6.2.
       3. Photograph – When required by the Center, the applicant’s photograph shall be captured in accordance with the requirements of section 3.3.6.4.
    10. Step 3: Authorization
        1. If any database checks are performed on the visitor, an authorizer will approve badge issuance following a credentialing determination of the returned results, in accordance with section 6.3, Credentialing Determinations.
    11. Step 4: Visitor Pass Production and Issuance
        1. A visitor pass will be printed and issued following verification of the visitor’s identity source documentation.
        2. If the visitor is approved for areas requiring electronic physical access an electronic access card will be assigned to the visitor and will accompany the visitor pass. The electronic access card will be returned at the end of the visit.

## Remote Enrollment Procedures

* + 1. Remote enrollment and issuance shall not replace the requirements for in-person enrollment and issuance procedures when physical access or access to high-risk logical assets is required.
    2. Any individual completing remote enrollment and issuance procedures who subsequently visits a NASA Center or Facility shall undergo the enrollment procedures described in section 3.3, Enrollment and Issuance Procedures.
    3. Access to very-low risk logical assets may be granted following completion of remote enrollment and issuance procedures.
    4. Access to low or moderate risk logical assets may be granted following completion of remote enrollment and issuance procedures and implementation of OPS and OCIO-approved risk-mitigations.
    5. Access to low or moderate risk logical assets with no OPS and OCIO-approved risk-mitigations shall not be allowed through the remote enrollment and issuance procedures. Such access will only be granted following the requirements in section 3.3, Enrollment and Issuance Procedures.
    6. Remote enrollment and issuance shall include, at a minimum, identity request, sponsorship, verification of identity, verification of identity data, capture of NASA-approved identity source documents, and capture of photograph.
    7. Identity proofing and vetting requirements shall follow the requirements in section 3.7, Identity Proofing and Vetting Requirements.
    8. Step 1: Identity Request
       1. The requester initiates an identity request within IdMAX for an applicant. Identity information is entered by the requester or the applicant via invitation, as required in IdMAX.
    9. Step 2: Sponsorship
       1. The sponsor validates the applicant’s identity and assignment data in the credential request. The sponsor reviews the Position Designation in IdMAX and approves or denies the request, establishing the need for a relationship between the applicant and NASA and the applicant’s need for access.
       2. The sponsor advises the applicant to complete a remote enrollment and issuance and present the necessary identity source documents, as identified in the NASA-Approved Identity Source Documents, in original form.
    10. Step 3: Enrollment Process
        1. The applicant will complete all required enrollment activities.
        2. NASA-Approved Identity Source Document – The applicant will present a primary and secondary NASA-approved identity source document in original form which shall be reviewed and processed in accordance with the requirements of section 3.3.6.2.
        3. Photograph – The applicant’s photograph shall be captured in accordance with the requirements of section 3.3.6.4.
        4. Signature – An electronic signature of the applicant shall be obtained. This signature may be obtained in the form of an approval action during completion of the remote-only enrollment and issuance procedures.
    11. Step 4: Authorization
        1. If any database checks are performed, an authorizer will approve credential issuance following a credentialing determination of the returned results, in accordance with section 6.3, Credentialing Determinations.
    12. Remote enrollment and issuance procedures shall follow the processes established in IdMAX.

## Remote Issuance Procedures

* + 1. Remote issuance shall not replace the requirements for in-person issuance procedures when physical access or access to high-risk logical assets is required.
    2. Remote issuance shall require biometric verification of the individual prior to completion of the issuance.
       1. Credentials shall be delivered to the individual in a manner which ensure the individual requesting the credential is the individual receiving the credential.

## Identity Proofing and Vetting Requirements

* + 1. Centers shall accept as valid the identity proofing and vetting of their peer Centers as a baseline requirement, consistent with this NPR. Additional identity proofing and vetting may be required should access requirements change.
    2. All individuals requiring access shall provide minimum identity data and PII necessary to establish an identity including, but not limited to, full legal name and date of birth. Additional identity data and PII including, address, place of birth, citizenship, social security number (SSN), and contact information may be required.
    3. A primary and secondary NASA-approved identity source document shall be required, unless otherwise specified.
    4. A minimum of a Tier I investigation will be required for all individuals needing routine, non-intermittent unescorted physical and/or logical access to NASA assets for a period exceeding 179 calendar days in a 365-day period beginning the first day of affiliation, regardless of work schedule.
    5. A minimum of an NCHC will be required for all individuals needing routine, non-intermittent unescorted physical and/or logical access to NASA assets for a period up to but not exceeding 179 days in a 365-day period beginning the first day of affiliation, regardless of work schedule.
    6. A minimum of an NCHC will be required for all individuals needing non-routine, intermittent unescorted physical access to a NASA center for any period of time.
    7. A minimum of an approved trusted partner federation or individual proofing mechanism will be required for all individuals requiring non-routine remote-only logical access to low or moderate risk logical assets for which OCIO-approved role level mitigations and controls have been implemented.
    8. Individuals requiring access to publicly accessible resources will be subject to the above investigative requirements only to the extent deemed necessary by the resource to which access is being requested and granted.
    9. Long-term Physical Only Access for Non-NASA Workers
       1. A primary and secondary NASA-approved identity source document shall be required.
       2. An NCHC, commonly referred to as a fingerprint check, will be required for all non-NASA Workers needing unescorted physical access to NASA assets for a period exceeding 179 days in a 365-day period beginning the first day of affiliation, regardless of work schedule.
    10. Visitors
        1. A primary NASA-approved identity source document shall be required, and a secondary NASA-approved identity source document may be required, at the discretion of the CCPS.
        2. An NCHC or National Crime Information Center (NCIC) may be required for any individual processed as a visitor at the discretion of the CCPS.

## Trusted Partnerships and Federation

* + 1. NASA may enter into Trusted Partner Agreements with partner organizations (e.g., domestic and foreign, government, commercial, educational, etc.) in order to leverage the identity proofing and vetting processes and/or credentialing of the Trusted Partner Organization.
       1. The Trusted Partner Agreement will outline all requirements necessary to establish trusted identities and credentials between NASA and the Trusted Partner Organization.
    2. OPS will review and approve, in coordination with relevant offices, all Trusted Partner Agreements.
    3. The Trusted Partner Agreement will identify the identity proofing and vetting processes and requirements (commonly referred to as HR processes) of the partner organization.
    4. The Trusted Partner Agreement will identify the credential issuance process and credential capabilities of the Trusted Partner Organization.
    5. NASA will review the identity proofing and vetting processes and requirements of the Trusted Partner Organization and assign an identity assurance level for identities associated with the Trusted Partner Organization.
    6. NASA will review the credentialing processes and requirements and credential capabilities of the Trusted Partner Organization and assign an authentication assurance level for credentials associated with the Trusted Partner Organization.
    7. The Trusted Partner Agreement may include processes and requirements to increase identity and authentication assurance levels to attain desired assurance levels.
    8. A trusted partner access plan (i.e., Access Control Plan (ACP)) may be assigned to a Trusted Partner Agreement that identifies a list of assets that can be accessed by identities associated with the Trusted Partner Agreement.
    9. The trusted partner access plan will be approved as part of the Trusted Partner Agreement.
    10. Individuals associated with a Trusted Partner Agreement who require identity, authentication, or access beyond that specified in the Trusted Partner Agreement will be processed as a NASA worker in accordance with the requirements of this policy.

# Foreign Nationals

## Overview

* + 1. This chapter outlines the requirements that NASA personnel shall follow in granting foreign nationals access to NASA assets for any purpose. The subsections outline additions and variations to existing processes, procedures, and authorizations necessary to obtain required access permissions in a timely manner. Also included are the requirements for the processing of persons who have multiple citizenships, foreign nationals from designated countries, LPR, and U.S. citizens working for a foreign entity.
    2. This chapter defines the identity management requirements specific to foreign nationals at NASA including, but not limited to, visit coordination, access approval, escort procedures, fingerprint checks, and background investigations for short-term or long-term assignments and visitor access.
    3. The requirements in this chapter shall apply to all foreign national workers and non-NASA workers who require physical and/or logical access to NASA resources; including, but not limited to, foreign nationals supporting a NASA contract, grant, or other agreement issued by NASA, foreign nationals who are civil servants, contractors, subcontractors, researchers, international partners as defined via International Space Act Agreements (ISAA), protocol visitors, foreign nationals with the news media, grantees, and visitors.
    4. Questions regarding the receipt and processing of access requests for foreign nationals and the conduct of approved visits and other access shall be directed to the NASA Center or Component Facility IVC. If the criteria for processing a specific foreign national cannot be accommodated within one of the scenarios documented in this chapter, a waiver request may be submitted to NASA OPS for review and approval (see section 1.3, Waivers and Exceptions of this document).

## NASA Foreign National Access Policy and Related Requirements

* + 1. Foreign national access is determined on a case-by-case basis. All visits and other approved access will be reviewed to ensure the request conforms to Agency and Federal policies and regulations, including U.S. national security, export control, nonproliferation, and foreign policies and regulations.
    2. Record keeping related to tracking foreign national access requests and visits will be accomplished via the NASA IdMAX system.
    3. In accordance with Federal policies and guidelines, NASA resources shall be given to U.S. citizens prior to consideration of foreign nationals.
    4. Assignments and other access for the purpose of implementing a mutually agreed upon program or project will comply with the terms of the NASA/foreign partner program or project agreement; particularly the provisions in the agreement dealing with responsibilities of the parties and the transfer of data and goods.
    5. Discussion or other release of information by NASA personnel to a foreign national during a meeting, visit, or other approved access that does not pertain to an approved program or project or an effort to establish an approved program or project shall be limited to information available or releasable to the general public, i.e., unclassified, non-sensitive, and non-export controlled.
    6. Scientific and Technical Information (STI) that is proposed for release outside of NASA shall be reviewed to ensure it does not contain sensitive information, including Controlled Unclassified Information (CUI), per NPR 2200.2, Requirements for Documentation, Approval, and Dissemination of NASA Scientific and Technical Information.
    7. Visits, assignments, or IT access requests for foreign nationals from nondesignated countries shall be coordinated and implemented at the Center level by the IVC and provided to the Center Export Administrator (CEA) and the OCIO, or designee, for review and recommendation.
    8. Visits, assignments, or IT access requests for foreign nationals from designated countries shall be coordinated initially through the Center IVC and provided to the CEA and OCIO, or designee, for review prior to being forwarded to NASA Headquarters Office of International and Interagency Relations (OIIR), Headquarters Export Administrator (HEA) for review and program points-of-contact, as necessary, for review.
    9. Final approval of visits by foreign nationals from nondesignated and designated countries resides with the IVC upon consideration of the recommendations of the CEA, HEA, OCIO, or designee, and Counterintelligence/Counterterrorism (CI/CT).
    10. A foreign national will be provided access to NASA physical and/or IT assets only after final approval.
    11. An approved foreign national access request will allow access to information that is releasable to the general public. Access requests with the purpose of gathering or sharing information or conducting discussions in areas that NASA considers sensitive (e.g., for proprietary, national security, or export control reasons) shall not be approved in the absence of a specific NASA programmatic interest.
    12. Foreign national identities and associated access permissions will be suspended on the day the foreign national’s affiliation ends.
    13. Identities and access permissions will be terminated the day the affiliation ends for foreign nationals from designated countries and 30 calendar days after affiliation ends for foreign nationals from nondesignated countries.
    14. Centers and/or programs may specify restrictions regarding physical and/or logical access privileges or escort requirements that are more restrictive than those documented in this NPR.
    15. Any violation or suspected violation of this policy shall be reported to the CCPS.

## Enrollment and Issuance Procedures for Foreign Nationals

* + 1. Identity proofing and vetting shall follow the requirements in section 4.7, Identity Proofing and Vetting Requirements.
    2. The enrollment and issuance procedures identified in this section shall be performed in-person at a NASA Center or Facility or a NASA-approved enrollment location. Specific procedures for foreign national visitors and remote-only enrollment and issuance procedures can be found in subsequent sections.
    3. Foreign nationals shall complete the following steps prior to initiation of any on-site enrollment and issuance procedures:

1. Obtain approval for the visit or assignment.
2. Obtain a visa applicable to the purpose of the visit or assignment.
3. Ensure that sponsorship is determined. If a foreign national is not under a contract where a COR has been officially designated, the foreign national will provide information directly to their visit/assignment host, and the host will fulfill the duties of the sponsor as required herein.
4. The foreign national visitor will begin the process 14 calendar days for nondesignated foreign nationals and 30 calendar days for designated foreign nationals so that pre-visit identity proofing and vetting can be conducted and completed by the IVC, as described in this chapter.
   * 1. Step 1: Identity Request
        1. The requester for a foreign national shall be a current PIV or Agency Smart Badge holder. The requester initiates an identity request within IdMAX. Identity information is entered by the requester or the applicant via invitation, as required in IdMAX.
     2. Step 2: Sponsorship
        1. The sponsor validates the applicant’s identity data in the credential request and updates the data as necessary. The sponsor reviews the position designation in IdMAX and will perform a risk-based determination based on the status of the foreign national and the assets that the foreign national is to access. This information is necessary to define the ACP and determine the level of investigation and escort requirements.
     3. Step 3: Foreign National Review
        1. The IVC shall directly receive and review all access requests for foreign nationals. The IVC validates receipt of the request and confirms sponsorship of the request. The IVC performs or facilitates the following reviews and activities, in any order, prior to final approval and authorization, as appropriate.
           1. Access Request Review – The IVC reviews the access request with the project office (requesting organization) and the sponsor to confirm access requirements, work description, dates of visit, assignment or length of access request, visa type and its appropriateness to the assignment and duration, position designation, and the ACP. The request shall be approved or rejected, as appropriate.
           2. Identity proofing and vetting – The IVC performs checks against appropriate databases, in accordance with the identity proofing and vetting requirements in section 4.7, Identity Proofing and Vetting Requirements.
        2. Security Review – The IVC reviews the access request for issues relevant to the Center, determines escort requirements, reviews the ACP, and approves or denies the request, as appropriate. If approved, a level of investigation appropriate to physical and/or IT access requirements, visit type, and length of residence in the U.S. is determined and initiated.
        3. Counterintelligence/Counterterrorism Review – Center and Headquarters CISAs perform name checks for foreign nationals of interest to determine intelligence service and/or terrorism affiliations.
        4. Export Control Review – Foreign national visit requests are reviewed by the CEA to ensure information being exchanged and access being granted does not violate export control laws. Further review is conducted by Headquarters Export Control if the foreign national is from a designated country, an intern, or part of the NASA Exchange Visitor Program. A recommendation to approve or deny the access request is made based on export control concerns related to any access being granted or information being shared. No additional identity proofing and vetting shall be required or performed during the export control review process.
     4. Step 4: Authorization
        1. The IVC shall confirm receipt of all reviews and provide final authorization of the access request.
        2. The IVC shall report the terms and conditions of the visit, as contained in the ACP and export control provisos, to the sponsor.
        3. If a foreign national is denied access (all or in part), the IVC shall inform the sponsor who may request a further review with the CCPS.
     5. Step 5: Enrollment Process
        1. The enrollment official validates receipt of the request from the authorizer and follows the enrollment procedures in section 3.3.6, Step 4: Enrollment Process, with the following variation:
        2. Authorization Documents – The enrollment official obtains legible scanned copies of the following visit authorization and admission documents:
5. Visa or Electronic System for Travel Authorization (ESTA) receipt for visa waivers. Visit authorization documents validate the type of visit and the type of work allowed. Expired visit authorization documents will be accepted as proof of visit authorization when accompanied by an unexpired admission document.
6. Admission stamp or paper Form I-94, Arrival/Departure Record, with Admitted-Until Date or “D/S” (duration of status). Admission documents validate admission to the U.S. and the length of time a foreign national may remain in the U.S. The I-94 or receipts (e.g., I-797) with a stated Admitted-Until Date, “D/S” or a specified extension (e.g., 180 days) will be accepted.
   * 1. Step 6: Credentialing Determination
        1. Credentialing determinations follows the procedures in section 3.3.7, Step 5: Authorization, of this NPR, in accordance with the identity proofing and vetting requirements in section 4.7, Identity Proofing and Vetting Requirements for Foreign Nationals.**Error! No bookmark name given.**
     2. Step 7: Credential Production and Issuance
        1. Credential production and issuance follow the procedures described in sections 3.3.8, Step 6: Credential Production, and 3.3.9, Step 7: Issuance Process, of this NPR.
     3. Step 8: NAMS Access Request
        1. If accessing NASA physical assets IT resources, access requests will be reviewed by the asset owner/approver who shall approve the request in NAMS, as appropriate.

## Enrollment and Issuance Procedures for Foreign National Visitors

* + 1. Foreign national visitors shall follow all procedures established in section 3.4, Visitor Enrollment and Issuance Procedures with the following modifications:
    2. Foreign national visitors who are minors, children, or infants shall be required to present their passport while in the presence of their parent or guardian.

1. The identity request shall be initiated and completed in IdMAX prior to being submitted to EVAMS by the IVC.
2. The IVC shall perform the role of authorizer for all access requests for foreign national visitors.
3. Authorization shall require completion of reviews conducted in accordance with the requirements in section 4.3.6, Step 3: Foreign National Review.
4. Identity proofing and vetting shall follow the requirements in section 4.7, Identity Proofing and Vetting Requirements.

## Remote Enrollment and Issuance Procedures for Foreign Nationals

* + 1. Any foreign national completing remote identity proofing who subsequently visits a NASA Center or Facility shall undergo enrollment following the requirements in section 4.3, Enrollment and Issuance Procedures for Foreign Nationals.
    2. The remote identity proofing and issuance procedures for foreign nationals will follow the requirements in section 3.5, Remote Enrollment Procedures with the following variations:

1. The IVC shall perform the role of authorizer for all remote-only access requests by foreign nationals.
2. Authorization shall include reviews conducted by the CEA, OIIR, OCIO, or designee, and CI/CT as appropriate, in accordance with the requirements in section 4.3.6, Step 3: Foreign National Review.
3. Identity proofing and vetting shall follow the requirements in section 4.7, Identity Proofing and Vetting Requirements.
4. Credential production and issuance will result in the issuance of a logical-only credential.

## Implementation

* + 1. If an identity application for a foreign national from a nondesignated country has been outstanding for longer than 10 working days from the initial request, the IVC should follow up with Center or Headquarters personnel to determine the cause(s) for the delay. Applications for foreign nationals from nondesignated countries outstanding for longer than 15 working days from the initial request may be approved by the IVC and escalated to the AIMO for awareness. For foreign nationals from designated countries, no follow ups or approvals based on outstanding approval timelines will be performed.
    2. The IVC may, in emergent situations and with approval of the CCPS, process an approval without review by other offices. In such situations, reviews by other offices should be reviewed immediately upon completion and the visit approval updated as appropriate.
    3. Program sponsors and hosts shall ensure that foreign nationals are aware and/or briefed on the terms and conditions of the visit, as contained in the ACP and export control provisos.

## Identity Proofing and Vetting Requirements for Foreign Nationals

* + 1. Centers shall accept as valid the identity proofing and vetting of their peer Centers as a baseline requirement, consistent with this NPR. Additional identity proofing and vetting may be required if access requirements exceed the original scope of access or authorization.
    2. All foreign nationals requiring access shall provide the minimum required identity data and PII necessary to establish an identity including, but not limited to, name, contact information, address, place of birth, citizenship, and contact information.
    3. A primary and secondary NASA-approved identity source document shall be required, unless otherwise specified.
    4. All foreign national access requests shall require completion of a database check of Visual Compliance, which includes a check against the Visual Compliance Unverified List, Entities List, Denied Persons List, Debarred Parties List, Specially Designated Nationals, and the Terrorist Screening database. The Visual Compliance check will be uploaded to the identity record of the foreign national when derogatory information is reported. Results with no derogatory information are not required to be uploaded to the identity record.
    5. For foreign nationals requiring logical-only access to very-low data or requiring logical-only access to low or moderate data for which OPS, OIIR, and OCIO-approved risk-mitigations are in place and who are outside the U.S., no additional checks and no visit authorization or admission documents will be required. A database check of the U.S. Customs and Immigration Service (USCIS) Systematic Alien Verification for Entitlements (SAVE) will not be required.
    6. For foreign nationals performing short-term or long-term assignments requiring escorted or unescorted physical access or requiring logical access and who are inside the U.S., the following shall be required:

1. Initiation of a database check of SAVE to confirm reciprocity of vetting performed by Customs and Border Patrol at the port of entry. The SAVE check should be completed within 5 days of the start of any short-term or long-term assignment.
2. Completion of an NCHC, in accordance with NPR 1600.3 and section 3.3.6.3 of this NPR.
3. Completion of an FBI Investigations File (name check search) as deemed necessary by CI/CT.
   * 1. For foreign national visitors, a valid passport or Department of State Diplomatic ID Card will be required. No additional checks or documentation are required.
     2. Access requests for foreign nationals shall be denied if the NCHC or Visual Compliance check produces any positive hit result. Positive hit results are to be reported to the CCPS and the HEA. Exceptions to this denial of access are granted in cases where the positive result in the Visual Compliance check can be effectively mitigated by an applicable proviso approved by the HEA.
     3. Access requests for foreign nationals shall be denied or terminated if the SAVE check verification process reports an invalid immigration status or any information, such as visa type, which conflicts with the purpose of the visit.
     4. Foreign nationals requiring a PIV shall be subject to 3-years residency within the U.S. and eligibility requirements for a background investigation.
        1. For foreign nationals who have resided in the U.S. or a U.S. territory for three years or more, a background investigation (i.e., Tier I background investigation or higher) will be initiated after employment authorization is appropriately verified. Foreign nationals may be eligible for issuance of a NASA PIV credential upon favorable adjudication of a Tier I investigation or higher with a favorable credentialing determination. In the event a foreign national chooses not to complete the appropriate forms for a background investigation required for full identity proofing and vetting, the Center Protective Services Office will require completion and a minimum annual revalidation of the NCHC, FBI Investigations File, Visual Compliance, and SAVE checks prior to issuance of an Agency Smart Badge or Center-specific badge, based on risk determination.
        2. For foreign nationals who have resided in the U.S. or a U.S. territory for less than three years, the background investigation shall be delayed until the three-year requirement is met. In such cases, the Center Protective Services Office will require completion of the NCHC, FBI Investigations File, Visual Compliance, and SAVE checks prior to issuance of an Agency Smart Badge or Center-specific badge, based on risk determination.
        3. Three years residing in the U.S. is defined as any presence in the U.S. or a U.S. territory for three continuous years or more during which any absences can be regarded as temporary and do not destroy the degree of continuity necessary to establish and maintain residence. Decisions about whether a person maintains continuity of residency are based on the circumstances of the particular case and at the discretion of the CCPS in consultation with the AIMO and the OPS Personnel Security Division.
     5. Derogatory results of any database check shall be attached to the identity record of the foreign national in IdMAX. Results with no derogatory information are not required to be uploaded to the identity record.

## Foreign National Escort Requirements

* + 1. The CCPS may immediately suspend or revoke a person’s escort authority if a violation or suspected violation occurs.
    2. In addition to requirements in this section, personnel escorting Foreign Nationals shall comply with Escort Responsibilities outlined in Section 2.3.14 of this NPR.
    3. The IVC shall work with the CEA, program managers, and sponsor to determine escort requirements while the foreign national is located at the Center.
    4. The AIMO will develop and maintain an escort-training module in SATERN that includes Center-specific escort requirements provided by the Center Protective Services Office. The Center Protective Services Office will develop escort training content specific to that Center and provide it to the AIMO for inclusion in the agency escort training.
    5. Employees shall report any violations of the ACP or suspicious activity to the Center IVC and the Center Counterintelligence Office.
    6. Sponsors, hosts, and escorts shall acknowledge understanding and acceptance of the ACP and escort requirements associated with each escorted individual, prior to the beginning of the visit/assignment.
    7. A decision to require additional escort requirements, remove escorting credentials, or changing escort ratios may be changed at the discretion of the CCPS and in accordance with this policy. Any changes to escort requirements shall be coordinated by the IVC and annotated in IdMAX. The CCPS shall coordinate any changes to designated country foreign national escort requirements with the AIMO to request waiver.
    8. For protocol visits, the responsible protocol visit host shall coordinate with the CCPS to determine the escort-to-visitor ratio.
    9. Determining Escort Requirements for nondesignated country Foreign Nationals
       1. Foreign nationals from nondesignated countries with a completed NCHC may be unescorted, at the discretion of the CCPS.
       2. The CCPS shall establish Center Security guidance to determine the escort-to-visitor ratio for foreign nationals from nondesignated countries or utilize a 1:5 ratio as a baseline requirement.
       3. Foreign nationals from nondesignated countries with a Tier 1 or higher background investigation may be allowed to escort other foreign nationals in the same program but may not escort foreign nationals from other programs or foreign nationals from designated countries even in the same program.
    10. Determining Escort Requirements for designated country Foreign Nationals
        1. Foreign nationals from designated countries shall be escorted at all times. Foreign nationals from designated countries who have undergone a Tier 1 or higher background may be exempted from the requirement to be escorted, at the discretion of the CCPS.
        2. Foreign nationals from designated countries shall not be allowed to perform duties as an escort.
        3. One escort shall be assigned to each foreign national from a designated country so that an escort-to-visitor ratio of 1:1 is maintained.  In coordination with the IVC, the CCPS may, for specific situations and after ensuring adequate and continuous supervision and no undue risk to NASA, adjust the escort-to-visitor ratio for foreign nationals from designated countries to 1:5.
        4. Per NPR 1660.1, NASA Counterintelligence and Counterterrorism, escorts of foreign nationals from designated countries shall complete a briefing with a Center CISA prior to the visit as well as an in-person debriefing with a Center CISA following the visit.

## Requirements for Visas

* + 1. Foreign national visitors shall not be required to provide a visa.
    2. Foreign nationals requiring remote-only access outside the U.S. shall not be required to provide a visa.
    3. All foreign nationals requiring physical or logical access to NASA inside the U.S. to perform work shall provide a valid visa. Expired visas are considered valid and will be accepted.
       1. The visa type shall match the description of the work being performed. Foreign national access will be denied if the work description and visa do not match.
       2. Foreign nationals performing work for NASA through an affiliate entity (e.g., contracting company, educational institute, etc.) shall provide a visa that substantiates the foreign national’s relationship with the affiliate entity and is applicable to the work being performed at NASA (e.g., educational visa when affiliated with an educational institute and supporting the educational institute’s work agreement with NASA). Foreign national access will be denied if the foreign national’s visa does not match the relationship with the affiliate or the work being performed at NASA.
       3. Foreign nationals requiring access to NASA to perform work on an asset owned or provided by a foreign entity (e.g., Canadian working on the Canadian Space Arm) shall provide a visa but the visa is not required to match the description of work. Visa waivers may be accepted in these situations.
    4. Visa waivers shall only be accepted in compliance with Department of State guidelines for use of a visa waiver; specifically:

1. The duration of the assignment shall be 90 days or less.
2. The work description shall be an activity permitted on a Visitor (B) Visa.
   * + 1. When a foreign national with a visa waiver needs to stay in the U.S. beyond the 90 days authorized by the visa waiver, the foreign national is required to either depart and re-enter the U.S. on a new visa waiver or obtain a full visa in accordance with USCIS requirements. Any new visa information will be provided to the Center IVC who will verify the visa information in SAVE.

## Requirements Based on Affiliation

* + 1. Foreign nationals shall not be processed until they have been associated to a legally-binding agreement that has been entered into IdMAX.
    2. If a foreign national will need access to NASA as a visitor (29 days or less in a single visit or cumulative during a 365-day period) the foreign national shall be granted escorted physical access and logical access only to the NASA visitor network via the Agency-managed wi-fi-portal. Visitors will be assigned to the Agency foreign national visitor agreement.
    3. If a foreign national is supporting NASA under an ISAA and requires periodic access to NASA facilities, the foreign national shall be processed in accordance with procedures in section 4.3, Enrollment and Issuance Procedures for Foreign Nationals. An ISAA, or other legally binding agreement (e.g., contract, grant, etc.), shall be required for any short-term or long-term assignment.
    4. If a foreign national will need access to NASA periodically as an accredited news media representative, the IVC shall coordinate with the Center public affairs office to obtain requisite information. Once the IVC has determined an agreement has been reached on requirements, the IVC will coordinate with the CCPS as to the level of investigation required. The foreign national will be given a physical access credential (Agency Smart Badge or Center-specific badge) commensurate with the level of investigation performed and access requirements. Investigation status information will be updated annually.
    5. Protocol Visits (formerly High-Level Protocol Visits)
       1. All protocol visits shall be sponsored by OIIR or the Center protocol office or equivalent office or organization at the Center. OIIR and the Center protocol office may, at their discretion, choose to implement additional requirements for a protocol visit.
       2. Protocol visits shall be processed as expeditiously as possible, in accordance with the requirements of this policy for processing foreign nationals.
       3. Foreign national diplomats and other important foreign national persons not sponsored by OIIR or the Center protocol office shall follow the procedures and requirements established in this NPR with no additional considerations for expedition.
    6. J-1 Exchange Visitor Visa.
       1. Under the provisions of 22 CFR Part 62, and as approved by the Department of State, NASA is authorized to conduct an exchange visitor program and can authorize foreign nationals to be assigned to NASA installations on J-1 exchange visitor visas. NASA has authority to sponsor two exchange visitor categories: Research Scholars and Foreign Government Visitors. The regulations regarding these categories and the exchange visitor program in general can be found at 22 CFR 62.1 through 62.90.
       2. If a foreign national is visiting NASA as part of the NASA Exchange Visitor Program (J-1 Visa), the IVC shall coordinate with the sponsor to obtain requisite information and to ensure that the foreign national is part of an existing ISAA partnership.
       3. For a foreign national to be considered for the NASA Exchange Visitor Program, the host Center or Component Facility shall document its request (with appropriate justification) in a memo to the cognizant Mission Directorate or Mission Support Office at NASA Headquarters with a copy to the Export Control and Interagency Liaison Division, OIIR, and, in parallel, contact the IVC to enter the request for review. If the Headquarters Office endorses the request, OIIR will review for final approval. If approved in principle, OIIR will prepare an ISAA between NASA Headquarters and the foreign sponsoring entity (e.g., foreign space agency or foreign university) and, once executed, if all requirements associated with authorizing a J-1 Visa have been satisfied, the authorization will be issued, covering the period of the approved assignment.
       4. No NASA funding is provided to the foreign national under the NASA Exchange Visitor Program. All funding shall come from the foreign sponsor or from personal funds, and NASA will assess if the funds available are sufficient to sustain the individual for the period of the assignment. NASA provides office space and supplies and, if necessary and approved pursuant to NASA policies, computer and network access. The period of assignment for approved foreign national participants is generally from six months to three years. Foreign nationals from designated countries and all foreign national undergraduate students are ineligible for participation in the NASA Exchange Visitor Program.
    7. Foreign National Interns
       1. Foreign national interns shall only be allowed access to NASA facilities for 30 days or more if their presence is in support of a cooperative activity conducted under an ISAA, or a domestic SAA, contract, grant, or cooperative agreement with a U.S. institution. Foreign national interns may only support a NASA internship program approved by OIIR and the Office of Education.
       2. Access to NASA facilities and information systems by foreign national interns, for any amount of time, shall be subject to the same restrictions that apply to other foreign nationals.
       3. Foreign national interns shall be recorded in IdMAX and identified based on their educational status (e.g., undergraduate, graduate, etc.).

## Requirements Based on Visitor Attributes

* + 1. Dual Citizenship.
       1. If the foreign national has dual citizenship with the U.S. and a foreign country (including designated countries), identity proofing and vetting shall follow the processes for a U.S. citizen. Any physical access restrictions will be determined and agreed to by the CCPS and the sponsor/host.
       2. If the foreign national has dual citizenship for two foreign countries and one or both of those countries is a designated country, the identity shall be vetted as a foreign national from a designated country.
    2. Foreign nationals born in a designated country shall be identity vetted and credentialed as a foreign national from a designated country. Foreign nationals from countries designated by the Secretary of State as sponsors of terrorism are generally not eligible for access to NASA facilities pending review by OIIR and in accordance with the requirements of section 4.2.8.
    3. U.S. citizens employed by a foreign entity shall be treated as U.S. citizens for the purpose of identity proofing and vetting.
    4. U.S. persons, Lawful Permanent Residents (LPR) and protected individuals shall be treated as U.S. citizens for the purposes of identity proofing and vetting, granting of access, and escort requirements with the following exceptions:
       1. During identity proofing and vetting, LPRs shall be required to present a valid Permanent Resident Card (PRC) or Alien Registration Receipt Card (ARRC) (Form I-551), commonly known as a Green Card, to verify and establish LPR status. The Green Card will be verified through a SAVE check or other electronic verification.
       2. LPRs shall be issued credentials that identify them as an LPR with the same expiration date requirements as a U.S. citizen.

## Requirements Based on Credential Type

* + 1. Foreign nationals shall not be issued a PIV credential by default unless issuance of the PIV supports the foreign national’s access requirements.
    2. Except as noted below, all credentials issued to foreign nationals shall meet the requirements identified in Chapter 5, NASA Credentials.
    3. The expiration date of Agency Smart Badges issued to foreign nationals shall be set for a period not to exceed the earlier of three years from the card production request (CPR) generation date, agreement end date, or assignment end date. The CCPS may make a risk-based determination to issue Agency Smart Badges to foreign nationals with a three-year expiration based on his or her evaluation of relevant local conditions.
    4. Final authority for decisions regarding expiration dates shall rest with the IVC.

## Access Control Plans, Technology Transfer Control Plans, and Access Provisioning

* + 1. The sponsor and/or host shall ensure the foreign national understands any terms and conditions of the visit, as contained in the Access Control Plan (ACP) and/or Technology Transfer Control Plan (TTCP) in addition to the provisos and other restrictions of the visit listed in IdMAX.
    2. TTCPs will be managed in accordance with the requirements of NPR 2190.1, NASA Export Control Program and may be included as part of a foreign national’s identity record.
    3. TTCPs will be made available to the IVC, requester, host, or sponsor upon request.
    4. The ACP included in each foreign national’s identity record will identify all assets the foreign national may access.
    5. Access shall only be granted to vetted foreign nationals from designated and nondesignated countries consistent with the ACP and/or TTCP.
    6. The decision to grant physical and/or logical access to foreign nationals to NASA’s restricted areas, NASA critical infrastructure (NCI), personally identifiable information, sensitive or classified information, export-controlled data, and/or other restricted assets may require a higher level of identity proofing and vetting and/or additional access requirements due to the heightened risk of exposing these areas and data.
       1. Access requirements established by this NPR and other cognizant NPRs shall not preclude additional requirements regarding access to the Center, buildings, or other secured areas.

## Onsite, Offsite, and Virtual Meetings

* + 1. NASA conducts virtual and in-person meetings throughout the world in support of Space Act Agreements and International Partnerships or in support of establishing such agreements and partnerships. Meetings in support of these agreements and partnerships shall follow the requirements of this section.
    2. Participants in meetings will be identity proofed and vetted only to the degree required to be granted access and/or authorization to the facility, materials and information being discussed and shared in the meeting.
    3. Meetings, and known attendees, should be coordinated with the IVC, CEA, and CI/CT to the extent possible.
    4. In accordance with NPR 2200.2, the materials being presented at any meeting shall be reviewed and approved prior to the meeting to ensure compliance with export laws and regulations. It is the responsibility of the individual presenting the materials to ensure the materials have been reviewed and all participants in the meeting have been granted access and/or authorization to view the materials being presented.
    5. Meetings held which violate NASA policies related to foreign nationals will be treated as a violation of security requirements, per NPR 1600.1, and shall be reported as a security incident to the CCPS and the CEA.

## Visiting Center Request

* + 1. Foreign nationals shall be assigned a primary Center and granted access to the primary Center. The credential issued to the foreign national will specify the primary Center to which access is allowed.
    2. Access to Centers other than the primary Center shall not be allowed until a Foreign National Visiting Center request has been completed. The request will be reviewed and approved by the foreign national’s sponsor and/or host and the visiting Center’s IVC and CEA prior to the visit.
    3. Foreign National Visiting Center Requests shall be submitted 5 calendar days prior to the visit to allow sufficient time to review the request. Requests submitted less than 5 calendar days prior to the visit may not be approved.
    4. Foreign nationals issued NASA PIV Smartcards shall complete a Foreign National Visiting Center Request prior to visiting another NASA Center or facility.
    5. Centers approving Foreign National Visiting Center requests shall accept the identity proofing performed by another Center. Documentation authorizing the visit should be reviewed and updated as necessary to ensure affiliation and work authorization status is valid.
    6. Centers shall not modify the home Center when approving a Foreign National Visiting Center request.
    7. The Foreign National Visiting Center Request shall be reviewed by the Center IVC and CEA

## Annual Review

* + 1. All foreign nationals shall undergo an annual review that will include updates of identity information, access needs, identity source documentation, and investigation and database checks.
    2. The annual review date shall be based on the date the identity was authorized by the IVC. Annual reviews will be initiated within 1 year of the previous authorization date and submitted to the IVC for authorization no later than 10 days prior to 1 year from the previous authorization date or access may be suspended.
    3. Identity requesters shall monitor the annual review dates for foreign nationals under their purview and initiate annual reviews for those foreign nationals. The identity requester will coordinate with the foreign national to review all biographical information, upload any new identity documentation, and review provisioned assets. The identity requester will coordinate the annual review with the host and sponsor to verify work description and related information. The identity requester will notify the IVC the foreign national identity is ready for annual review.
    4. The annual review shall be approved by the foreign national’s sponsor and/or host and the IVC and CEA.
    5. SAVE checks shall be performed annually to determine continued positive standing of the foreign national. Visual Compliance checks are continuously run against the Visual Compliance database and negative results should be reviewed as they are received.
    6. NCHCs shall be run every 3 years or when a new credential is issued to the foreign national.

## Requirements for Logical Access

* + - 1. Foreign nationals with logical access shall be given access credentials commensurate with the level of identity proofing and vetting performed and the authentication requirements for access.
    1. Foreign national “limited privileged” access to IT systems shall be allowed only if the foreign national is onsite at a NASA Center, involved in a program under an ISAA, and the foreign national’s ACP and TTCP include that access. Notification of such access will be provided to the OCIO, or designee.. The sponsor will verify that an ISAA, ACP, and TTCP are in place and has accountability for ensuring the security of IT system data being accessed by the foreign national.
    2. Any foreign national having access to NASA logical assets shall provide a written certification that they fully understand and will adhere to NASA rules and regulations regarding the integrity and confidentiality of NASA data being accessed. This certification may be a completed NASA IT Security Training or a signed document signaling understanding of IT access requirements as outlined in NPR 2810.1. Either of these activities will satisfy the completion of the NASA IT Security Training requirement prior to the activation of IT access. Recertification will be required in accordance with NPR 2810.1.

# NASA Credentials

## Types of NASA Credentials

* + 1. NASA issues PIV Smartcards, Agency Smart Badges, Center-specific badges, and visitor passes (collectively referred to as NASA credentials). PIV Smartcards and Agency Smart Badges allow physical and/or logical access to NASA assets. Center-specific badges allow physical access to NASA assets and do not allow logical access. Visitor Passes validate a visit request but require presentation of a primary identity source document prior to being granted physical access.
    2. Logical-only access credentials and their usage are addressed by NPR 2841.1 and include, but are not limited to, username and password, hard tokens, and digital certificates.
    3. Each NASA credential or logical-only credential shall be bound to an established identity and undergo the appropriate registration, enrollment, and issuance process for that specific credential.
    4. All NASA credential templates shall be approved by the AIMO prior to their creation and utilization.
    5. NASA credentials shall be created utilizing the ICAM infrastructure, in compliance with NPR 2841.1 and this NPR.
    6. Persons holding a Federal PIV credential issued by another Federal entity or CAC issued by DoD and requiring access to NASA shall register their non-NASA PIV or CAC in the IdMAX system. If the non-NASA PIV or CAC does not work (i.e., unable to authenticate electronically) at the NASA Center and/or cannot be registered in IdMAX, an Agency Smart Badge may be issued to the individual to supplement their non-NASA PIV or CAC.

## NASA PIV Smartcard

* + 1. NASA PIV Smartcards shall be required for all NASA workers who have been deemed as needing routine and regular physical only, logical only, or both physical and logical access to NASA Centers, facilities, and IT systems and resources for a period exceeding 179 calendar days (beginning the first day of affiliation, regardless of work schedule) in a 365-day period and to whom issuance of a PIV does not represent a greater risk (e.g., interns affiliated for 180 days or more who have been submitted for an investigation but have no need for a PIV; individuals who do not need access to other NASA Centers or Federal facilities; additional cases as approved by the AIMO). The 179-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. N.ASA PIV Smartcards will be issued to United States (U.S.) citizens and may be issued to foreign nationals.
    2. NASA PIV Smartcards shall be issued following the identity proofing, registration, and issuance processes defined in this document.
    3. NASA PIV Smartcards shall be issued only after favorable adjudication of an NCHC (also referred to as a fingerprint check) and submission of a background investigation, which will be a Tier I background investigation, at a minimum. Continued possession of the PIV Smartcard will be determined based on a credentialing determination of the returned background investigation.
    4. NASA PIV Smartcards shall have an expiration date set for a period of five and a half (5.5) years from the Card Production Request (CPR) generation date.
    5. NASA PIV Smartcards shall be accepted at all Centers for access to public areas within the NASA perimeter.
    6. NASA PIV Smartcards shall not be issued to individuals holding a Federal PIV credential issued by another Federal entity or CAC issued by DoD. 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.
    7. Physical Characteristics - The information on a NASA PIV credential exists in both visual printed and electronic forms. The NASA PIV credential shall be equipped with technologies that allow for physical access and logical access.

1. NASA PIV credentials contain the following security and distinguishable features on the front of the card:
   1. Holographic overlay.
   2. Smart chip.
2. NASA PIV credentials have the following printed in a vertical orientation on the front of the badge.
   1. The photograph of the applicant in the top left corner.
   2. The legal name of the applicant printed below the applicant photograph.
   3. Two badge expiration dates, one located in the upper right corner (MMM YYYY format) and the second to the right of the applicant photograph, below the Agency identifier and over the Agency logo (YYYYMMMDD format).
   4. The NASA Agency identifier logo, to the right of the applicant photograph and behind the affiliation, badge expiration, and NASA Agency identifier.
   5. The affiliation of the applicant, to the right of the applicant photograph and over the Agency logo.
   6. The NASA Agency identifier, to the right of the applicant photograph, below the affiliation, and over the Agency logo.
   7. The unique badge identification number, consisting of a three-digit Center code plus six unique digits, printed below the NASA Agency identifier and the affiliation color band.
   8. Solid color band, with an alphanumeric color indicator, across the middle of the badge, over the full name with the color determined by the affiliation of the badge holder.
3. NASA PIV credentials have the following printed horizontally on the back of the badge:
   1. The statement: “This credential is the property of the U.S. Government. Counterfeiting, altering, or misusing violates Section 499, Title 18 of the U.S. Code.”
   2. Return address.
   3. Applicant height.
   4. Applicant eye color.
   5. Applicant hair color.
   6. A 3x9 bar code of the unique badge identifier.
   7. Preprinted Agency card serial number.
   8. The PCI identification number consisting of a six-character department code, the Agency code for NASA, and a five-digit PIF number.

## Agency Smart Badge

* + 1. Agency Smart Badges are PIV-interoperable smartcards equipped with technologies that allow for physical and/or logical access that may be issued to any person who does not meet the requirements for a PIV (PIV-ineligible) and who needs unescorted access to a NASA Center and/or access to a NASA IT system. This includes NASA workers not exceeding the 179 day requirement, applicants awaiting their PIV, tenants on NASA Centers, foreign nationals in the U.S. for less than 3 years, foreign nationals unable to complete the Tier I investigation requirement, and individuals to whom issuance of a PIV represents a greater risk (e.g., interns affiliated for 180 days or more who have been submitted for an investigation but have no need for a PIV; individuals who do not need access to other NASA Centers or Federal facilities, additional cases as approved by the AIMO).
    2. Agency Smart Badges shall be issued following the identity proofing, registration, and issuance processes defined in this document.
    3. Agency Smart Badges shall be issued only after favorable adjudication of a completed NCHC.
    4. Agency Smart Badges shall have an expiration date set for a period not to exceed three years from the Card Production Request (CPR) generation date.
    5. The default expiration date of an Agency Smart Badge shall be 3 years.
    6. Agency Smart Badges shall only allow access to the Center at which they were issued.
    7. Agency Smart Badges issued for logical access only shall not be accepted for physical access to Centers.
    8. Physical Characteristics - Agency Smart Badges shall be printed horizontally so as not to be confused with or resemble the NASA PIV credential.

1. NASA Agency Smart Badges contain the following security and distinguishable features on the front of the card:
   1. Holographic overlay.
   2. Smart chip.
2. Agency Smart Badges will have the following printed in a horizontal orientation on the front of the badge:
   1. The photograph of the applicant in the top left corner.
   2. The legal name of the applicant printed below the applicant photograph.
   3. The NASA Agency identifier logo in the center of the badge.
   4. Two badge expiration dates, one located above the NASA Agency identifier (MMDDYYYY format) and one above the Agency logo (MMM YYYY format).
   5. The designation of the issuing Center, on the right side, below the smartcard chip.
   6. The unique badge identification number, above the NASA Agency identifier.
   7. Solid colored affiliation color band on the bottom of the badge based on the affiliation of the badge holder.
   8. The affiliation of the applicant, in the center of the solid colored affiliation color band.
3. Agency Smart Badges have the following printed horizontally on the back of the card:
   1. The statement: “This credential is the property of the U.S. Government. Counterfeiting, altering, or misusing violates Section 499, Title 18 of the U.S. Code.”
   2. Return address.
   3. Applicant height.
   4. Applicant eye color.
   5. Applicant hair color.
   6. A 3x9 bar code of the unique badge identifier.
   7. Preprinted Agency card serial number.
   8. The PCI identification number consisting of a six-character department code, the Agency code for NASA, and a five-digit issuing facility number.

## Center-Specific Badges

* + 1. Center-specific badges shall allow physical-only access to the issuing NASA Center.
    2. Center-specific badges may, at the discretion of the CCPS and based on a risk-based determination, documented as part of the permanent record, be issued to any person who needs non-electronic physical access to a NASA Center, does not need logical access, and does not qualify for a NASA PIV Smartcard or Agency Smart Badge. This may include seasonal interns, volunteers, construction workers, and others as approved by the AIMO. Escort requirements for individuals with a Center-specific badge will be included in the risk-determination made by the CCPS.
    3. Center-specific badges shall be issued following the identity proofing, registration, and issuance processes defined in this document.
    4. Center-specific badges shall be issued only after favorable review of an NCHC, at a minimum.
    5. Center-specific badges shall have an expiration set for a period not to exceed the earlier of the agreement end date or 3 years from the date of issuance.
    6. Center-specific badges shall only allow access to the Center at which they were issued.
    7. Physical Characteristics – Center-Specific Badges shall be printed vertically and with design characteristics which do not cause confusion with or resemble the NASA PIV smartcard or Agency Smart Badge.

1. The photograph of the applicant.
2. The legal name of the applicant.
3. The name of the issuing Center (Center name may be common abbreviation, e.g., ARC, AFRC, etc., as appropriate).
4. The full badge expiration date if the badge will be used for physical access.

## Visitor Passes

* + 1. Visitor passes shall allow non-electronic physical-only access to the issuing NASA Center when presented along with a NASA-approved identity source document.
    2. NASA visitor passes may be issued to visitors requiring non-electronic, escorted physical-only access to a NASA Center.
    3. Visitor passes shall be issued only after review and inspection of a primary NASA-approved identity source document. A second NASA-approved identity source document may be required at the discretion of the CCPS.
    4. Visitor passes may be issued without fingerprint capture.
    5. Centers may require additional vetting (e.g., NCIC or NCHC) prior to issuance of a visitor pass.
    6. Visitor passes shall have an expiration set for a period not to exceed 29 days from the date of issuance.
    7. Visitor passes shall only allow access to the Center at which they were issued.
    8. Physical Characteristics – Visitor passes shall not be printed to resemble the NASA PIV smartcard or Agency Smart Badge. Visitor passes will utilize an Agency template from EVAMS and contain the following as minimum criteria:

1. The legal name of the applicant.
2. The full name of the issuing Center.
3. The full badge expiration date.

## Derived PIV Credentials

* + 1. The Derived PIV Credential is an additional common identity credential under Homeland Security Presidential Directive-12 and Federal Information Processing Standards (FIPS) 201 that is issued by NASA, primarily for mobile authentication.
    2. Derived credentials shall be issued by NASA following the processes established in FIPS 201 and NPR 2841.1, or other NPR established by the OCIO for derived credentials.

## Additional Characteristics

* + 1. Visual Color Coding for Affiliation Type - NASA PIV and Agency Smart Badges shall use colored markings on the badge to identify the affiliation of the badge holder. NASA PIV credentials use a color band through the name of the applicant, and Agency Smart Badges use a band on the bottom of the credential and include the affiliation. The band will include a single capital letter identifying the color in the band (e.g., “G” for green), located within a white circle with a black outline on the right of the band. The purpose of the letter is to assist individuals with visual impairment in recognizing the color.
    2. Contractors at NASA JPL who are U.S. citizens shall have a solid silver color below the green contractor color band.
    3. IPA employees shall include the label “IPA” in black letters on the front of the badge.
    4. Press corps and media shall include the label “PRESS” printed vertically down the right side of the Agency Smart Badge or Center-specific badge.
    5. Emergency Response Officials (ERO) Credentials
       1. The ERO designation shall only be applied to NASA PIV credentials.
       2. ERO credentials shall contain a red strip containing the words “Emergency Response Official” at the bottom of the badge.
       3. ERO credentials shall include, on the back of the credential, text stating “After credential verification, the EMERGENCY RESPONSE OFFICIAL should be given access to controlled areas.”
       4. ERO credentials shall only be issued to those individuals performing a role identified in NPR 8715.2, NASA Emergency Management Program Procedural Requirements. These roles include, but are not limited to, Center and facility emergency and disaster response personnel, NASA and OIG sworn law enforcement officials, Continuity of Operations (COOP) personnel, Continuity of Governance (COG) personnel, and personnel in the Emergency Relocation Group (ERG), and personnel deployed to support the NASA National Response Framework (NRF) Emergency Support Function (ESF) Annexes.
       5. ERO credentials shall only be issued to those individuals who have completed the requisite training established for that specific role in NPR 8715.2.
    6. Foreign National Credentials
       1. Foreign national badge characteristics shall take precedence over all other affiliation characteristics.
       2. Foreign national badges shall have a light blue color border around the applicant photo.
       3. Foreign nationals requiring escort will be recognized by red lettered “ESCORT ONLY” across the middle of the badge.
       4. International Partners shall have a flag of the applicant’s country of citizenship in the lower right corner of the badge.

## Digital Characteristics

* + 1. The digital data stored on the NASA credential supports physical and/or logical access use, encryption, and signing capability and provides security and authentication protection for the credential and credential holder.
       1. Card Holder Unique Identifier (CHUID) - The CHUID is used by access control applications and is the only data that is accessible through both the contact and contactless interfaces. Applications can read this data without any action from the badge holder. The CHUID is composed of the following data elements which shall not be modified during post-issuance updates:

1. Federal Agency Smart Credential Number (FASC-N).
2. NASA Agency code.
3. System code identifying the original issuing Center.
4. A credential number.
5. Credential holder’s Uniform Universal Personal Identification Code (UUPIC).
6. Expiration date.
   * + 1. Digital certificates for card authorization key (CAK), authentication, signing, and encryption are encoded to the smartcard in accordance with FIPS 201 and FIPS 140.
       2. Biometrics (typically fingerprints of the right and left index fingers) are stored as minutiae templates that represent a specific biometric but cannot be reverse engineered to recreate an image of that biometric.
       3. Digital Representation of Printed Information - Certain items printed on the front and back of the card are stored on the smartcard as a security and authentication measure, including name, affiliation, organization, badge expiration date, Agency card serial number, and issuer identification.
       4. Photograph - The facial image used in creating the photo printed on the front of the badge is stored in the badge. A facial image is required, and obscuring headwear may not be worn for the photograph.
       5. The PIN is used to secure and protect the electronic data stored on the PIV credential. The PIN is used by the PIV credential holder to allow applications to access data and as part of the authentication process. It is stored in a secure section of the smart card, separate from the rest of the PIV credential digital data. All PIV credential data, with the exception of the CHUID, require the PIV credential holder to enter their PIN before an application can either access or use the data. The PIN is a minimum of a six-digit number selected by the credential holder and written to the credential during finalization. It shall not be stored in any system and should not be written down or otherwise recorded by the credential holder or any other person. The credential is automatically locked after no more than 15 consecutive tries of entering an invalid PIN. Credential PIN reset details and requirements for resetting a PIN are identified in Section 6.7, Credential PIN Reset.

## The Uniform Universal Personal Identification Code (UUPIC)

* + 1. UUPIC Number / Employee Number - A UUPIC is a component of NASA Identity Management that uniquely identifies a NASA identity.  The Identity Management system is managed by OPS, working in concert with the OCIO and the Office of the Chief Human Capital Officer (OCHCO), to ensure proper functioning, assignment, use, and protection of the UUPIC.
    2. UUPIC Characteristics - UUPICs shall only be issued through the population of seed data (name, unique identifier (SSN, foreign national visitor number, etc.), and date of birth) into the UUPIC repository. This information is required for all NASA identities including, but not limited to, civilians, contractors, partners, and remote IT system users that require a NASA identity.  Any request for a UUPIC will be initiated via an approved identity creation workflow method.  The reliable assignment of the UUPIC to persons uses at least two unique attributes, in addition to name attributes, from approved identity source documents.  The ICAM database is the authoritative source of the UUPIC numbers.  UUPIC numbers will be issued in random sequence, consistent with NASA policy, and will meet the following requirements:

1. Be a nine-digit numerical code without any significance as to the characteristics of the individual.
2. Be treated as a string to preserve UUPICs with leading 0s.
3. Cannot be created or derived based on other data contained in the UUPIC application.
   * 1. UUPIC Usage - The UUPIC shall serve as a replacement for the SSN by providing a unique identifier that can serve as a data point across NASA information systems.  The UUPIC may not be used as a login identifier or user account name for any information systems, databases, Web sites, etc.  The UUPIC may be available to NASA employees for lookup and may be used for positive identification of individuals within NASA information systems.  The UUPIC may not be used for purposes other than those described in this policy without the concurrence of OPS.  With the exception of account initiation in IdMAX, use of the UUPIC for any identification purposes outside those needed for positive identification of individuals across and only within information systems is prohibited without the consent of OPS.  The UUPIC may never be posted on any Internet accessible Web site.  Any deviation from this policy will be coordinated with OPS through OCIO in advance.  Requests for a UUPIC will be initiated via the approved NASA on-boarding workflow for civil servants and contractors.  UUPIC numbers are stored internally along with the first, middle, and last names and other information necessary to uniquely associate the UUPIC with a person.

# Credential Lifecycle Management

## General Credential Management

* + 1. Ownership. A credential is not personal property but is the property of the U.S. Government. All personnel shall be responsible for adhering to the following requirements:

1. Appropriately safeguarding issued credentials.
2. Immediately reporting the loss or false use of a credential.
3. Challenging noncredentialled personnel.
4. Notifying the proper authority of a name change.
5. Properly displaying a credential when on NASA property.
6. Surrendering a credential upon resignation, retirement, or the direction of the issuing authority.
   * 1. Reciprocity. PIV credentials issued by other Federal Government departments and agencies or CACs issued by DoD shall be accepted for the purpose of establishing the identity of the individual and as a credential for access when credential registration is successful.
     2. Misuse. Forging, falsifying, or allowing misuse of a credential or other forms of NASA identification in order to gain unauthorized access to NASA physical and logical resources is punishable under 18 U.S.C. 799 by fine or imprisonment for not more than one year, or both, and may further result in termination of employment and access to NASA resources.
     3. Production. Credentials shall only be produced by approved personalization service providers or at Centers using approved production processes.
     4. Delivery. Unprinted or unfinalized credentials shall be shipped directly to a Center by the credential manufacturer. The PIF Manager or other appropriate authority will designate a point of contact that is responsible for receipt of, signing for, and inventory and storage of credential stock.
     5. Stock protection. Credential stock will be accessible only by authorized personnel and maintained in a secure manner, pursuant to Section 6.2, Credential Inventory, Storage and Handling. Credential stock will be monitored through the use of a log which includes, at a minimum, the date of check in, the date of check out, and the name of the person(s) performing the credential stock check-ins or check-outs.

## Credential Inventory, Storage and Handling

* + 1. Credential stock, including credentials yet to be issued and returned credentials, shall be stored using the following minimum requirements:

1. Properly identified and treated as “controlled material” for inventory.
2. Segregated from classified materials, firearms, ammunition, or currency.
3. Stored in a secure area protected by the enterprise physical access control system (EPACS).
   * 1. Credentials which are lost, stolen, or unaccounted for while in storage shall be reported immediately to the PIF manager after discovery. Credential details, including credential identification numbers and status, will be reported to the ICAM credentialing team within 24 hours of discovery in order to update the card management system. The PIF manager will forward a report outlining all pertinent facts to the AIMO no later than two days after receiving reports of the lost, stolen, or unaccounted for credentials.
     2. Defective credentials shall be identified, reported, and delivered to the core technical team. The issuance official will record the defective credential identification number and the defective status in the credential storage log. A new credential will be created following Sections 3.3.8, Step 6: Credential Production.
     3. All credential encoding failures shall be reported to the ICAM credentialing team within five days of discovery and include the identification number, failure description, and any other pertinent information.

## Credentialing Determinations

* + 1. All credentialing determinations shall adhere to the adjudication principles found in NPR 1600.3.
    2. The authorizer shall make a credentialing determination of favorable or unfavorable based on the results of the database check, background investigation or continuous evaluation information.
    3. A credentialing determination may occur at any time during the issuance process or after the issuance process has been completed and should be completed within 90 days of receiving the results of the database check, background investigation or continuous evaluation information.
    4. When a favorable credentialing determination is made, the applicant’s record shall be updated to reflect a favorable credentialing determination and the background investigation indicator in the credential data model will be set to indicate background investigation completion.
    5. When an unfavorable credentialing determination is made, the applicant’s record shall be updated to reflect an unfavorable credentialing determination and the credential will be suspended and confiscated. The sponsor will be notified of the denial decision.
       1. The credential holder shall be provided the opportunity to appeal an unfavorable credentialing determination, pursuant to NPR 1600.3.
       2. If the credential holder does not appeal, if the appeal is denied, or if the result of the appeal is an unfavorable credentialing determination, the credential shall be revoked.
       3. If the result of the appeal is a favorable credentialing determination, the credential shall be reactivated and returned to the credential holder and the actions in section 6.3.4 shall be applied.

## Credential Usage: Display, Protection, and Proper Usage

* + 1. NASA shall provide an electromagnetically opaque badge holder to physically protect the credential and electronically protect the information contained in the credential. Other holders found on the approved products list may be purchased by a Center at their discretion. Such holders are the responsibility of the purchasing Center to ensure that they are electromagnetically opaque.
    2. Credentials shall be properly displayed and worn at all times while the bearer is on a NASA Center or component facility. Credentials will be worn above the waist on the outermost garment with the photograph visible.
    3. The use of a permanent-type symbol or the affixing of any device (e.g., tenure pin, decals, etc.) on a PIV Smartcard or Agency Smart Badge (or any alteration or modification thereof) shall not be allowed.
    4. The punching of holes or any alteration that affects the integrity of a PIV Smartcard or Agency Smart Badge shall not be allowed.
    5. Access to non-public areas within a NASA Center perimeter may be accessed using NASA PIV Smartcards and Agency Smart Badges and will be handled on an as-needed basis in compliance with the policies established by that Center for access to facilities.
    6. The visitor pass shall only be valid for the term issued, pursuant to section 5.5, Visitor Passes. The visitor pass will be returned at the end of the visit.
    7. For logical access, smartcard credentials shall be placed in a card reader so the credential can be authenticated. Additional credential usage and permission requirements related to logical access are established in the Subscriber Agreement, provided to and signed by the applicant for:

1. Authorized uses of the credential.
2. Authorized uses of the PKI certificates and services provided with the credential.
3. Additional usage requirements for logical access credentials are established in NPR 2810.1.
   * 1. For physical access, the credential shall be placed in proximity to the card reader so the credential can be authenticated. The credential may need to be removed from the badge holder and held directly to the card reader for authentication. For certain multi-factor physical access, the credential will be inserted into the card reader and a PIN and/or biometric provided.

## Credential Renewal

* + 1. Credential renewal shall occur prior to credential expiration and facilitate replacement of the credential without the need to repeat the full enrollment and reissuance procedures described in section 3.3, Enrollment and Issuance Procedures unless the existing enrollment is no longer valid.
    2. Credential holders may apply for a renewal prior to the expiration date on their PIV credential, as allowed by IdMAX.
    3. The renewal request shall be coordinated with the sponsor, who ensures personnel records are accurate and current before the issuance of a new credential.
    4. A biometric match of the credential holder’s fingerprints shall be performed prior to the collection of new biometrics.
    5. New biometrics shall be collected as described in section 3.3.6, Step 4: Enrollment Process.
    6. The old and/or expired credential shall be collected and destroyed at the time of renewal issuance pursuant to section 6.14, Credential Destruction.
    7. The authorizer shall approve the renewal and coordinate the request for a new background investigation to be performed, in accordance with NPR 1600.3.
    8. If a renewal is in process and enrollment of new biometrics is not completed prior to the credential expiration, then the credential shall be re-issued as described in Section 6.6, Credential Re-issuance.

## Credential Re-issuance

* + 1. The old credential shall be revoked, pursuant to Section 6.8, Credential Revocation when the credential:

1. Has passed its expiration date without a renewal occurring.
2. Has been compromised.
3. Is lost, stolen, or damaged.
4. Requires a change in printed information (name change, citizenship change, etc.).
5. Card holder’s status or affiliation changes.
   * 1. NASA PIV credentials shall not be re-issued for an individual transferring from one Center to another Center.
     2. The applicant shall undergo the entire enrollment and issuance process, in accordance with section 3.3, Enrollment and Issuance Procedures.
     3. Credential holders who have officially changed their name shall submit a request for a reissuance of their credential. The credential holder will be required to reenroll and provide approved identity source documentation that reflects the legal name change prior to enrollment occurring and issuance of the new credential.

## Credential PIN Reset

* + 1. Credentials that are disabled or locked-out due to a maximum of 15 consecutive invalid PIN entry attempts shall have their PIN reset. It is the responsibility of the credential holder to arrange for a PIN reset to occur.
    2. Biometric verification of the applicant’s biometrics to the biometrics stored on the card shall occur prior to the PIN being reset.
       1. If the biometrics cannot be matched after 3 tries or the fingerprints are unclassifiable, the applicant will be required to provide a primary identity source document to the enrollment official, or other designated official, who will compare the photographs on the credential, in the identity source document, and on the screen within the credential management system to confirm the identity of the individual. Once the identity is confirmed, the enrollment official will assist the applicant to perform a PIN reset.
    3. PIN reset shall not require the reissuance of a credential.

## Credential Revocation

* + 1. Credentials shall be revoked under the following conditions:

1. Change in need for access.
2. Termination of employment, both voluntary and involuntary.
3. Unfavorable credentialing decision based on results of a background investigation or continuous evaluation.
4. Administrative action.
5. Death of the credential holder.
   * 1. Revocation of a credential shall result in the following:
6. The credential holder’s relationship shall be set to “inactive.”
7. The credential shall be returned and terminated.
8. Notification shall be provided to the sponsor, and other appropriate personnel, of the credential revocation.

## Lost and Stolen Credentials

* + 1. Lost and stolen credentials shall be reported to the Center PIF Manager immediately after discovery of the loss/theft. The lost/stolen credential will be suspended in accordance with section 6.11, Credential Suspension. If the credential is not reported found within 24 hours the credential will be revoked and/or disabled, cancelling all certificates and access privileges of that card. The identity of the credential holder itself will remain active, as only the card is disabled.
    2. The credential holder shall, within three business days of reporting the loss/theft, appear in person at the badging office to verify loss/theft of the credential and be issued a new credential. The credential holder will be required to undergo a credential re-issuance per section 6.6, Credential Re-issuance.
    3. It is the responsibility of NASA Centers to establish policy for the handling of multiple lost and stolen credentials. Centers may adopt one of the below methods for managing credential holders who report their credential as lost or stolen on multiple occasions. The following list is not comprehensive, and additional methods may be chosen by the Center:

1. Allow for the replacement of two credentials after which the credential holder will undergo awareness training for each subsequent lost credential prior to receiving the credential.
2. Implement a lost/stolen credential form which requires signature of the credential holder’s manager, sponsor, or other appropriate individual(s).

## Forgotten Credentials

* + 1. The credential holder will appear at the badging office to request a temporary replacement credential/pass for physical access.

## Credential Suspension

* + 1. Suspended credentials shall be immediately disabled and all related access, both physical and logical, shall be disabled.
    2. Credentials shall be set to “suspended” and temporarily disabled in situations where the credential is at risk such as when the credential has been forgotten or misplaced and is no longer in the possession of the credential holder. Lost or stolen credentials will be handled pursuant to section 6.9, Lost and Stolen Credentials.
    3. Credentials shall be set to “suspended” and temporarily disabled in situations where the credential holder presents a significant risk to the Agency (e.g., threat made by the credential holder against another person).
    4. Credentials, and all related access, that have been suspended may be re-enabled or revoked in accordance with those processes and requirements.

## Credential Return

* + 1. Cardholders shall return credentials to NASA once an individual’s affiliation with NASA has ended. Credentials should be returned to the issuing authority no later than the last day of association with NASA. The issuing authority will be responsible for recording receipt of the credentials that are returned and properly storing the credentials until destruction. Credentials are not allowed to be kept as souvenirs.
    2. Credentials may be placed in the mail for return to OPS at NASA Headquarters.
    3. The responsibility of credential return oversight is:

1. HR for NASA civil servant.
2. Contract program manager for contractors.
3. Grant technical official for grantees.
4. The requester or sponsor for all other identities.

## Credential Termination

* + 1. Credentials returned to the badging office that do not meet any of the requirements previously established in this chapter and are to be terminated shall have all data, certificates, and access privileges invalidated, revoked, and/or disabled. Credentials that are to be terminated will have their status set to “terminated,” and a reason will be supplied for the termination. Deactivation of a credential and associated identity, if necessary, will be completed within 18 hours of notification of the need for credential termination. Terminated credentials will be destroyed following the requirements in section 6.14, Credential Destruction.

## Credential Destruction

* + 1. Credentials meeting the following criteria shall be destroyed:

1. Expired credentials.
2. Credentials discovered or located after being declared lost or stolen.
3. Credentials that are damaged.
4. Terminated credentials.
5. Revoked credentials.
   * 1. Credentials shall be thoroughly destroyed using heavy-duty crosscut shredders that are capable of smart card destruction, by depositing into a burn bag for burning, or by another method meeting National Security Agency compliant destruction procedures.

Appendix A: Definitions

Access – With regard to NASA assets, the explicit granting of permission to enter and/or use NASA facilities, interact with NASA personnel, and/or use NASA information and related information processing services.

Access Control – The process of granting or denying specific access requests.

Access Control Plan (ACP) – For a program, project, or foreign national, the assets to which that foreign national may request access. An ACP may be supplemented by a TTCP.

Accreditation – Formal declaration by a Designated Approving Authority (DAA) that an IT system is approved to operate in a particular security mode for the purpose of processing classified national security information (CNSI), using a prescribed set of safeguards. Accreditation Authority is synonymous with DAA.

Adjudication – A fair and logical Agency determination, based upon established adjudicative guidelines and sufficient investigative information, as to whether or not an individual’s access to classified information, suitability for employment with the U.S. Government, or access to NASA facilities, information, or IT resources is in the best interest of national security or efficiency of the U.S. Government.

Affiliation – The official relationship between an individual or group of individuals and NASA, most commonly established through a Space Act Agreement (i.e. international partner), contract (i.e. contractor), grant (i.e. grantee), or other official agreement (e.g. Federal employee, intern, etc.).

Asset – A system, object, data, resource, technology, facility, or any combination thereof that has importance or value to NASA; includes but is not limited to NASA Centers and facilities, NASA information systems and/or data, contracts, property, records, unobligated or unexpended balances of appropriations, and other funds or resources.

Authentication – (1) The validation and confirmation of a person’s claim of identity. (2) The validation and identification of a computer network node, transmission, or message. (3) The process of establishing confidence of authenticity. (4) Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to facilities and information systems.

Authorization – The privilege granted to a subject (e.g., individual, program, or process) by a designated official to do something, such as access information based on the individual’s need to know.

Background Investigation – The process of looking up and compiling criminal records, commercial records, and financial records of an individual.

Badge – See definition for Credential. A physical credential with visual elements that enable an authorized person (e.g., security officer) or device (e.g., smartcard reader) to grant access using a NASA-approved authentication mechanism.

Center Chief of Protective Services (CCPS) –The senior Center Protective Services Office official who is responsible for management of the Center security program.

Certification – A formal process used by the certifying official to ensure that an individual has met all established training requirements as necessary to perform their security responsibilities.

Child (Children) – Any person between the ages of 2 and 13.

Component Facilities – NASA-owned facilities not located on any NASA Center (e.g., Michoud Assembly Facility, Wallops Flight Facility, White Sands Test Facility, and NASA IV&V).

Contractor – For the purpose of this NPR, any non-NASA entity or individual working on a NASA installation or accessing NASA IT for an employer which has been contracted by NASA to perform work.

Controlled Unclassified Information (CUI) – previously Sensitive but Unclassified Information (SBU). Information that the United States government creates or possesses that is sensitive and important enough to require safeguarding or dissemination controls. CUI is not classified, but it cannot be released to the public without further review and will be limited to those with a lawful government purpose.

Credential – A physical/tangible or electronic object through which data elements associated with an individual are bound to the individual’s identity. Credentials utilize NASA-approved authentication mechanisms to grant physical and/or logical access to assets.

Credentialing Determination – Following the adjudication guidelines established by the Federal government, a decision to issue a credential based on the results of any database checks or background investigations.

Designated Country – A country with which the United States has no diplomatic relations, a country determined by the Department of State to support terrorism, a country under Sanction or Embargo by the United States, and/or a country of Missile Technology Concern. A current list of NASA designated countries can be found in IdMAX or on the OIIR webpage at <https://oiir.hq.nasa.gov/nasaecp>.

Employee – Individual who is hired or contracted by NASA to perform specific tasks or duties in exchange for compensation.

Enterprise Visitor Access Management System (EVAMS) – NASA's authoritative data system for standardized visitor data collection, hardware, reporting, and auditing.

Escort (verb) - Physical presence by an approved individual maintaining operational control (maintaining line of sight, speaking distance, etc.) of the visitor and the visitor’s activities while on the Center and in buildings. Escort begins the moment the visitor checks in and ends the moment the visitor is checked out. Due to space constraints in the visitor lobby or parking area, Centers may designate specific locations (e.g., parking lots) to and from which visitors may travel without the physical presence of an escort (person).

Escorts (noun) – Trained and designated holders of a NASA PIV, DoD CAC, or other Federal agency PIV that has been registered in IdMAX.

Exception – The approved continuance of a condition authorized by the AA for OPS that varies from a requirement and implements risk management on the designated vulnerability.

Foreign National – Any person who is not a U.S. citizen or U.S. person (lawful permanent resident or protected individual).

Foreign National from a Designated Country – A foreign nationals who is a citizen of or who was born in a designated country. This may include foreign nationals residing in, having travelled through, or travelled from a designated country.

Grant Recipient – Organization (i.e., universities, nonprofits, etc.) that has received a Federal award (grant or cooperative agreement) directly from NASA to carry out an activity under a NASA program.

Identity – The set of attributes that uniquely identify an individual for the purpose of gaining logical and physical access to protected resources and identification in electronic transactions.

Identity Proofing – The process for providing sufficient information (e.g., identity history, credentials, and documents) to an enrollment officialwhen attempting to establish an identity or issue a credential.

Identity Source Document – A NASA-approved document used to verify aspects of a person’s identity. The list of NASA-approved identity source documents can be found in the ICAM Portal.

Identity Verification – The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the credential or system and associated with the identity being claimed.

Identity proofing and vetting – A review of information about a person for possible approval or acceptance. In this document, a vetted person has been reviewed to determine eligibility for access to NASA physical and/or logical assets.

Infant – Any person under the age of 2.

Intermittent Access – Any physical and/or logical, non-continuous access not exceeding 180 cumulative days in a 365-day period.

Intern – Any individual taking part in a NASA internship program pursuant to an active SAA as approved by the Office of Education (OE), Office of Science, Technology, Engineering, and Math (OSTEM). For foreign national interns, participation will only be through the NASA International Internship program, International Space University cooperation, or other foreign national internship program overseen by OE with support from OIIR.

International Partners – Foreign entities or persons who are involved in a particular international program or project under an International Space Act Agreement (ISAA).

Lawful Permanent Resident (LPR) – An individual defined by 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. 1324b(a)(3). A foreign national, legally permitted to reside and work within the U.S. and issued the Permanent Resident Card (PRC) or Alien Registration Receipt Card (ARRC) (Form I-551), also known as a Green Card. LPRs may be employed in the Federal sector for specific needs or under temporary appointments per 5 CFR, Part 7, Section 7.4). LPRs may not be granted access to classified national security information (CNSI). LPRs are not prohibited from accessing export-controlled commodities but still require a work-related “need-to-know” and are still considered foreign nationals under immigration laws. Replaces the term “Permanent Resident Alien (PRA).”

Limited privileged access – Granted to a user to use system-level commands and files to bypass security controls for part of a system.

Logical Access – Access to information records, data, and information technology systems and applications.

Long-Term – Any physical and/or logical access for a period exceeding 180 calendar days in a 365-day period.

Minor – Any person between the ages of 13 and 18.

NASA Worker – Persons granted access to NASA who directly support the mission and goals of NASA and/or are compensated by NASA (e.g., Federal civil servants and contractors).

National Criminal History Check (NCHC) – A background check procedure performed by the FBI Criminal Justice Information Services Division. This check returns a listing of certain information taken from fingerprint submissions retained by the FBI in connection with arrests and, in some instances, Federal employment, naturalization, or military service. If any results related to an arrest are found, the results will include the name of the agency submitting the fingerprints to the FBI, the date of the arrest, the arrest charge, and the disposition of the arrest, if known to the FBI. Commonly referred to as an identity history summary check or fingerprint check.

National Crime Information Center (NCIC) – A background check procedure performed by the FBI. This check involves a search of the records stored in the FBI Central Records System Universal Index for any appearance of the name, as well as close phonetic variants and permutations of that name. If any occurrences of the name are found, relevant paper and electronic files are retrieved from local FBI offices and from other law-enforcement agencies and analyzed. Commonly referred to as a name check, name query, or name search.

Non-NASA Worker – Persons granted access to NASA who conduct independent work or participate in activities not directly for the benefit or consumption of NASA (e.g., tenants, researchers using computational hours on a NASA supercomputer, members of a social club, carpool participants, etc.).

Operational Control – With regard to escorting, maintaining line of sight, speaking distance, etc. of the escorted individual at all times.

Privileged Access – Access granted to a user so that files, processes, and system commands are readable, writable, executable, and/or transferable. This allows a user to bypass security controls.

Protected Persons – A non-U.S. citizen allowed into the country under “refugee,” “displaced person,” and “religious or political” persecution status.

Protocol Visit – Previously High-Level Protocol Visit (HLPV). Any visit sponsored by OIIR or the Center protocol office or equivalent office or organization at the Center.

Revocation – The removal of an individual’s eligibility to access physical or logical assets based upon a credentialing decision that continued access poses a risk to the Agency.

Risk-Based Determination – An official acknowledgement by a management official that they accept the risk posed by not implementing a recommendation or requirement, designed to reduce or mitigate the risk.

Risk Management – A means whereby NASA management implements select measures designed to reduce or mitigate known risks.

Short-Term – Any physical and/or logical access for a period of up to but not exceeding 179 calendar days in a 365-day period.

Smartcard – Credential issued with an individual’s unique vetted identity information encoded and physically printed on the exterior and with embedded integrated circuits which can process data.

Student – This term has been deprecated from this policy.

Supervision - Awareness of a visitor’s presence and location and accountability for the actions performed by the visitor while at a NASA Center or facility.

Technology Transfer Control Plan (TTCP) – A document which details the export controlled items and foreign persons involved in an activity and what mechanisms exist for the transfer and marking of export controlled items. The TTCP supplements the foreign national’s ACP. Refer to NPR/NAII 2190.1 for additional information.

Tenant – Any individual or organization not affiliated with NASA who occupies land or property within the NASA perimeter.

Tier I Background Investigation – The minimum background investigation required for all long-term NASA workers. This investigation includes checks of claimed identity information (date and place of birth, citizenship/status, and social security number), criminal history (law enforcement agencies), military service (conduct and discharge), educational history, employment history, Federal debt, terrorism, conduct, alcohol abuse, and drug use/involvement.

Tour – A subset of visit; a guided excursion, generally offered to the general public, by which escorted access is granted to non-public areas of interest on a Center.

Transient – A person (i.e., construction worker, club member, childcare drop off/pickup, delivery driver, retiree, Center transit, and others requested by Center Chiefs of Protective Services/Security and approved by the AIMO) who requires intermittent access.

U.S. Citizen (U.S. National) – As defined by 8 U.S.C. Chapter 12, Subchapter III and in Parts I and II, any individual having been born in the United States or certain territories or outlying possessions of the United States and subject to the jurisdiction of the United States; born abroad to a parent or parents who were citizens at the time of birth while meeting certain other requirements; or granted citizenship after fulfilling the requirements necessary to be granted naturalization.

U.S. Person (non-U.S. Citizen) – For the purpose of implementing protection and accountability under the International Traffic in Arms Regulations (ITAR); a person who is an LPR as defined by 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. 1324b(a)(3).

Visa – Issued by the Department of State, a visa indicates eligibility to seek entry to the United States for a specific purpose. Admission to the U.S. for a specified status and duration is controlled by Department of Homeland Security Customs and Border Protection inspectors.

Visa Waiver – The Visa Waiver Program (VWP) allows citizens of participating countries to travel to the United States without a visa for stays of 90 days or less, when they meet all requirements, per Department of State rules and regulations. Travelers must be eligible to use the VWP and have a valid Electronic System for Travel Authorization (ESTA) approval prior to travel.

Visit – Any means by which, and any duration for which, access is obtained to non-public NASA assets.

Visitor – Any person who needs non-electronic, escorted or supervised physical-only access to a NASA Center or facility and no logical access, except guest wireless as allowed by the Center, for a period of 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 (e.g., members of the public on a public tour or watching a public launch, family members visiting a worker or non-NASA worker, vendor delivering or replacing equipment or supplies).

Waiver – The approved continuance of a condition authorized by the AA for OPS that varies from a requirement and implements risk management on the designated vulnerability.

Appendix B: Acronyms

|  |  |  |
| --- | --- | --- |
| AA | Associate Administrator | |
| ACP | Access Control Plan | |
| AIMO | Agency Identity Management Official | |
| ARRC | Alien Registration Receipt Card | |
| ASB | Agency Smart Badge | |
| CA | Certification Authority | |
| CAC | Common Access Card | |
| CCPS | Center Chief of Protective Services | |
| CEA | Center Export Administrator | |
| CHUID | Cardholder Unique Identifier | |
| CI/CT | Counterintelligence/Counterterrorism | |
| CISA | Counterintelligence Special Agent | |
| CISO | Chief Information Security Officer | |
| CNSI | Classified National Security Information | |
| COG | Continuity of Governance | |
| COOP | Continuity of Operations | |
| COR | Contracting Officer’s Representative | |
| CPR | Card Production Request | |
| CUI | Controlled Unclassified Information | | |
| DAA | Designated Approving Authority | |
| DAO | Designated Authorizing Official | |
| DoD | Department of Defense | |
| EO | Executive Order | |
| EPACS | Enterprise Physical Access Control System | |
| E-QIP | Electronic Questionnaire for Investigation Processing | |
| ERG | Emergency Relocation Group | |
| ERO | Emergency Response Official | |
| ESF | Emergency Support Function | |
| ESTA | Electronic System for Travel Authorization | |
| EVAMS | Enterprise Visitor Access Management System | |
| FAR | Federal Acquisition Regulation | |
| FASC-N | Federal Agency Smart Credential Number | |
| FBI | Federal Bureau of Investigation | |
| FFRDC | Federally Funded Research and Development Center | |
| FICAM | Federal Identity, Credential, and Access Management | |
| FIPS | Federal Information Processing Standards | |
| FNAM | Foreign National Access Manageement | |
| GIC | Grant Information Circular | |
| HEA | | Headquarters Export Administrator | |
| HLPV | High-Level Protocol Visit | |
| HSPD | Homeland Security Presidential Directive | |
| ICAM | Identity, Credential, and Access Management | |
| IdMAX | Identity Management and Account Exchange | |
| IIF | Information in Identifiable Form | |
| IPA | Intergovernmental Personnel Act | |
| ISAA | International Space Act Agreement | |
| IT | Information Technology | |
| ITAR | International Traffic in Arms Regulations | |
| IVC | International Visit Coordinator | |
| JPL | Jet Propulsion Laboratory | |
| LPR | Lawful Permanent Resident | |
| NAFI | Non-Appropriated Funds Instrumentality | |
| NAMS | NASA Access Management System | |
| NASA | National Aeronautics and Space Administration | |
| NCHC | National Criminal History Check | | |
| NCI | NASA Critical Infrastructure | | |
| NCIC | National Crime Information Center | | |
| NIST | National Institutes of Standards and Technology | | |
| NPD | NASA Policy Directive | | |
| NPR | NASA Procedural Requirements | | |
| NRF | National Response Framework | | |
| OCHCO | | Office of the Chief Human Capital Officer | |
| OCIO | Office of the Chief Information Officer | | |
| OE | Office of Education | | |
| OIG | Office of Inspector General | |
| OIIR | Office of International and Interagency Relations | | |
| OMB | Office of Management and Budget | | |
| OPM | Office of Personnel Management | | |
| OPS | Office of Protective Services | | |
| OSTEM | Office of Science, Technology, Engineering, and Math | | |
| PCI | PIV Card Issuer | | |
| PKI | Public Key Infrastructure | | |
| PIA | Privacy Impact Assessment | | |
| PIF | PIV Issuing Facility | | |
| PII | Personally Identifiable Information | | |
| PIN | Personal Identification Number | | |
| PIV | Personal Identity Verification | | |
| PRA | Permanent Resident Alien | | |
| PRC | Permanent Resident Card | | |
| SAA | Space Act Agreement | | |
| SAO | Senior Authorizing Official | | |
| SATERN | System for Administration, Training, and Educational Resources | | |
| SAVE | Systematic Alien Verification for Entitlements | | |
| SBU | Sensitive But Unclassified | | |
| SORN | System of Records Notice | | |
| SP | Special Publication | | |
| SSN | Social Security Number | | |
| STI | Scientific and Technical Information | | |
| TTCP | Technology Transfer Control Plan | | |
| U.S. | United States | | |
| U.S.C. | United States Code | | |
| USCIS | United States Citizenship and Immigration Services | | |
| UUPIC | Universal Uniform Personal Identification Code | | |
|  |  | | |

Appendix C: References

1. Immigration and Nationality, 8 U.S.C. § 1101.
2. Unfair Immigration-Related Employment Practices, 8 U.S.C. § 1324.
3. Violation of Regulations of National Aeronautics and Space Administration, 18 U.S.C. § 799.
4. Fraud and Related Activity in Connection with Computers, 18 U.S.C. § 1030.
5. Computer Security Act, 40 U.S.C. § 11331.
6. Federal Information Security Management Act of 2002, 44 U.S.C. § 3541.
7. Uniform Administrative Requirements, Cost Principles, and Audit Requirements For Federal Awards, 2 CFR 1800.913 Investigative Requirements.
8. Numbering System for Federal Accounts Relating to Individual Persons, Executive Order (E.O.) 9397, (1943).
9. Security Requirements for Government Employment, E.O. 10450, 3 CFR part 936, (1949-1953).
10. Access to Classified Information, E.O. 12968, 3 CFR 391, (1995 Comp).
11. Suitability Determinations - Subpart B, 5 CFR 731.202 and 731.501.
12. Civil Service Rules, 5 CFR 7.4.
13. Federal Acquisition Regulation (FAR) Clause 52.204-9, Personal Identity Verification (PIV) of Contractor Personnel.
14. OMB Memo M-03-22, September 23, 2003, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.
15. OMB Memo M-19-17, May 21, 2019, Enabling Mission Delivery through Improved Identity, Credential, and Access management.
16. NPD 1371.1, Waivers of the Residence Abroad Requirement for Employees of NASA Contractors and Grantees.
17. NPR 1050.7, Authority to Enter Into Partnership Agreements.
18. NPR 1371.1, Requests for Waivers of the Residence Abroad Requirements for Exchange Visitors Sponsored by NASA Contractors and Grantees.
19. NASA Grant Information Circular (GIC) 06-02, September 22, 2006.
20. Federal Identity Credential and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011.
21. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations.
22. NIST SP 800-104, A Scheme for PIV Visual Card Topography.
23. Office of Personnel Management (OPM) Federal Investigations Notice No. 10-05, Reminder to Agencies of the Standards for Issuing Credentials under HSPD-12, May 17, 2010.
24. OPM Memorandum, Credentialing Standards Procedures for Issuing Personal Identity Verification Cards under HSPD-12 and new Requirement for Suspension or Revocation of Eligibility for Personal Identity Verification Credentials, December 15, 2020.
25. 509 Certificate Policy for the U.S. Federal Public Key Infrastructure (PKI) Common Policy Framework, v2.5 October 16, 2006.