



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

**NASA**  
**Procedural**  
**Requirements**

**NPR 1600.4**  
Effective Date: August 01,  
2012  
Expiration Date: August 01,  
2017

**COMPLIANCE IS MANDATORY**

---

## **Identity and Credential Management**

**Responsible Office: Office of Protective Services**

# **Table of Contents**

## **Preface**

- P.1 Purpose
- P.2 Applicability
- P.3 Authority
- P.4 Applicable Documents and Forms
- P.5 Measurement/Verification
- P.6 Cancellation

## **Chapter 1. Introduction**

- 1.1 Overview
- 1.2 Scope
- 1.3 Waivers and Exceptions

## **Chapter 2. Roles and Responsibilities**

- 2.1 Overview
- 2.2 Agency Roles and Responsibilities
- 2.3 Center Roles and Responsibilities
- 2.4 Separation of Duties for the PIV Role
- 2.5 Training
- 2.6 Privacy

## **Chapter 3. Enrollment and Credential Issuance**

- 3.1 Overview
- 3.2 Chain of Trust
- 3.3 NASA Credential Types

### 3.4 Applicant Categories

### 3.5 On-site Enrollment and Issuance Procedures for NASA Credentials

## **Chapter 4. Foreign Nationals**

### 4.1 Overview

### 4.2 NASA Foreign National Access Policy and Related Requirements

### 4.3 Processing On-site Foreign National Visit Requests

### 4.4 Foreign National Request and Sponsor

### 4.5 Requirements and Risk Review

### 4.6 Authorization

### 4.7 Implementation

### 4.8 Variations Based on Type of Onsite Visit Request

### 4.9 Variations Based on Visitor Characteristics

### 4.10 Identity Vetting Requirements Based on Length of U.S. Residence

### 4.11 Identity Vetting Requirements and Credential Type for Visits, Temporary Employees, and Permanent Employees

### 4.12 Processing Information Technology (IT) Remote Only Requests

## **Chapter 5. Characteristics of NASA Badges**

### 5.1 NASA Credential Types

### 5.2 NASA PIV Credential Data

### 5.3 The Universal Uniform Personal Identification Code (UUPIC)

## **Chapter 6. PIV Credential Management Lifecycle**

### 6.1 PIV Credential Inventory

### 6.2 PIV Credential Storage and Handling

### 6.3 Final Adjudication and Subsequent Investigation

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

### 6.5 PIV Credential Renewal

### 6.6 PIV Credential Re-issuance

### 6.7 PIV Credential PIN Reset

### 6.8 PIV Credential Revocation

### 6.9 Lost and Stolen Credentials

### 6.10 Forgotten Credentials

### 6.11 PIV Credential Suspension

### 6.12 PIV Credential Return

### 6.13 PIV Credential Termination

### 6.14 PIV Credential Destruction

## **Appendix A. Definitions**

## **Appendix B. Acronyms**

## **Appendix C. NASA PIV Photo Identification Badge Standards**

# Appendix D. Subscriber Agreement

# Preface

## P.1 Purpose

- a. This NASA directive establishes Agency-wide identity and credential management policy and establishes high-level implementation requirements as set forth in NASA Policy Directive (NPD) 1600.2, NASA Security Policy, as amended. Identity and credential management are the activities that deal with identifying individuals and controlling their access to resources (e.g. facilities and IT systems) by associating user rights and restrictions with the established identity.
- b. 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

- a. This NASA directive is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to JPL (a Federally Funded Research and Development Center), other contractors, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.
- b. This NASA directive is applicable to all other personnel completing work through Space Act Agreements or Memorandums of Agreement/Understanding, those assigned or detailed under the Intergovernmental Personnel Act, partners, cooperative agreements, and visitors.

## P.3 Authority

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

## P.4 Applicable Documents and Forms

- a. E-Gov Act of 2002, Pub. L. No.107-347, 116 Stat. 2899 (2002), 44 U.S.C. Ch 36.
- b. Rehabilitation Act of 1973, Public Law 93-112, 29 U.S.C. Ch 29.
- c. Privacy Act of 1974, U.S. Pub. L. No.93-579, 88 Stat. 1896, (1974).
- d. Security requirements for Government employment Exec. Order No. 10450, 3 CFR 936 (1949-1953).
- e. Equal employment opportunity Exec. Order No.11246.
- f. Access to Classified Information Exec. Order No.12968, 3 CFR 391 (1995 Comp).
- g. Suitability Determinations - Subpart B, 5 CFR § 731.202 and 5 CFR § 731.501.
- h. 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 Standard for Federal Employees and Contractors."

- i. NASA Procedural Requirement (NPR) 1382.1, NASA Privacy Procedural Requirements.
- j. NPR 1600.1, Security Program Procedural Requirement.
- k. NPR 2190.1, NASA Export Control Program.
- l. NPR 2810.1, Security of Information Technology.
- m. NASA Grant Information Circular (GIC) 06-02, September 22, 2006.
- n. Federal Acquisition Regulation Clause 52.204-9, Personal Identity Verification (PIV) of Contractor Personnel.
- o. Federal Information Processing Standards Publication 201 (FIPS 201).
- p. NIST Special Publication (SP) 800-79, Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations.
- q. NIST SP 800-104, A Scheme for PIV Visual Card Topography.
- r. Homeland Security Presidential Directive 12 (HSPD-12).
- s. X.509 Certificate Policy for the U.S. Federal Public Key Infrastructure (PKI) Common Policy Framework, v2.5 October 16, 2006.
- t. NPR2841.1, Identity, Credential, and Access Management Services.
- u. NPR 1600, NASA Personnel Security.
- v. Office of Personnel Management (OPM) Federal Investigations Notice No. 10-05, May 17, 2010, "Reminder to Agencies of the Standards for Issuing Credentials under HSPD-12."
- w. NIST Special Publication (SP) 800-53, May 1, 2010, Recommended Security Controls for Federal Information Systems and Organizations.
- x. Office of Management and Budget (OMB) Memo M-11-11, February 3, 2011, "Continued Implementation of Homeland Security Presidential Directive (HSPD)-12 Policy for a Common Identification Standard for Federal Employees and Contractors."

## **P.5 Measurement/Verification**

To determine compliance with this NASA directive, the Office of Protective Services (OPS) shall provide assessments/audits of the application of this policy requirement. This will consist of periodic reporting from the Centers, including information collected for the satisfaction of OMB. The specific metrics utilized will conform to those described in Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 1.0, November 10, 2009.

## **P.6 Cancellation**

- a. NPD 1600.2E, NASA Security Policy dated April 28, 2004.
- b. NPR 1371.2, Processing Requests for Access to NASA Installations or Facilities by Foreign Nationals or U.S. Citizens Who are Reps of Foreign Entities dated April 7, 2003, cancelled on June

3, 2011.

c. NPR 1600.1, NASA Protective Services Program Requirements, Appendix J, dated August 1, 2012.

d. NASA Memorandum (NM) 1600-46, Security Identification System Requirements dated January 19, 2007.

e. NM 1600-50, Photo Identification Color-Coding Requirements dated September 6, 2006.

f. NM 1600-52, Personal Identity Verification Policy and Procedures dated May 24, 2007.

g. NM 1600-95, NASA Interim Directive (NID): NASA Identity and Credential Management dated June 3, 2011.

h. NASA Interim Directive (NID) 1600-96 NASA Personnel Security dated July 20, 2011.

i. Memorandum for Center Chiefs of Security, Center ICAM Business Leads signed by OPS AA Jack L. Forsythe, July 20, 2010, "Changes to Foreign National Processing."

j. Letter signed by Will Morrison for Jack L. Forsythe, May 2, 2008, "Interim Guidance for the Vetting of Foreign Nationals Post Issuance of Homeland Security Presidential 12 (HSPD-12)."

k. Letter signed by OSPP AA David A. Saleeba, December 4, 2007, "Interim Revision to Foreign National Escort Policy Requirements."

/S/

Dr. Woodrow Whitlow, Jr.  
Associate Administrator  
Mission Support Directorate

# Chapter 1. Introduction

## 1.1 Overview

1.1.1 In recent years, the Federal Government has increased emphasis on improving the physical and logical security of the hundreds of thousands of facilities that the Federal Government owns and leases as well as the IT systems to support the diverse mission work of Federal agencies. The Government Accountability Office (GAO) has identified the need to develop a common framework that includes key practices for guiding agencies' physical security efforts, such as employing a risk management approach to facility protection, leveraging advanced technology (e.g., smart cards), improving information sharing and coordination, and implementing performance measurement and testing. (See <http://www.gao.gov/new.items/d0549.pdf>). GAO has also outlined the need for standard performance metrics to evaluate the effectiveness of physical security protections.

1.1.2 This NASA directive establishes the policies and high-level procedures that shall be used throughout NASA to achieve the improvements in physical security protections required by GAO. Strong Identity, Credential, and Access Management (ICAM) practices and adherence to the Federal common framework for ICAM as outlined in the Federal ICAM (FICAM) Roadmap Guidance Document will address any weaknesses within NASA's physical security infrastructure.

1.1.3 Identity management and credential management allows the identity of an individual to be verified in the digital realm, so that identity can be trusted to conduct business. Even low-risk employees possess access behind physical and logical safeguards that can give them unprecedented access to critical information and systems. This document seeks to establish a common, standardized basis for ICAM within NASA.

1.1.4 ICAM business processes include all the processes necessary to support proofing and vetting the identity of all people requiring access (physical, logical, or both) to NASA resources. ICAM business processes also include all the necessary processes for issuing credential and granting access based on favorable identity proofing and vetting. The governance structure that has been established for this is documented in NPR 2841.1, Identity, Credential, and Access Management Services.

## 1.2 Scope

1.2.1 The policies and procedures identified within this document define the approved processes for NASA to manage personal identities and the issuance of NASA Personal Identity Verification (PIV) credentials. This NPR also establishes the policy for the management of other types of NASA credentials, visitor badges, and Center-specific badges. Non-PIV logical access tokens such as RSA Tokens are not covered in this document. The policies and procedures for vetting an identity are covered in NM 1600-96. Usage of this vetted and bound identity for physical access is covered by NPR 1600.1 and logical access by NPR 2810.1 Security of Information Technology. The policies and procedures for granting remote only IT access to foreign nationals are described in this NPR (see sections 4.3.10 and 4.12). 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.

1.2.2 The terms "PIV credential" and "non-PIV credential" are used frequently in this document. The term "PIV credential" refers to the credential which is issued to civil service and contractor employees who need physical or logical access to NASA facility and IT systems for 180 days or

more. NASA's procedures for issuing PIV credentials must conform to HSPD-12. All other credentials issued by NASA are referred to as "Non-PIV" credentials. Non-PIV credentials include such things as: visitor badges, Center-specific badges, RSA tokens, etc.

## 1.3 Waivers and Exceptions

1.3.1 Centers might occasionally experience difficulty in meeting specific requirements established in the series of NASA security program NPR's and may request waivers and/or exceptions to those specific requirements. The process for submitting requests for waivers or exceptions to specific elements of the NASA Identity and Credential Management program is as follows:

a. The Asset, Program, or Project Manager and Center Chief of Security (CCS)/Chiefs of Protective Services (CCPS) shall justify the exception request through security risk analysis: e.g., cost of implementation; effects of potential loss of capability to the Center; compromise of national security information; injury or loss of life; loss of one-of-a-kind capability; or inability to perform its missions and goals, etc.

(1) Justification will also include an explanation of any compensatory security measures implemented in lieu of specific requirements.

(2) The exception request shall be submitted to the Center Director.

b. The Center Director shall confirm that the exception request has the concurrence of both the CCS and, as necessary, the Center Chief Information Officer. The Center Director will then either recommend approval or return the exception request to the CCS/CCPS for further study or closure. The Center Director forwards concurrence to the Mission Support Directorate Associate Administrator at NASA Headquarters.

c. The Mission Support Directorate Associate Administrator shall forward exception requests to the Assistant Administrator (AA) for the Office of Protective Services (OPS) at Headquarters or return proposals to the Center Director for further study or closure. Approval authority of the waiver or exception request resides with the Mission Support Directorate Associate Administrator.

d. The AA for OPS will coordinate implementation of any approved waiver or exception, for further study, or denial and closure.

# Chapter 2. Roles and Responsibilities

## 2.1 Overview

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

## 2.2 Agency Roles and Responsibilities

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

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

2.2.3 PCI Designated Accreditation Authority (DAA) - The Deputy AA for OPS shall be the PCI DAA. The PCI DAA reviews the certification documentation and the recommendation prepared by the PCI assessor and accredits the PCI as required by HSPD-12. Through accreditation, the DAA accepts responsibility for the operation of the PCI at an acceptable level of risk to NASA. The SAO can also fulfill the role of the DAA.

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

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

## 2.3 Center Roles and Responsibilities

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

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

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

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

- a. HR specialist for NASA civil service employees;
- b. Contracting Officer's Technical Representatives (COTR) or other Federal civil service technical personnel responsible for work requirements for contractors;
- c. Grants technical official for grantees;
- d. Authorizing official or designee for Economy Act, Space Act, CSLA or CSCA agreements, or
- e. The NASA civil servant program or project manager who requires the foreign national to access NASA facilities or IT systems.

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

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

denies NASA PIV credential issuance. The PIV authorizer records the final result of adjudicated investigations, and when the adjudicated investigations are favorable, authorizes continued use of an issued PIV credential as required in NM 1600-96 NASA Personnel Security.

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

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

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

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

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

## **2.4 Separation of Duties for the PIV Role**

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

**2.4.2** Individuals and entities assigned to the PIV enrollment official, PIV authorizer, PIV investigation reviewer, PIV issuance official, and the PIV digital signatory roles shall complete

training that is specific to their duties prior to being allowed to perform in their function.

## 2.5 Training

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

## 2.6 Privacy

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

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

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

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

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

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

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

- a. Authorized uses of the PIV credential;
- b. Authorized uses of the PKI certificates and services provided with the PIV credential;
- c. Notification requirements for the applicant; and
- d. Requirements to return the PIV credential at the end of use.

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

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

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

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

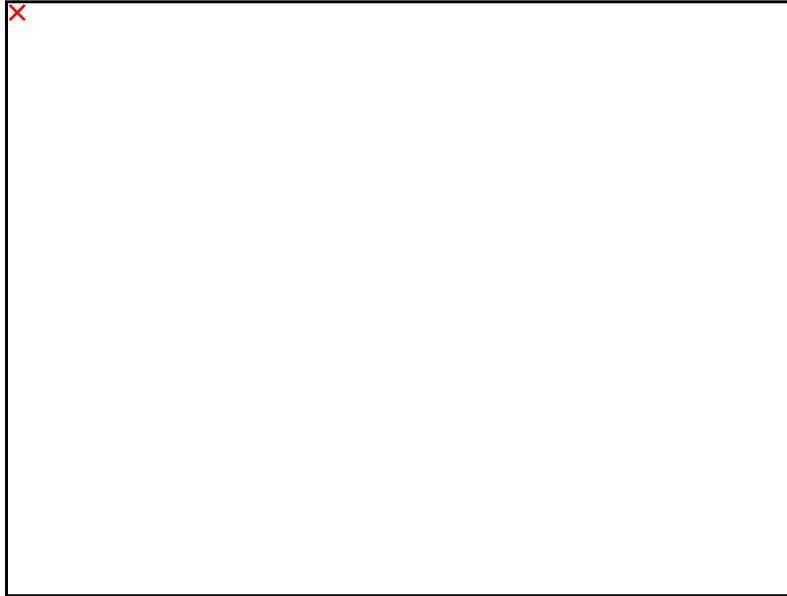
2.6.9 NASA shall archive and safeguard all stored data pursuant to NPD 1440.6, NASA Records Management, and NPR 1441.1, NASA Records Retention Schedules. Identity files are maintained for a minimum of two years after an individual's relationship with the Agency has ended. NASA may, at its discretion,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

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

# Chapter 3. Enrollment and Credential Issuance

## 3.1 Overview

3.1.1 The NASA Identity Management and Credential Management Processes are designed to conform to the system-based model for identity proofing, registration, and issuance process that is described in NIST FIPS 201-1 and is represented diagrammatically in the document via Figure 3.1:



*Figure 3.1*

## 3.2 Chain of Trust

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

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

## 3.3 NASA Credential Types

3.3.1 NASA uses both PIV credentials and non-PIV credentials. Access is granted via NASA PIV credentials. NASA PIV credentials allow physical only, logical only, and/or both physical and logical access to resources at NASA. Each NASA credential is linked to an established identity and shall go through the appropriate issuance steps as outlined in this chapter. See NPR 2810.1, for policy and procedures regarding NASA non-PIV credentials that allow access to only logical systems. NASA visitor badges are NASA non-PIV badges which allow only physical access to the issuing NASA Centers. For short-term visitors, Centers are authorized to issue Center-specific badges (i.e. NASA non-PIV badges) for physical access to that Center based on a risk-based determination documented as part of the permanent record. Requirements for the characteristics of these credentials, including printing elements and technology capabilities are detailed in Chapter 5,

## Characteristics of NASA Badges.

3.3.2 NASA PIV credentials shall be required for all persons who have been deemed as needing routine and regular access to NASA Centers, facilities, and IT systems and resources for a period exceeding 179 days in a 365-day period. These persons include all NASA employees, all NASA contractors, agreement partners, and non-NASA tenants in NASA facilities. NASA PIV credentials will be issued to both U.S. citizens and foreign nationals. NASA PIV credentials will be issued following the identity-proofing, registration, and issuance processes defined in this document for the management of identities of all new and current employees, contractors, and affiliates including foreign nationals.

3.3.3 NASA PIV credentials will be issued only after completion of a FBI fingerprint check and submission of a background investigation, which will be a National Agency Check and inquires (NACI) background investigation at a minimum. NASA PIV credentials will have an expiration date set for a period not to exceed five years from the Card Production Request (CPR) generation date. NASA PIV credentials will not be issued to individuals holding a Federal PIV credential issued by another Federal entity or to individuals holding a PIV-I credential issued by an organization whose PIV-I credentials conform to the Federal PIV-I standard. Exceptions to this policy may be made only when the exception has been documented and approved via the process described in section 1.4 of this document. The exception request will specifically explain why a non-NASA credential is not usable in the NASA ICAM services.

3.3.4 Any person (e.g., NASA employee, NASA contract personnel, non-NASA tenant, or other category of individuals such as volunteers, guest researchers, interns, grantees, etc.) who needs access to a NASA facility or NASA IT system and who will be affiliated with NASA and its Centers or facilities for a period of less than 180 days shall possess a NASA non-PIV Center-specific badge (e.g., a NASA temporary badge). The 180-day period begins the first day of affiliation and ends 180 calendar days later regardless of the work schedule. If an individual's affiliation extends for 180 days in a 365-day period, the individual will be issued a NASA PIV credential if the individual is a NASA employee (either a civil service or a Federal contractor employee). All other individuals who are not visitors, such as volunteers, construction workers, guest researchers, interns, grantees, etc., but who are determined to need intermittent access with no IT access may be exempted from the 180-day limit on use of a NASA non-PIV Center-specific badge consistent with risk-based assessments by CCS/CPS. Issuance of NASA non-PIV badges requires a minimum favorable adjudication of a National Crime Information Center (NCIC) name query and completion of steps 1-4 of section 3.5, On-Site Enrollment and Issuance Procedures of this NPR. Escort requirements for individuals with a NASA non-PIV badge will be based on risk-determination by the CCS.

3.3.5 NASA visitor badges shall be issued to individuals requiring access to a NASA Center for a period less than 30 days in any single visit and not more than a cumulative total of 29 days in a 365-day period. Escort requirements for individuals with visitor badges will be based on risk-determination by the CCS/CPSC.

3.3.6 NASA non-PIV Center-specific badges shall be issued to accommodate unique situations of the Center not otherwise accommodated by NASA PIV credentials and NASA visitor badges. All NASA Center-specific badge templates will have the approval of the Agency Identity Management Official prior to their creation and utilization. NASA Center-specific badges will be issued upon completion of a favorable adjudication of an NCIC name query. This is a minimum requirement, and additional security measures may be employed at the discretion of the CCS/CPSC. Issuance of these badges will be based on a risk-based access determination by the CCS. NASA Center-specific badges may be issued to individuals who hold a PIV credential issued by another Federal Government agency or department if their current non-NASA PIV credential does not work at the NASA Center. This may include contractors from another NASA Center in the event that electronic

verification of a requirement to access the NASA Center is not available at a point of entry. Issuance of NASA Center specific badges requires completion of steps 1-3 of section 3.5, On-Site Enrollment and Issuance Procedures, verification of a favorably adjudicated investigation, and capture of the individual's photograph, section 3.5.4, Step 4: Enrollment Process.

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

## **3.4 Applicant Categories**

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

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

3.4.3 NASA grantees are individuals who are working under a grant and performing activities for and/or at NASA Centers and facilities.

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

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

3.4.6 Tenants are individuals who require physical access to a NASA facility but do not work directly for NASA including individuals requiring access pursuant to a Space Act, Economy Act agreements, etc. There may or may not be a "formal" agreement associated with a tenant (example: Credit Union). The tenant may require logical access to certain NASA applications. A tenant may work for another Government agency as either a civil servant or contractor and may have a PIV badge from their agency. Tenants include those entities and their contractors and employees under Economy Act, Space Act, Commercial Space Competitiveness Act (CSCA), or Commercial Space Launch Act (CSLA) agreements or those individuals needing physical or logical access based on the above authorities. Tenants shall be issued Center-specific badges.

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

## 3.5 On-Site Enrollment and Issuance Procedures for NASA Credentials

3.5.1 Step 1: Credential Request - A requester completes a credential request within the NASA Identity Management System for an applicant. The requester submits the request to the sponsor via the NASA Identity Management System. For civil servants, this information is submitted by the HRO via Workforce Transformation Tracking System (WTTS). The information submitted includes the following:

- a. Name of the applicant;
- b. Date of birth of the applicant;
- c. Home address;
- d. Social Security Number (SSN);
- e. Position of the applicant;
- f. Contact information for the applicant;
- g. Name of the requester;
- h. Organization of the requester; and
- i. Contact information for the requester.

3.5.2 Step 2: Sponsorship - The sponsor validates the receipt of the request from the requester and reviews the data in the request. The sponsor reviews the Position Risk Determination in the NASA Identity Management System and approves or denies the request, establishing the need for a relationship between the applicant and NASA and the applicant's need for a PIV credential.

3.5.3 Step 3: Check for background investigation or database checks - The authorizer or investigation reviewer validates the receipt of the request from the sponsor. The authorizer and supporting staff review the OPM and other Federal databases and take appropriate steps to validate the applicant's investigation status with regard to a current investigation.

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

3.5.3.2 If no investigation is on file or in progress, the authorizer coordinates initiation of an invitation in the OPM e-QIP for the applicant to complete the appropriate background investigation form and authorizes the enrollment official to obtain the applicant's flat and rolled fingerprints, I-9 documents, and photograph.

3.5.3.3 If the applicant is requesting a non-PIV Center-specific badge then the authorizer or designee conducts the appropriate database check and approves the credential if the database check is favorable. The submission of the captured fingerprints to OPM is optional as determined by the CCS.

3.5.4 Step 4: Enrollment process - The enrollment official validates the receipt of the request from the authorizer. The sponsor advises the applicant that they will appear in-person before the enrollment official and present two forms of identity source documents in original form. The

applicant appears in person before the authorized enrollment official and presents two forms of identity source documents in original form per USCIS Form I-9, one of which will be a Federal or state issued picture identification. The enrollment official inspects the source document for authenticity and validates the source document through visual or electronic scrutiny and, when necessary, with the authority or entity which issued it.

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

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

3.5.4.3 Enrollment USCIS Form I-9 documentation - The enrollment official obtains and maintains legible photocopies or scanned copies of the original USCIS Form I-9 documentation. Any document that appears invalid (e.g., absence of security hologram or other known security features on a state issued driver's license, security features on a birth certificate or passport, smeared ink, etc.) are to be rejected by the enrollment official and reported to the proper authority for review. Photocopies of rejected documents are to be made and retained for a period not to exceed one year or until any appeal process is completed. USCIS Form I-9 documents that do not pass electronic examination are rejected and another approved USCIS Form I-9 document will be obtained and subjected to electronic scrutiny. In the event the applicant is required to provide documentation to resolve discrepancies or omissions in data collected, the enrollment official shall review the information with the applicant as necessary. The information submitted by the applicant will be used to update the applicant identity record.

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

3.5.5 Step 5: Adjudication process - If no investigation is on file or in progress, the fingerprints captured during enrollment shall be submitted to OPM with a request for a background investigation. The authorizer receives the results of the fingerprint check. If the fingerprint check comes back with a status of unclassifiable, the Center will use the results of a name check to process the PIV credential request. The authorizer makes a determination based upon receipt of the fingerprint check results or evidence of an acceptable existing background investigation (as found in section 3.5.3, Step 3: Check for background investigation), if the applicant is eligible to receive a PIV credential. If the adjudication of the available background investigation is favorable, the authorizer will submit a PIV credential issuance request to authorize the creation and issuance of a PIV credential. Final adjudication of the record is performed in compliance with NASA personnel security policies.

3.5.6 Step 6: Badge production process - The PIV authorizer submits a request for badge printing if

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

3.5.7 Step 7: Issuance process - The applicant appears before the issuance official, who establishes whether the badge was printed in a batch job, previously printed on-site, or is to be printed on-site. If the badge is printed in a batch job or previously printed on-site, the issuance official will obtain the card stock from storage. If the badge is to be printed on-site, the issuance official will obtain a blank badge from storage, verify the identity of the applicant against the database, and print the badge. The issuance official checks the printed badge to verify the identity of the applicant, conducts a biometric match, and encodes the badge with an applicant entered PIN number. Upon completion of the badge printing and encoding, the badge is officially released to the applicant. An approved electronically shielded badge holder shall be offered to the applicant in order to protect the badge and the privacy of information on the badge.

# Chapter 4. Foreign Nationals

## 4.1 Overview

4.1.1 This chapter outlines the requirements that NASA personnel shall follow in granting access by foreign nationals to NASA physical and/or IT resources for any purpose other than an appropriately authorized tour of facilities that is or would normally be conducted for the general public. The subsections outline the processes, procedures, and authorizations necessary to successfully obtain required access permissions in a timely manner. Upon completion of identity proofing and vetting, a specific threat determination shall be made prior to granting access that is consistent with the conditions specified in the relevant Technology Transfer Control Plan. These requirements apply to foreign national civil servants, contractors, researchers, international partners as defined via International Space Act Agreements (ISAA), high-level protocol visitors (HLPV), foreign nationals with the news media, NASA sponsored J-1 Visas, and visitors. Also included are the requirements for the processing of persons who have multiple citizenships and persons who are U.S. citizens working for foreign entities.

4.1.2 This NPR shall be the authoritative source for all 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 permanent, temporary, and visitor access. A foreign national is any person who is not a United States citizen. Lawful Permanent Residents (LPR) are not United States citizens; however, they are entitled by law to most of the same rights and privileges (and are held to the same accountability for such) as U.S. citizens. Therefore, LPRs will have identity proofing and vetting accomplished in the same manner as U.S. citizens.

4.1.3 Foreign nationals shall complete the following steps prior to being issued a NASA PIV credential:

- a. Obtain visit approval for the visit or assignment;
- b. The foreign national visitor is responsible for seeing that sponsorship is determined. If a foreign national is not under a contract where a COTR 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; and
- c. The foreign national visitor must begin the process long enough before the visit so that pre-visit identity vetting can be conducted and completed by the Center International Visit Coordinator (IVC), as described in this chapter.

4.1.4 Questions regarding the receipt and processing of access requests for foreign nationals or NASA contractor or grantee foreign national employees or visitors 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 here, an exception request can be submitted to the NASA OPS for review and approval (see section 1.4 of this document).

## 4.2 NASA Foreign National Access Policy and Related Requirements

4.2.1 NASA partners extensively with its foreign aeronautical, scientific, and technical counterparts in support of broad Agency objectives and program goals. Frequently, this working relationship results in the need for foreign national access to physical and IT resources. Visits also facilitate acquisition of information about foreign programs of interest to NASA and provide other benefits to the U.S. Government. All visits and other approved access will conform with Agency and national policies and regulations, including U.S. national security, nonproliferation and foreign policies, and export control laws and regulations. Record keeping related to tracking foreign national visits will be accomplished via the NASA Identity Management System.

4.2.2 Visits and other access for the purpose of implementing a mutually agreed program or project shall 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. Discussion or other release of information by NASA personnel to a foreign national during a visit or other approved access that does not pertain to an agreed program or project will be limited to information releasable to the general public, i.e., unclassified, non-sensitive, and non-export-controlled. Visits, assignments, or IT access requests for foreign nationals from non-designated areas are coordinated and implemented at the Center through the IVC. Visits, assignments, or IT access requests for foreign nationals from designated areas (see Office of International and Interagency Relations (OIIR) Web page at <http://oiir.hq.nasa.gov/nasaecp>) are coordinated initially through the Center Export Administrator and the Center IVC, then forwarded to NASA Headquarters OIIR, Export Administrator, and Program points-of-contact (as necessary) for review and final approval. A foreign national will be provided access to NASA physical or IT assets only after final approval.

## **4.3 Processing On-Site Foreign National Visit Requests**

4.3.1 NASA Center or Component Facility IVC will directly receive and review all requests from, or on behalf of, foreign nationals for access to its buildings, installations, facilities, or IT resources. All foreign national access requests, other than for an appropriately authorized public tour, shall undergo an identity vetting process based on visit type, foreign national residency, and country affiliation. The Center IVC will approve the requests for foreign nationals from non-designated countries after obtaining appropriate Center approvals. Requests for foreign nationals from designated countries will be forwarded to and approved by Headquarters' OIIR before final approval by the Center IVC.

4.3.2 If the visit's purpose is for gathering information or conducting discussions in technological areas that NASA considers sensitive (e.g., for proprietary, national security, or export control reasons), then the visit shall be disapproved in the absence of a specific NASA programmatic interest. Requests should be approved only to the extent the foreign national understands that discussions and information provided by the NASA representatives will be confined to information that is releasable to the general public. All identity proofing and vetting for foreign nationals from non-designated countries will be performed at the Center. All current Center review processes may continue as they do now at each Center's discretion.

4.3.3 Only holders of active NASA PIV credentials shall be allowed to escort foreign nationals. Foreign nationals who hold valid NASA PIV credentials may escort other foreign nationals.

4.3.4 Centers shall accept as valid the identity vetting of their peer Centers as a baseline requirement. Additional identity vetting may be required should access requirements change (e.g., if the foreign national needs privileged access or the IT Security Plan warrants a higher-level investigation).

4.3.5 A person with multiple citizenships, all foreign, and when one or more of the citizenships is

from a designated country, shall be processed as from a designated country.

4.3.6 NASA Center personnel shall apply the credentialing processes and standards as provided in the OPM Memorandum of July 31, 2008, Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12 to non-U.S. nationals who work as employees or contractor employees, including those who require long-term logical or physical access to NASA facilities. For individuals who are non-U.S. nationals in the United States or a U.S. territory for three years or more, a background investigation (i.e. NACI or equivalent) will be initiated after employment authorization is appropriately verified.

4.3.6.1 For foreign nationals who are in the U.S. or a U.S. territory for less than three years, NASA Center personnel shall delay the background investigation until the three-year requirement is met. In such cases, an alternative facility access identity credential may be issued as appropriate based on a risk determination. Before an alternative identity credential may be issued, the individual's employment authorization will be verified and an FBI fingerprint-based criminal history check will be completed. Center personnel will request an FBI Investigations File (name check search), a name check against the Terrorist Screening Database, and a USCIS Check against Systematic Alien Verification for Entitlements (SAVE). Some of these database checks may be requested directly from OPM or through automated tools such as NCIC and Visual Compliance.

4.3.6.2 Centers shall perform additional database checks to determine if there are changes to the foreign national's identity status. These status checks may be performed separately or through a Visual Compliance as follows:

- a. Visual Compliance Unverified List;
- b. Entities List;
- c. Denied Persons List;
- d. Debarred Parties List;
- e. Specially Designated Nationals; and
- f. Terrorist database.

4.3.7 Foreign national non-PIV credentials shall be issued for a maximum period of three years of date of visa/passport expiration, date of I-94/W expiration, or assignment end date, whichever comes first. Foreign nationals on visa waivers may have credentials issued for a period of three years of date of visa waiver expiration, date of I-94/W expiration, or assignment end date, whichever comes first. Foreign nationals on visa waivers will return their credential to the Center security office after each visit and will present their current passport to the Center security office to retrieve their credential at the beginning of each visit. When a foreign national with a visa waiver needs to stay in the U.S. beyond the 90 days, they are required to provide the visa information to the Center IVC.

4.3.8 To receive a PIV credential, foreign nationals who have been in the U.S. longer than three years shall complete the SF-85/NACI or the SF-85P Public Trust (via e-QIP if the person has an SSN) or a paper copy of the background investigation can be mailed to OPM if the foreign national does not have an SSN.

4.3.9 Foreign nationals with PIV credentials shall be allowed to access all Center perimeters without additional identity proofing or vetting. Additional access (physical or IT) will be determined by the physical or IT asset owner and coordinated through the receiving Center's International Visits Coordinator prior to the foreign national's arrival. Centers that use Physical Access Control Plans must ensure they are valid and accurate. Technology Transfer Control Plans (TTCP), as required by

NPR 2190.1, NASA Export Control Program, will be updated as necessary. Physical access beyond the perimeter (escorted or not) is at the discretion of the Center security office. If required, the security office will issue a Center credential for access purposes.

#### 4.3.10 Escort Requirements

4.3.10.1 Identity vetting requirements established by this NPR shall not preclude each Center security office from enacting additional requirements regarding access to the Center, buildings, or other secured areas. Access requirements for foreign nationals are outlined in the TTCP.

4.3.10.2 The IVC must work with the Center security office to determine escort requirements while the foreign national is located at the Center and to assure the foreign national sponsor understands and agrees to those requirements.

### 4.4 Foreign National Request and Sponsor

4.4.1 The requester for a foreign national shall be a currently employed NASA civil servant or contractor. The sponsor will be a NASA civil servant or a Jet Propulsion Laboratory (JPL) California Institute of Technology (Caltech) employee who is a U.S. citizen. The sponsor will perform a risk assessment based on the status of the foreign national and the assets that the foreign national is to access. This information is necessary to determine the level of investigation or escort requirements while the foreign national is at a NASA facility.

4.4.2 To expeditiously process the request, the sponsor shall ensure that the following information is provided to the IVC:

- a. Full legal name;
- b. Date of birth;
- c. Place of birth;
- d. Residence (including country);
- e. Citizenship(s);
- f. Passport and visa information (including visa waiver);
- g. SSN (if one is available);
- h. Foreign national number (if no SSN is available);
- i. Contact information;
- j. Sponsor name;
- k. Physical access requirements;
- l. IT access requirements (on-site and/or remote);
- m. Data access requirements (including export control license requirements);
- n. NASA affiliation (civil servant, contractor, partner, etc.); and
- o. Work description (includes purpose, program, authority, or other information that allows approvers to make an informed decision). The more information provided, the quicker the request can be processed.

## 4.5 Requirements and Risk Review

4.5.1 The IVC will be a currently employed NASA civil servant or contractor. The IVC shall review the foreign national request and perform the following:

- a. Confirm sponsorship.
- b. Review with the project office and sponsor the access requirements, work description, dates of visit, assignment or length of IT access request, and sponsor's risk assessment. Review and approve TTCP which is described in NPR 2190.1, NASA Export Control Program.
- c. Review with the Center security office broader security issues, including counterintelligence, counterterrorism, threats against national security, and pertinent data about country of origin (designated and high-threat countries). Determine appropriate level of investigation relative to physical and IT access requirements. Determine circumstances whereby escort-only status will be applied. Review and approve TTCP, if accessing NASA physical resources.
- d. Ensure the Center security office begins the background investigation based on visit type, foreign national residency, and country affiliation commensurate with risk levels outlined in the TTCP.
- e. Ensure the Counterintelligence/Counterterrorism Office performs their background investigation (as needed) and reports results back to the Center security office.
- f. With the Export Control Office and the Center export administrator, review export control issues to ensure information being exchanged does not violate export control laws and make risk-based determination on access protocols. Review and approve TTCP, if accessing NASA IT resources.
- g. With the Chief Information Security Officer (CISO), review IT access requirements (on-site and remote), and make risk-based determination on access protocols. Review and approve TTCP, if accessing NASA IT resources.
- h. With the public affairs office (if the individual is a member of the press or a public affairs member with a foreign space agency), review access requirements and protocols.
- i. With Headquarters' OIIR (if the individual is part of the NASA Exchange Visitor Program), obtain endorsement from the appropriate Mission Directorate/Mission Support Office at NASA Headquarters. Review and approve TTCP for physical and IT access.
- j. Confirm all Center authorizations have been received.

## 4.6 Authorization

4.6.1 The IVC shall coordinate and provide final approval for identity vetting, physical access, and IT access for foreign nationals from non-designated countries. In circumstances where the IVC is not a civil servant with adjudicator authority, the Center security office's PIV authorizer will provide the final approval.

4.6.2 Centers or programs may specify restrictions regarding physical or IT access privileges or escort requirements that are more restrictive than those documented in this NPR.

4.6.3 If a foreign national will be accessing multiple Centers, the sponsor and Center IVC must collaborate with affected Centers to determine applicable access and escort restrictions.

4.6.4 If a foreign national will be accessing an IT resource from multiple locations (including remote), the sponsor and system owner must determine how that access will be provisioned at multiple locations.

4.6.5 The IVC shall coordinate input for identity vetting, physical access, and IT access for foreign nationals from designated countries. Once the IVC has determined that agreement has been reached on requirements, including completion of the TTCP, the IVC will forward all information to the Headquarters' OIIR desk officer. The Headquarters' OIIR desk will then return the approval to the IVC who will issue the final approval. In circumstances where the IVC is not a civil servant with adjudicator authority, the Center security office's PIV authorizer will provide the final approval.

## **4.7 Implementation**

4.7.1 Once all approvals have been received, the IVC will report to the foreign national's sponsor the terms and conditions of the on-site assignment which include, but are not limited to, the security and export control provisos. The sponsor shall ensure implementation of the foreign national's access credentials. The sponsor will ensure that the foreign national's access requirements as documented in the TTCP are adhered to throughout the foreign national's on-site assignment.

4.7.2 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 CCS.

4.7.3 If a foreign national application has been outstanding for longer than 30 days from initial request, the IVC shall follow up with Center or Headquarters personnel to determine the cause(s) for the delay. Applications outstanding for longer than 30 days from initial request will be escalated to the AIMO for resolution.

## **4.8 Variations Based on Type of Onsite Visit Request**

4.8.1 If a foreign national is working for NASA at an overseas location, to the extent practicable, all aspects of "Processing On-Site Visit Requests" in paragraph 4.3 shall be performed. In instances where an NACI cannot be rendered, a determination will be made between the program manager and the CCS performing the investigation as to the level of investigation required. The foreign national will be given a physical access credential commensurate with the level of investigation performed and access requirements. Non-PIV credentials will expire at the end of the program/project or contract term. Investigation status information will be updated annually. Access to IT resources will be administered with a non-PIV credential.

4.8.2 If a foreign national is supporting NASA under an International Space Act Agreement (ISAA) and requires periodic access to NASA facilities, the foreign national shall be processed in accordance with procedures in paragraph 4.8.1. Visits or assignments over 30 days in duration generally require an ISAA or other agreement.

4.8.3 If a foreign national is visiting 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 that agreement has been reached on requirements, the IVC will coordinate with the CCS as to the level of investigation required. The foreign national will be given a physical access credential commensurate with the level of investigation performed and access requirements. Only non-PIV credentials will be issued. Investigation status information will be updated annually. Access to IT resources will be administered with a non-PIV credential.

4.8.4 If a foreign national is visiting NASA for a High-Level Protocol Visit (HLPV), the IVC shall

coordinate with the Center protocol office to obtain requisite information. Once the IVC has determined that agreement has been reached on requirements, including completion of the TTCP (if necessary), the IVC will forward all information to the Headquarters' OIIR desk officer and Export Control Office (if TTCP was created) for review and approval.

4.8.5 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 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.

4.8.6 If a foreign national is visiting NASA as part of the NASA Exchange Visitor Program (J-1 Visa), the IVC shall coordinate with the Center sponsor to obtain requisite information and to ensure that the foreign national is part of an existing ISAA partnership. Once the IVC has determined that agreement has been reached on requirements, including completion of the TTCP (if necessary), the IVC will forward all information to the Headquarters OIIR desk officer and Export Control Office (if TTCP was created) for review and approval.

4.8.6.1 For a foreign national to be considered for the NASA Exchange Visitor Program, the host Center or Component Facility must 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 Office 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, the 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.

4.8.6.2 No NASA funding is provided to the foreign national under the NASA Exchange Visitor Program. All funding must come from the foreign sponsor or from personal funds, and NASA must 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 areas are ineligible for participation in the NASA Exchange Visitor Program.

## **4.9 Variations Based on Visitor Characteristics**

4.9.1 If a foreign national has dual citizenship, the IVC shall determine if one of the countries of citizenship is the U.S. If one country of citizenship is the U.S., the identity vetting process will follow that for a U.S. citizen. The physical access credential provided the individual will be one for a U.S. citizen (PIV or Proximity). Physical access restrictions will be determined and agreed to by the Center Security Office (CSO) and the sponsor. If the foreign national has dual citizenship for two foreign countries, the IVC will determine the countries of citizenship. If both countries are non-designated, the foreign national identity will be vetted as non-designated. If any one country is designated, the foreign national identity must be vetted as designated.

4.9.2 U.S. citizens shall go through the same identity vetting process regardless of their employer (U.S. or foreign). All U.S. citizens are bound by the same Federal laws. The minimum identity vetting process for a full-time civil servant or contractor working at a NASA facility is the National Agency Check and Inquiries (NACI).

4.9.3 Physical access permissions are granted by the Center Security Office. IT access permissions are granted by IT system owners. A higher level of risk is associated with having access to either physical or IT resources and whether export controlled data is involved. All conditions contribute to whether access should be granted and whether a higher level identity vetting requirement is necessary (e.g., access to restricted areas, mission essential infrastructure, and sensitive or classified information).

4.9.4 Lawful Permanent Residents (LPR) shall undergo the same identity vetting as U.S. citizens. LPR identity records will be maintained in the NASA identity management system. The credential provided to LPRs will be the blue stripe LPR PIV credential. This credential will conform to the color coding requirements for Zone 15 described in NIST Special Publication 800-104. The letters "LPR" will be displayed superimposed on the NASA logo in the lower right-hand corner of the front of the PIV credential. In the event an LPR chooses not to complete the SF 85/85P required for issuance of a NASA PIV credential, then the LPR will only be issued an LPR non-PIV Center-specific badge following the requirements described in section 3.4.7.

## **4.10 Identity Vetting Requirements Based on Length of U.S. Residence**

4.10.1 For foreign nationals who have been a resident in the U.S. for less than three cumulative years, the following identity vetting process is required:

- a. A visual compliance database check that reveals no violations or derogatory information; and
- b. Reciprocity of vetting performed by Customs and Border Patrol officials at the port of entry FBI fingerprint check.

4.10.2 The foreign national non-PIV Center-specific (foreign national blue) badge shall be issued. The term of issue will be the length of assignment or time in which the foreign national has resided in the U.S. for three years, whichever is shorter.

4.10.3 Foreign nationals who have been residing in the U.S. for three years cumulatively or greater shall be asked to complete the SF 85/85P, so that an appropriate OPM investigation may be conducted. Foreign nationals are eligible for issuance of a NASA PIV credential upon favorable adjudication of an NACI investigation or higher. In the event a foreign national chooses not to complete the SF 85/85P, required for full identity vetting, the Center security office will require a minimum annual revalidation of the visual compliance database search along with an NCIC check. The foreign national blue credential will be issued based on the results of the identity vetting revalidation, and the term of issue will be the length of assignment.

## **4.11 Identity Vetting Requirements and Credential Type for Visits, Temporary Employees, and Permanent Employees**

4.11.1 For foreign national visits of 29 days or less, the following shall be required:

- a. A visual compliance database check that reveals no violations or derogatory information;
- b. Reciprocity of vetting performed by Customs and Border Patrol at the port of entry; and
- c. An appropriate credential issued for the type of visit as defined by the CCS.

4.11.2 For foreign national temporary employees whose assignments will last 30 to 179 days, the

same procedures as described in section 4.11.1 shall be applied. A non-PIV foreign national credential may be issued for this assignment category.

4.11.3 For foreign national permanent employees whose assignments will last 180 days or more, the following conditions shall be applicable:

a. A foreign national who has resided in the U.S. for 36 months or greater may complete SF 85/85P to initiate an OPM investigation and upon completion and favorable adjudication may be issued a NASA PIV credential.

b. A foreign national who has resided in the U.S. for less than 36 months will undergo identity vetting as described in section 4.10.1 and may be issued a non-PIV foreign national credential.

## **4.12 Processing Information Technology (IT) Remote Only Requests**

4.12.1 In accordance with the Federal Information Systems Management Act (FISMA), the OMB Circular A-130, and NPR 2810.1, NASA has established security requirements and procedures to assure an adequate level of protection for NASA IT systems that includes the appropriate screening of individuals having access to NASA IT systems. The level of reliability checks and/or investigations is dependent on the sensitivity of the information to be handled and the risk of magnitude of loss or harm that could be caused by the individual.

4.12.2 Foreign national "limited privileged" access to IT systems shall be allowed only if the foreign national is involved in a program under an ISAA. The sponsor will verify that an ISAA is in place and has accountability for ensuring the security of IT system data being accessed by the foreign national.

4.12.3 IT remote access ONLY for foreign nationals will be enabled by the requestor's sponsor. There is no Federal requirement for identity vetting. NASA collects basic information that allows an approximation of IT access assurance of user ID/password and/or RSA token access. When the capability is available to perform in-person identity verification through trusted agents, remote IT only access users will undergo the identity verification process. Until that capability is available, an NCIC is performed as an identity proofing check. The worker's sponsor, in coordination with the IT system owner, shall determine whether identity vetting is warranted based on the security requirements of the system documented in the IT System Security Plan. If identity vetting is required, the investigation should be conducted and recorded. If fingerprints are captured, ensure the following:

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

4.12.4 Any foreign national having access to NASA data 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 NASA IT Security Training requirement prior to activation of IT access. Recertification will be performed annually as outlined in NPR 2810.1.



# Chapter 5. Characteristics of NASA Badges

## 5.1 NASA Credential Types

5.1.1 NASA PIV Credentials - 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 through a proximity antennae and logical access through an embedded chip.

a. NASA PIV credentials contain the following security and distinguishable features on the front of the card:

- (1) Holographic overlay; and
- (2) Smart chip.

b. NASA PIV credentials have the following printed vertically 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 (MM YYYY format) and the second to the right of the applicant photograph, below the Agency identifier, and over the Agency logo (YYYYMMDD format);
- (4) The NASA Agency identifier logo;
- (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, below the NASA Agency identifier and the affiliation color band; and
- (8) Solid color band across the middle of the badge, over the full name with the color determined by the affiliation of the badge holder, per section 5.1.5, Visual Color Coding for Employee Type.

c. NASA PIV credentials have the following printed horizontally on the back of the badge:

- (1) Return address;
- (2) Applicant height;
- (3) Applicant eye color;
- (4) Applicant hair color; and
- (5) Bar code.

5.1.2 NASA Temporary Badge - Temporary badges may be equipped with technologies that allow for physical access through a proximity antennae and/or logical access through an embedded chip. Temporary badges shall not resemble the NASA PIV credential.

a. Temporary badges will have the following printed vertically on the badge:

- (1) The silhouette of a vertical Space Shuttle on the right side of the badge, located above the solid affiliation color area;
- (2) The photograph of the applicant in the top left corner;
- (3) The legal name of the applicant, printed below the applicant photograph;
- (4) The NASA Agency identifier, to the right of the applicant photograph;
- (5) The designation of the issuing Center, below the applicant name;
- (6) The unique badge identification number, below the NASA Agency identifier;
- (7) The badge expiration date that is 180 days or less from the date of Center/facility affiliation, below the badge identification number;
- (8) Solid colored lower section based on the affiliation of the badge holder, per section 5.1.5, Visual Color Coding for Employee Type; and
- (9) OPS mailing information on the bottom front of the badge.

b. Temporary badges have the following printed horizontally on the back of the card:

- (1) Return address;
- (2) Applicant height;
- (3) Applicant eye color; and
- (4) Applicant hair color.

5.1.3 NASA Visitor Badges - Centers may prescribe the topology for visitor badges as long as they meet the following criteria:

- a. The legal name of the applicant;
- b. The full name of the issuing Center; and
- c. The full badge expiration date that is 29 days or less from the date of Center/facility affiliation.

5.1.4 NASA Center-specific badges - Center-specific badges will contain the following information:

- a. The photograph of the applicant;
- b. The legal name of the applicant; and
- c. The name of the issuing Center (Center name may be common abbreviation, e.g., ARC, DFRC, etc., as appropriate).

5.1.5 Visual Color Coding for Employee Type - NASA PIV and Center-specific badges use colored markings on the badge to determine the affiliation of the badge holder. NASA PIV credentials use a color band through the name of the applicant, and Center-specific badges use a colored lower section below the photograph and including the name. Unless otherwise indicated, the color being used is for both NASA PIV and Center-specific badges as described in Table 5.1.5.

***Table 5.1.5, PIV Credential Color Coding***

| <b>Employee Type</b> | <b>Color Coding</b> |
|----------------------|---------------------|
|----------------------|---------------------|

|   |  |
|---|--|
| <b>Federal Employee</b>   | A plain white color band.  |
| <b>Contractor Employee</b>  | Contractors will have a green color band. On the right side of the band is a "G" inside a white circle to assist individuals with visual impairment in recognizing the green color.  |
| <b>Contractors at the NASA Jet Propulsion Laboratory (JPL), a Federally Funded Research and Development Center (FFRDC),</b> | Contractors at the JPL who are U.S. citizens will be recognized by the addition of a solid silver color below the green contractor color band.   |
| <b>Interagency Personnel Agreement (IPA) Employee</b>   | A plain white color band. The lower right corner on the front of the badge the label "IPA" will appear in black letters.   |
| <b>Foreign Nationals</b>  | Foreign national badge characteristics take precedence over all other affiliation characteristics. Foreign national badges have a light blue color band. On the right side of the band is a "B" inside a white circle to assist individuals with visual impairment in recognizing the light blue color. Foreign national badges have a light blue color border around the applicant photo. |
| <b>International Partners</b>   | International partners will have a flag of the applicant's country of citizenship in the lower right corner of the badge in addition to the light blue foreign national color band and border.   |
| <b>Emergency Response Officials</b>   | Emergency response officials (ERO) will be recognized by a Red stripe containing the words "Emergency Response Official" on the bottom of the badge in Zone 12 per the requirements of NIST Special Publication 800-104. The back of an ERO badge contains text stating their position as ERO and access permissions after verification of the badge holder's identity.                    |

5.1.6 Emergency Response Officials (ERO) Badges - Emergency Response Office badges shall be issued only to the following persons:

a. EROs to include individuals who are:

(1) Continuity of Operations (COOP) and Continuity of Governance (COG) personnel associated with COOP at a NASA Center or an alternate operating site during emergency/crisis situations. This includes only those persons who are members of the Emergency Relocation Group (ERG) and their respective support staff and Emergency Operation Center (EOC) personnel who are appropriately certified and trained.

(2) Disaster response personnel for each facility who possess NIMS training or professional certifications.

b. Personnel to be deployed to support the NASA National Response Framework (NRF) Emergency Support Function (ESF) Annexes. Support personnel may not be issued the ERO PIV credential unless they possess the above mentioned NIMS training or professional certifications.

c. NASA, special agents, NASA, security police, or security officers who have graduated from NASA Federal Law Enforcement Training and members of the NASA Inspector General (IG) staff who are sworn law enforcement officers.

d. Center protective services and security staff who provide support, or other security functions for emergency/contingency operations as deemed necessary by the CCPS/CCS so long as they possess

the above mentioned NIMS training or professional certifications

e. Center Directors, Deputy Center Directors, and Directors of Center Operations and their deputies.

5.1.7 Personnel who will be fulfilling support duties shall be issued a NASA PIV credential, without the ERO designation, to facilitate verification of identity and ease movement through the various checkpoints. Support personnel may not be issued the ERO PIV credential unless they possess the above mentioned NIMS training or professional certifications.

5.1.8 Table 5.1.8 details the color coding for Center-specific badges:

***Table 5.1.8, Color Coding for Badges***

| <b>Employee Type</b>        | <b>Color Coding</b>  |
|-----------------------------|--|
| <b>Contractor</b>           | Non-PIV contractors will be recognized by a blue lower section. Non-PIV contractors at JPL (an FFRDC) who are U.S. citizens will be recognized by a silver lower section with red lettering for the "JPL (an FFRDC)" Center designation on their Center-specific badges. |
| <b>Foreign Nationals</b>    | Non-PIV foreign nationals will be recognized by a blue lower section designation on their Center-specific badges.  |
| <b>Detailees</b>            | Non-PIV Detailees will be recognized by a white lower section designation on their Center-specific badges.   |
| <b>Interns and Grantees</b> | Interns and grantees will be recognized by a Center-specific badge with a white lower section designation on their Center-specific badges.   |

5.1.9 Badges for Press Corps - The press corps shall be recognized by the word "PRESS" printed vertically down the right side of the Center-specific badge. U.S. press corps will be further recognized by a brown lower section. Foreign national press will also contain all characteristics from the foreign national color coding as detailed in Table 5.1.5.

## **5.2 NASA PIV Credential Data**

5.2.1 Data printed on a NASA PIV credential shall consist of:

- a. Name (last name, first name, and middle initial);
- b. Photo;
- c. Affiliation (civil servant, detailees, contractor, grantee, or foreign national, etc.);
- d. Badge expiration date;
- e. Badge number consisting of a three-digit Center code plus six unique digits and printed as a number on the front, and a 3x9 bar code on the back;
- f. Height, eye color, and hair color;
- g. Agency card serial number; preprinted and used for tracking card stock; and
- h. Issuer Identification consisting of a six character department code, the agency code for NASA, and a five-digit issuing facility number.

5.2.2 The digital data stored on the NASA PIV credential supports physical and/or logical access use, encryption, and signing capability and provides security and authentication protection for the PIV credential and PIV credential holder.

5.2.2.1 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:

- a. Federal Agency Smart Credential Number (FASC-N);
- b. NASA Agency code;
- c. System code identifying the original issuing Center;
- d. A credential number;
- e. PIV credential holder's UUPIC; and
- f. Expiration date.

5.2.2.2. Digital Certificates

a. PKI X.509 certificates are used for authentication of the PIV credential and digital signing, encryption, and authentication of the PIV credential holder.

b. Credentials used for logical access have a certificate for PIV credential authentication. Additional certificates are loaded based on the duties and needs of the PIV credential holder.

5.2.2.3 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 re-create an image of that biometric.

5.2.2.4 Digital Representation of Printed Information - Certain items printed on the front and back of the card are stored on the chip as a security and authentication measure including name; affiliation; organization; badge expiration date; Agency card serial number; and issuer identification.

5.2.2.5 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.

5.2.2.6 The Personal Identification Number (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 PIV credential holder and written to the PIV credential during finalization. It is not stored in the identity management system and should not be written down or otherwise recorded by the PIV credential holder. The PIV credential is automatically locked after no more than 15 consecutive tries of entering an invalid PIN. PIV credential PIN reset details and requirements for resetting a PIN are identified in Section 6.7.

## **5.3 The Uniform Universal Personal Identification Code (UUPIC)**

5.3.1 UUPIC System Management - The UUPIC system is the database and application that stores personnel information required for the creation of unique identities, and that generates the UUPIC. This system shall be owned by OPS, working in concert with the OCIO and OHCM, to ensure proper functioning, assignment, use, and protection of the UUPIC system. OPS are responsible for administrative identity management in the UUPIC system. The UUPIC system will be treated as a high confidentiality, integrity, and reliability system. Access to the system will be controlled by two-factor authentication, firewalls, and encryption techniques. The UUPIC generated by the system may be available to NASA employees for lookup and may be used for positive identification of individuals within NASA information systems. However, the UUPIC may not be used as a login identifier or user account name for any information systems, databases, Web sites, etc. Additionally the UUPIC may not be used for purposes other than those described above without the concurrence of the AIMO and the Director of Agency Workforce Systems, within OHCM (or assigned delegate), with the exception of account initiation in the identity management system. System owners requiring access to the UUPIC system will submit a signed Service Level Agreement (SLA) and/or MOU to OPS.

5.3.2 Approval to Access the UUPIC System - The system owner requiring access to the UUPIC system shall submit a signed SLA/MOU to the ICAM Logical Access Management team detailing the purpose for accessing the UUPIC system. The ICAM Logical Access Management team will work with the system owner to ensure proper documentation and authority to access the UUPIC system. The ICAM Logical Access Management team will make a recommendation to approve or disapprove UUPIC system access to the AIMO. In the event of a denial for UUPIC access, the requesting system owner may appeal by sending a letter, along with the SLA/MOU, to OPS and OCIO. OPS and OCIO will respond with a final decision within 60 days of receipt of the appeal.

5.3.3 UUPIC Characteristics - UUPICs shall only be issued through the population of seed data (name, SSN, or foreign national visitor number for foreign nationals without a SSN, and date of birth) into the UUPIC database. This information is required for all NASA civilians, contractors, partners, and virtual IT system users. Any request for an UUPIC will be initiated via an approved work-flow method. The UUPIC database will auto-populate the NIMS, IDMS, and EPACS upon returning a UUPIC number. The reliable assignment of the UUPIC to persons uses at least two unique attributes, in addition to name attributes, from the documents as specified in the Department of Justice Form I-9, Employment Verification Data. The Agency directory is used as the UUPIC repository for general access to the UUPIC number. UUPIC numbers will be issued in random sequence, consistent with NASA policy, and will meet the following requirements:

- a. Is a nine-digit numerical code without any significance as to the characteristics of the individual;
- b. Is displayed as a set of 3 x 3 x 3 numbers, for example: 123 456 789; and
- c. Cannot be reverse engineered based on other data contained in the UUPIC application.

5.3.4 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. Therefore, the UUPIC may not be used as a login identifier or user account name for any information systems, databases, Web site, etc. With the exception of account initiation in NIMS, 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 the AIMO. 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 an UUPIC will be initiated via the approved workflow method. The UUPIC database will auto-populate the appropriate identity management systems upon returning a UUPIC number. 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.

# Chapter 6. PIV Credential Management Lifecycle

## 6.1 PIV Credential Inventory

6.1.1 Ownership. A PIV credential is not personal property, but is the property of the U.S. Government. All personnel shall be responsible for appropriately safeguarding issued credentials, immediately reporting the loss or false use of a PIV credential, challenging non-credentialed personnel, notifying the proper authority of a name change, properly displaying a PIV credential when on NASA property, and surrendering a PIV credential upon resignation, retirement, or the direction of the issuing authority.

6.1.2 Reciprocity. PIV credentials issued by other Federal Government departments and agencies shall be accepted for the purpose of establishing the identity of the individual.

6.1.3 Misuse. Forging, falsifying, or allowing misuse of a PIV 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.

6.1.4 Production. Printing of credentials shall only be performed by approved personalization service providers and will be shipped directly to a Center by the service provider.

6.1.5 Stock protection. Unprinted or unfinalized PIV credentials shall be shipped directly to a Center by the PIV credential manufacturer. The PIV credential issuing facility manager or other appropriate authority will designate a point of contact that is responsible for receipt of, signing for, and inventory and storage of PIV credential stock. PIV credential stock will be accessible only by authorized personnel and maintained in a secure manner, pursuant to Section 6.2, PIV Credential Storage and Handling. PIV 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 PIV credential stock check-ins or check-outs.

## 6.2 PIV Credential Storage and Handling

6.2.1 Credentials shall be stored using the following minimum requirements:

- a. Properly identified and treated as "controlled material" for inventory;
- b. Segregated from classified materials, firearms, ammunition, or currency; and
- c. Stored in a secure area protected by guard(s), key lock(s), and/or card reader(s).

6.2.2 Credentials which are lost, stolen, or unaccounted for while in storage shall be reported immediately or within 24 hours to the PIV credential issuing facility manager after discovery. PIV credential details, including PIV credential identification numbers and status, will be reported to the NEACC within 24 hours of discovery in order to update the card management system. The PIV credential issuing facility manager will forward a report outlining all pertinent facts to the OPS Security Management Division Director no later than two days after receiving reports of the lost, stolen, or unaccounted for credentials.

6.2.3 A defective PIV credential shall be identified, reported, and delivered to the core technical team. The issuance official will record the defective PIV credential identification number and the defective status in the PIV credential storage log. A new PIV credential will be created following Sections 3.4.4 of this document.

6.2.4 All PIV credential encoding failures shall be reported to the core technical team within five days of discovery and include the identification number, failure description, and any other pertinent information.

6.2.4.1 PIV credential encoding failures include:

- a. Rejection by a card reader or machine;
- b. Error message(s) during encoding of the PIV credentials; and
- c. PIV credential is not recognized by physical access control systems (PACS) or logical access control systems (LACS).

6.2.4.2 If the PIV credential becomes defective as a result of the encoding failure, refer to Section 6.2.3 of this NPR.

## 6.3 Final Adjudication and Subsequent Investigation

6.3.1 Final adjudication may occur at any time in the process. Final adjudication should be conducted within 90 days of receipt of the background investigation. Final adjudication may occur after the issuance process has completed and an applicant has received a PIV credential following favorable fingerprint check results. Upon receipt of the background investigation, the authorizer shall adjudicate the results of the background investigation as favorable or unfavorable. This adjudication will be documented and performed in accordance with OPM policy.

6.3.2 When background investigation results are favorable, the authorizer shall update the applicant's record to reflect favorable adjudication of the background investigation and the background investigation indicator in the PIV credential data model will be set to indicate background investigation completion. When background investigation results are unfavorable, the authorizer will update the applicant's record to reflect unfavorable determination of the background investigation result. The authorizer will revoke all physical and logical access rights associated with the PIV credential. The PIV credential will be immediately confiscated. The sponsor will be notified of the denial decision.

6.3.3 The PIV credential holder shall be provided the opportunity to appeal, pursuant to NPR 1600.3. If the PIV credential holder does not appeal or if the appeal is denied, the identity associated with the confiscated PIV credential will be terminated and the credential will be destroyed.

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

6.4.1 NASA shall provide an electromagnetically opaque badge holder selected from an approved products list to physically protect the badge and electronically protect the information contained in the badge. 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. The badge will be properly displayed and worn at all times while the bearer is on a NASA Center or component facility. They will be worn above the waist on the outermost garment with the photograph visible. The use of a permanent-type symbol or the affixing of any device (e.g., tenure pin, decals, etc.) on a PIV credential (or any alteration or modification

thereof) is not allowed.

6.4.2 PIV credentials held by both civil servants and contractors shall be accepted at all Centers for access to public areas and authorized IT resources at that Center. Access to non-public areas at each Center will be handled on an as-needed basis in compliance with the policies established by that Center for access to facilities and/or IT resources. Silver JPL contractor PIV credentials will be accepted at all NASA Centers.

6.4.3 NASA Center-specific and visitor badges shall only be used for access to the Center or facility from which it was issued. NASA Center-specific and visitor badges may be used for access to secure NASA computer systems and networks. Policies for temporary access to NASA IT resources are addressed by NPR 2810.1.

6.4.4 The visitor badge shall only be valid for the term issued, pursuant to section 3.3.4, NASA Visitor Badges. The visitor badge will be returned at the end of the visit. Individuals who are issued an escort required visitor badge will be escorted by an individual holding a valid NASA PIV credential.

6.4.5 A CCS may establish Center-specific badges for the following purposes:

- a. To provide access for relatives, guardian, or next of kin to wellness facilities (child care, health care, etc.);
- b. To provide visual verification in the absence of electronic verification for PIV credentials issued by another Federal agency and department; and
- c. To recognize retirees and other individuals previously affiliated with NASA (such as ex-astronauts) who no longer require access for official NASA business.

6.4.6 PIV credential usage requirements related to logical access are established in the NASA Subscriber Agreement, provided to and signed by the applicant for:

- a. Authorized uses of the PIV credential; and
- b. Authorized uses of the PKI certificates and services provided with the PIV credential.
- c. Additional usage requirements for logical access credentials are established in NPR 2810.1, Security of Information Technology.

6.4.7 The background investigations associated with the issuance of the Common Access Card (CAC) by DoD have been determined by OPM to be equivalent to the background investigation requirements for issuing a PIV credential. Centers will continue to issue a NASA Center-specific badge that reflects the individual's authorization to access the Center. This differentiates the DoD employee working at a Center from the one at home on leave. PIV credentials issued by other Federal Government agencies will be accepted for the purpose of identity verification at a Center. Access will be granted to the facility using a NASA Center-specific badge or the PIV credential with a card reader to establish granted access rights.

## **6.5 PIV Credential Renewal**

6.5.1 Credential renewal shall occur prior to PIV credential expiration and facilitate replacement of the PIV credential without the need to repeat the full enrollment and reissuance procedures described in Section 3.5. PIV credential holders may apply for a renewal starting six weeks prior to the expiration date on their PIV credential. The PIV credential holder will coordinate with the sponsor, who ensures personnel records are accurate and current before the issuance of a new PIV credential.

New biometrics are collected as described in Section 3.5.4. The old and/or expired PIV credential is to be collected and destroyed at the time of renewal pursuant to Section 6.14, PIV Credential Destruction. If warranted, the authorizer will approve the renewal and coordinate the request for a new background investigation to be performed. If a renewal is in process and is not completed before the enrollment is completed then the credential must be re-issued as described in Section 6.6.

## **6.6 PIV Credential Re-issuance**

6.6.1 The old PIV credential shall be revoked, pursuant to Section 6.8, PIV Credential Revocation for the following conditions and the applicant will undergo the entire registration and issuance process. PIV credential re-issuance will occur when the PIV credential:

- a. Has reached its expiration date;
- b. Has been compromised;
- c. Is lost, stolen, or damaged; or
- d. Requires a change in printed information (name change, citizenship change, etc.) or card holder's status.

6.6.2 NASA PIV credentials shall not be re-issued for an individual transferring from one Center to another.

6.6.3 PIV credential holders who have officially changed their name shall submit a request for a reissuance of their PIV credential. The PIV credential holder will be required to reenroll and provide approved USCIS Form I-9 documentation that reflects the legal name change prior to enrollment occurring and issuance of the new PIV credential.

## **6.7 PIV Credential PIN Reset**

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 PIV credential holder to arrange for a PIN reset to occur. Biometric verification of the applicant's biometrics to the biometrics stored on the card will occur prior to the PIV credential being returned to the applicant. PIN reset does not require the reissuance of a PIV credential.

## **6.8 PIV Credential Revocation**

6.8.1 Credentials shall be revoked under the following conditions:

- a. Exit on duty;
- b. Change in need for access;
- c. Termination of employment;
- d. Unfavorable fingerprint check or background investigation determinations; or
- e. Death of the PIV credential holder.

6.8.2 Revocation of a PIV credential shall result in the following:

- a. The PIV credential holders' relationship shall be set to "inactive;"
- b. The PIV credential shall be returned and terminated; and
- c. Notification shall be provided to the sponsor of the PIV credential revocation.

## 6.9 Lost and Stolen Credentials

6.9.1 Lost and stolen credentials shall be reported to the PIV credential Issuing Facility Manager within 18 hours of discovery of the loss/theft. The PIV credential holder will, within five business days of reporting the loss/theft, appear in person at the badging office and provide their SSN or Foreign National Management System Identification Number (FNMSID) to verify loss/theft of the PIV credential and be issued a new PIV credential. The lost/stolen PIV credential will be revoked and/or disabled, cancelling all certificates and access privileges of that card. The identity of the PIV credential holder itself will remain active, as only the card is disabled. The PIV credential holder will be required to undergo a PIV credential re-issuance, Section 6.6 PIV Credential Re-issuance. Until the new PIV credential is created, the PIV credential holder will obtain a visitor or Center-specific PIV credential and temporary non-PIV logical access credentials per NPR 2810.1, Security of Information.

6.9.2 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 PIV credential holders who report their PIV credential as lost or stolen on multiple occasions. The following list is not comprehensive and additional methods may be chosen by the Center:

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

## 6.10 Forgotten Credentials

6.10.1 It is the responsibility of NASA Centers to establish policy for the handling of forgotten credentials. Centers may adopt any number of the below methods for managing PIV credential holders who forget their PIV credential. The following list is not comprehensive and additional methods may be chosen by the Center:

- a. Require the PIV credential holder to retrieve the PIV credential;
- b. Allow issuance of a visitor badge to the PIV credential holder with verification of identity through an USCIS Form I-9 document such as a driver's license; or
- c. Suspend the forgotten PIV credential until the PIV credential holder appears in the badging office with the forgotten PIV credential for it to be activated.

## 6.11 PIV Credential Suspension

Credentials shall be set to "suspended" and temporarily disabled when the PIV credential has been misplaced and the PIV credential holder knows the current location of the PIV credential but cannot retrieve it at this time. Lost or stolen credentials will be handled pursuant to section 6.9, Lost and Stolen Credentials. The PIV credential holder will appear at the badging office, no later than 18

hours after discovery of the misplacement, and file a report stating the PIV credential has been misplaced and provide the location of the PIV credential that was last known. Until the PIV credential is recovered or declared lost or stolen, the PIV credential holder will obtain a visitor or Center-specific credential. PIV credential holders will report to the badging office within five business days of the original report to update the PIV credential status as being recovered, lost, or stolen. Lost and stolen credentials will adhere to section 6.9, Lost and Stolen Credentials. Credentials that are found will be set to "active" upon report of the PIV credential being found and visual confirmation of the PIV credential. Any Center-specific or visitor badge that was issued will be returned.

## 6.12 PIV Credential Return

6.12.1 Credentials shall be returned 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 PIV credentials that are returned and properly storing the PIV credentials until destruction. Credentials are not allowed to be kept as souvenirs. The responsibility of PIV credential return oversight will be:

- a. HR for NASA civil servant;
- b. Contract program manager for contractors;
- c. Grant administrator for grantees; or
- d. IVC for foreign nationals.

## 6.13 PIV Credential Termination

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 PIV credential and associated identity will be completed within 18 hours of notification of the need for PIV credential termination. Terminated credentials will be destroyed following the requirements in section 6.14, PIV Credential Destruction.

## 6.14 PIV Credential Destruction

6.14.1 Credentials meeting the following criteria shall be destroyed:

- a. Expired credentials;
- b. Credentials discovered or located after being declared lost or stolen;
- c. Credentials that are damaged; and
- d. Terminated credentials.

6.14.2 Credentials shall be thoroughly destroyed using heavy-duty cross cut shredders that are capable of smart card destruction, by depositing into a burn bag for burning, or by more rigorous methods.



# Appendix A: Definitions

**Access** - The ability to obtain and use information and related information processing services; and/or enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).

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

**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 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 Government.

**Asset** - A system, object, person, or any combination thereof that has importance or value; includes contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources.

**Authorized holder** - Anyone who satisfies the conditions for access to classified information in accordance with Section 4.1 (a) in Exec. Order No. 13,526.

**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.

**Center Chief of Security (CCS)** - The senior Center security 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.

**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 who is subject to Executive Order 11246..

**Credential** - A physical/tangible or electronic object through which data elements associated with an individual are bound to the individual's identity. Credentials are presented to access control systems in order to gain access to assets.

**Debarment** - Official determination made in writing by the Center Director or CCS that bars, for

cause, an individual from accessing NASA property.

Escort - The management of a visitor's movements and/or accesses implemented through the constant presence and monitoring of the visitor by appropriately designated and properly trained U.S. Government or approved contractor personnel. Training shall include the purpose of the visit, where the individual may access the Center, where the individual may go, whom the individual is to meet, authorized topics of discussion, etc.

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

Executive Order (EO) - An order issued by or on behalf of the President, usually intended to direct or instruct the actions of executive agencies or Government officials, or to set policies for the executive branch to follow.

Foreign National - A synonym for "foreign person" (see definition of "Foreign Person" below).

Foreign Person - Any person who is not a U.S. citizen and who is not a lawful permanent resident as defined by 8 U.S.C. 1101(a) (20) or any person who is not a protected individual as defined by 8 U.S.C. 1324b(a) (3). This also means any foreign corporation, business association, partnership, trust, society or any other entity or group that is not incorporated or organized to do business in the U.S., as well as any international organizations, any foreign government, and any agency or subdivision of foreign governments (e.g., diplomatic missions).

Grant Recipient - Organization (i.e., universities, nonprofits, etc.) or individual that has received official designation and funding to perform specific research on behalf of NASA.

I-9 document - One of the documents listed on the OMB Form I-9, Employment Eligibility Verification.

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 a Registration Authority (RA) when attempting to establish an identity or issue a credential.

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 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.

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) - Replaces the term "Permanent Resident Alien (PRA)" - A non-U.S. citizen, legally permitted to reside and work within the U.S. and issued the Resident Alien Identification (Green Card). Afforded all the rights and privileges of a U.S. citizen with the exception of voting, holding public office, employment in the federal sector (except for specific needs or under temporary appointments per 5 CFR, Part 7, Section 7.4), and access to classified national security information (CSNI). (NOTE: LPR's are not prohibited from accessing export controlled commodities, but will still have a work-related "need-to-know" and are still considered

foreign nationals under immigration laws.

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, information technology systems and applications. Name check - A background check procedure performed by the Federal Bureau of Investigation (FBI). The FBI name check is performed by the FBI as a part of the National Name Check Program which dates back to EO 10450, issued during the Eisenhower Administration. The FBI name check for an individual involves a search of the FBI's Central Records System Universal Index for any appearance of the name of the individual, as well as close phonetic variants and permutations of that name, in any of the records stored in the Universal Index. If any such occurrences are found, the name check also involves retrieval and analysis of the relevant paper and electronic files from local FBI offices and from other law-enforcement agencies. NASA-Controlled Facility - NASA Centers and individual facilities where access is controlled by issuance and mandatory use of photo-identification badges, armed security force personnel, and electronic access control systems to ensure only authorized personnel are admitted.

NASA PHOTO-ID - Refers to the NASA photo-ID that has any number of imbedded and external technologies capable of activating any type of facility, IT, or personal recognition access control system. Technology shall include: Exterior bar code and magnetic stripe embedded proximity chip, and embedded "smart card" chip.

NASA National Agency Check - A Check conducted electronically by NASA Security Offices of the files of the FBI (including fingerprint files), Office of Defense Central Index of Investigations (DCII), the Office of Personnel Management (OPM), or other Government agencies, as appropriate. The files of the Bureau of Immigration and Customs Enforcement (BICE), the Central Intelligence Agency (CIA), and the U.S. State Department shall be reviewed, as available, when the individual is a resident alien or naturalized citizen of the United States.

National Agency Check (NAC) - The NAC is a search of the following four indices:

- a. U.S. Office of Personnel Management (U.S. OPM) Security/Suitability Investigations Index (SII) contains investigations completed by U.S. OPM and by other Federal agencies.
- b. Federal Bureau of Investigation (FBI) Identification Division (FBIF) contains a fingerprint index and name file.
- c. FBI Records Management Division (FBIN) contains files and records of all other investigations (e.g., background, criminal, loyalty, intelligence); and
- d. Defense Clearance and Investigations Index (DCII) contains investigations, including criminal investigations, conducted on civilian and military personnel in the Department of Defense.

(Note: The NAC is not a background investigation. It is one of the components that make up a background investigation.)

National Agency Check and Inquiries (NACI) - The NACI is a NAC that also includes written inquiries sent to employers, educational sources, law enforcement agencies, and references. The NACI is the minimum acceptable investigation for access to government facilities.

Non-designated Country - A country with which the United States has favorable diplomatic relations.

Permanent Resident Alien (PRA) - A non-U.S. citizen legally permitted to reside and work within the United States and issued the Resident Alien Identification (Green Card). Afforded all the rights

and privileges of a U.S. citizen with the exception of voting, holding public office, employment in the Federal sector (except for specific needs or under temporary appointments per 5 CFR, Part 7, Section 7.4), and access to CNSI.

(NOTE: PRA's are not prohibited from accessing export controlled commodities but will still have a work related "need-to-know" and are still considered Foreign nationals under immigration laws.)

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.

Revocation - The removal of an individual's eligibility to access physical or logical assets based upon an adjudication that continued access poses a risk to the Agency.

Risk Acceptance - 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 Assessment - A formal process whereby a project, program, or event is evaluated to determine the types and level of risk associated with its implementation.

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

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.

Transient - A person (i.e., construction worker, club member, childcare drop off/pickup, delivery driver, retiree, Center transit, and others approved by Center Chiefs of Protective Services/Security) who requires intermittent access for 180 days or more.

U.S. Person (non-U.S. Citizen) - For the purpose of implementing protection and accountability under the ITAR; a person who is a 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). It also means any corporation, business association, partnership, society, trust, or any other entity, organization or group that is incorporated to do business in the U.S. It also includes any governmental (Federal, state, or local) entity. It does not include any foreign person as defined in this chapter.

Visitor - Any person who needs physical access to a NASA facility for less than 30 days.

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

# Appendix B: Acronyms

|        |   |
|--------|---|
| AA     | Associate Administrator                               |
| AIMO   | Agency Identity Management Official                   |
| BPL    | Business Process Lead                                 |
| C&A    | Certification and Accreditation                       |
| CA     | Certification Authority                               |
| CAC    | Common Access Card                                    |
| CBP    | Customs and Border Patrol                             |
| CCS    | Center Chief of Security                              |
| CHUID  | Cardholder Unique Identifier                          |
| CIA    | Central Intelligence Agency                           |
| CISO   | Chief Information Security Officer                    |
| CNSI   | Classified National Security Information              |
| CPR    | Card Production Request                               |
| COG    | Continuity of Governance                              |
| COOP   | Continuity of Operations                              |
| COTR   | Contracting Officer's Technical Representative        |
| CSCA   | Commercial Space Competitiveness Act                  |
| CSLA   | Commercial Space Launch Act                           |
| CSO    | Center Security Office                                |
| CTTA   | Certified Tempest Technical Authority                 |
| DAA    | Designated Accreditation Authority                    |
| DCII   | Defense Clearance and Investigations Index            |
| DoD    | Department of Defense                                 |
| EOC    | Emergency Operations Center                           |
| 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                            |
| FASC-N | Federal Agency Smart Credential Number                |
| FBI    | Federal Bureau of Investigation                       |

|        |   |
|--------|---|
| FBIN   | Federal Bureau of Investigation Records Management Division |
| FICAM  | Federal Identity, Credential, and Access Management         |
| FIPS   | Federal Information Processing Standards                    |
| FISMA  | Federal Information Systems Management Act                  |
| FNMS   | Foreign National Management System                          |
| FNMSID | Foreign National Management System Identification Number    |
| GAO    | Government Accountability Office                            |
| GIC    | Grant Information Circular                                  |
| HLPV   | High-level protocol visitors                                |
| HR     | Human Resources   |
| HRO    | Human Resources Office                                      |
| HSPD   | Homeland Security Presidential Directive                    |
| ICAM   | Identity, Credential, and Access Management                 |
| ICE    | Immigration and Customs Enforcement                         |
| ID     | Identification  |
| IdMAX  | Identity Management and Account Exchange                    |
| IDMS   | Identity Management System                                  |
| IG     | Inspector General   |
| IIF    | Information in Identifiable Form                            |
| IPA    | Intergovernmental Personnel Act                             |
| ISAA   | International Space Act Agreement                           |
| IT     | Information Technology                                      |
| ITAR   | International Traffic in Arms Regulations                   |
| ITSM   | Information Technology Security Manager                     |
| IV&V   | Independent Verification & Validation                       |
| IVC    | International Visit Coordinator                             |
| JPL    | Jet Propulsion Laboratory                                   |
| LACS   | Logical Access Control System                               |
| LAM    | Logical Access Management                                   |
| LPR    | Lawful Permanent Resident                                   |
| MEI    | Mission Essential Infrastructure                            |
| MOU    | Memorandum of Understanding                                 |
| NAC    | National Agency Check                                       |
| NAFI   | Non-Appropriated Funds Instrumentality                      |

|        |  |
|--------|--|
| NEACC  | NASA Enterprise Applications Competency Center                 |
| NFLET  | National Federal Law Enforcement Training                      |
| NCIC   | National Crime Information Center                              |
| NIMS   | National Incident Management System                            |
| NIST   | National Institutes of Standards and Technology                |
| NM     | NASA Memorandum  |
| NPD    | NASA Policy Directive  |
| NPR    | NASA Procedural Requirements                                   |
| NRF    | National Response Framework                                    |
| OCIO   | Office of the Chief Information Officer                        |
| OMB    | Office of Management and Budget                                |
| OPM    | Office of Personnel Management                                 |
| OPS    | Office of Protective Services                                  |
| PACS   | Physical Access Control System                                 |
| PCI    | Personal Card Issuer   |
| PDR    | Position Risk Determination                                    |
| PKI    | Public Key Infrastructure                                      |
| PIA    | Privacy Impact Assessment                                      |
| PIF    | PIV Issuing Facility   |
| PII    | Personally Identifiable Information                            |
| PIN    | Personal Identification Number                                 |
| PIV    | Personal Identity Verification                                 |
| PIV-I  | PIV Interoperable  |
| POC    | Point of Contact   |
| PSO    | Protective Services Office                                     |
| RSA    | Remote Secure Access   |
| SAO    | Senior Authorizing Official                                    |
| SATERN | System for Administration, Training, and Educational Resources |
| SAVE   | Systematic Alien Verification for Entitlements                 |
| SII    | Security/Suitability Investigations Index                      |
| SLA    | Service Level Agreement  |
| SORN   | System of Records Notice                                       |
| SP     | Special Publication  |
| SSN    | Social Security Number   |

|       |  |
|-------|--|
| TCAC  | Transition Common Access Card                  |
| TTCP  | Technology Transfer Control Plan               |
| USCIS | United States Citizen and Immigration Service  |
| UUPIC | Universal Uniform Personal Identification Code |

# Appendix C: NASA PIV Photo Identification Badge Standards

**Table C-, NASA Photo Identification Standards**

|  |                             |  |
|--|-----------------------------|--|
| 1. LETTERING   | COLOR-FONT                  | POINT  |
| a. Badge No: #####   | Black-Helvetica             | 6pt. Upper & lower case. Left Justified.         |
| b. First/MI/Last Name  | Black-Helvetica             | 12 pt. Upper & lower case. Lower left justified. |
| c. Center Numerical Designation  | Black-Helvetica             | 18 pt. Lower left.                               |
| d. P.O. Box  | Black-Helvetica             | 6 pt. Upper & lower case. Bottom centered.       |
| 2. NASA PHOTO-ID STANDARD FEATURES   | CHARACTERISTIC              | SIZE   |
| a. Photograph  | Color                       | (2.9cm x 3.9cm) 7 x 9 picas.                     |
| b. Card Stock  | Standard                    | (5.5cm x 8.6cm) 13 x 20.3 picas.                 |
| c. Strap Slot (authorized for Center specific photo-ID only.                     | Precut & Centered           | (1.4cm x .3cm) 3.5 x 7 picas.                    |
| d. Logo  | Silhouette of Space Shuttle |  |
| e. Reliability color for all Photo-ID  | White                       |  |
| 3. COLOR CODING  | CARD COLOR                  |  |
| a. Civil Service   | WHITE                       |  |
| b. Consultant/Contractor/Press   | GREEN                       |  |
| c. Military/Other Agency (Detailee)  | WHITE                       |  |
| d. Interns/Co-Ops, Summer Students   | WHITE                       |  |
| e. Foreign National  | BLUE                        |  |
| f. Jet Propulsion Laboratory, a Federally Funded Research and Development Center | SILVER                      |  |
| 4. CENTER  | CENTER ALPHA DESIGNATOR     |  |
| a. Ames Research Center  | ARC                         |  |
| b. Dryden Flight Research Center   | DFRC                        |  |
| c. Glenn Research Center   | GRC                         |  |
| d. Goddard Space Flight Center   | GSFC                        |  |
| e. NASA Headquarters   | HQ                          |  |

|  |      |
|--|------|
| f. Jet Propulsion Laboratory, a Federally Funded Research and Development Center | JPL  |
| g. Johnson Space Center  | JSC  |
| h. Kennedy Space Center  | KSC  |
| i. Langley Research Center   | LARC |
| j. Marshall Space Flight Center  | MSFC |
| k. Stennis Space Center  | SSC  |

## PART 2.

## Privacy Act Notice

a. General - Pursuant to 5 U.S.C. 552a, Public Law 93-579, Privacy Act of 1974, as amended, the following information is being provided to persons who are asked to provide information in order to obtain a NASA Personal Identity Verification (PIV) Card.

b. Authority - This information is collected under the authority of the National Aeronautics and Space Act, 51 U.S.C. § 20132, and Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons.

c. Purposes and Uses - The primary use of collecting the information requested by this form is to facilitate the issuance of a NASA PIV Card. Social security numbers are requested to keep NASA records accurate because other employees may have the same birth date. When collected, this information shall be maintained in NASA Privacy Act Systems of Records (10SECR). Generally, the information contained in this category of records is used within NASA for determining suitability for Federal employment and access to classified information (security clearances), as well as access to security areas, NASA Centers, and other matters connected with security programs and operations.

d. In addition to the internal uses of such information, it shall also be disclosed to Federal, state, local, or foreign agencies in connection with official business, including law enforcement, intelligence activities, determinations concerning access to classified information, and matters concerning immigration. Information connected with law enforcement or administrative inquiry or investigation will be disclosed to NASA contractors, subcontractors, or grantees. Disclosure will also be made to the White House or Congressional offices in the course of certain inquiries. Additionally, in the event of a courts or formal administrative proceeding, information will be disclosed in the course of presenting evidence or during pretrial discovery. NASA will disclose information to the Department of Justice or other agencies in connection with such a proceeding.

e. Effect of Non-Disclosures - Providing this information is voluntary. However, if the form is not completed, a NASA PIV Card shall not be obtained. This may result in various undesired actions such as disqualification for employment or access.

# Appendix D: Subscriber Agreement

## D.1 NASA Public Key Infrastructure (PKI) Subscriber Agreement (HSPD-12 compliant badge) (version 1.0, August 2007):

D.1.1 YOU SHALL READ THIS NASA PKI SUBSCRIBER AGREEMENT BEFORE REQUESTING, ACCEPTING, OR USING A NASA HSPD-12 COMPLIANT BADGE. BY SUBMITTING A REQUEST FOR A NASA HSPD-12 COMPLIANT BADGE, YOU ACKNOWLEDGE YOUR ACCEPTANCE OF THE TERMS OF THIS SUBSCRIBER AGREEMENT.

D.1.1.1 By submitting a request for a NASA HSPD-12 compliant badge you agree to use the badge and any related NASA PKI certificate and services only in accordance with this Subscriber Agreement, including:

D.1.1.2 Make true representation at all times regarding information in your HSPD-12 compliant badge request, related Public Key Certificate request, and other identification and authentication information related to a NASA PKI Certificate;

D.1.1.3 Use your badge exclusively for authorized NASA business such as to gain access to NASA facilities and/or systems;

D.1.1.4 Inform NASA within 24 hours of the loss of your badge;

D.1.1.5 Take reasonable precautions to protect your badge from loss, disclosure, modification, or unauthorized use;

D.1.1.6 Inform NASA within 48 hours of a change to any information included in your HSPD-12 compliant badge request and related Public Key Certificate application;

D.1.1.7 Return the badge to NASA upon expiration, demand by NASA, or when you no longer require the badge, for reasons including job transfer, extended leave, resignation, or termination of employment. NASA HSPD-12 compliant badge contains a NASA Public Key Certificate suitable for providing authentication.

D.1.1.8 Failure to abide by NASA certificate policies and practices may constitute grounds for revocation of certificate privileges, and may result in administrative action and/or criminal prosecution under the computer fraud and abuse act (18 U.S.C Sec. 1030 (c)). NASA reserves the right to refuse to issue a NASA Public Key Certificate. Additional information regarding NASA Public Key Certificates is available at <http://nasaca.nasa.gov/docs.html>.

D.1.1.9 This agreement shall be governed by and construed in accordance with United States Federal law. NASA badges and Public Key Certificates are deemed Government supplied equipment, and as such, all users are bound by U.S. Federal law governing the use of Government provided equipment.

D.1.1.10 If any provision of this Agreement is declared by a court of competent jurisdiction to be invalid, illegal, or unenforceable, all other provisions shall remain in force. Further information, including HSPD-12 badge applicant rights and responsibilities, is available on the Agency Web site at <http://hspd12.nasa.gov>.

## **D.2 Account Access:**

The following statement describes your responsibility for using the badge for logical access to NASA computer assets: Unauthorized use of the computer accounts and computer resources to which I am granted access is a violation of Federal law; constitutes theft; and is punishable by law. I understand that I am the only individual to access these accounts and will not knowingly permit access by others without written approval. I understand that my misuse of assigned accounts and my accessing others' accounts without authorization is not allowed. I understand that this/these system(s) and resources are subject to monitoring and recording, and I will have no expectation of privacy in my use of and content on these systems and the computer equipment. I further understand that failure to abide by these provisions may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution. (NPR 2810.1A, 11.3.3.2)

## **D.3 Statement:**

I hereby certify that the information provided by me is true and correct to the best of my knowledge and belief. I certify that I am the individual described in the NASA badge request. I agree to maintain control of the badge at all times once my fingerprint activates it and upon receipt and to abide by the agreements above. Once issued to me, I will immediately notify the Center Protective Services Office (Security) if I discover that it is not under my control due to misplacement, loss, or other cause.