NM 1600-95
NRW 1400-45
NPD 1600.2

NASA Interim Directive

Effective Date: June 3, 2011
Expiration Date: June 3, 2012

COMPLIANCE IS MANDATORY

NASA Identity and Credential Management

Responsible Office: Office of Protective Services

Table of Contents

Preface

P.1 PURPOSE

a. This NASA Interim Directive (NID) 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.

b. This NID 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 NID is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to JPL, other contractors, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

b. This NID 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

The National Aeronautics and Space Act, as amended, 51 U.S.C. § 20113(a)

P.4 APPLICABLE DOCUMENTS

a. 5 Code of Federal Regulations Sections 731.202 and 731.501

b. E-Gov Act of 2002, Public Law 107-347, 44 U.S.C. Ch 36

c. Executive Order 10450 of April 17, 1953 (as amended)

d. Executive Order 12968 of August 2, 1995

e. Federal Acquisition Regulation Clause 52.204-9, Personal Identity Verification (PIV) of Contractor Personnel

f. Federal Information Processing Standards Publication 201 (FIPS 201)

g. Homeland Security Presidential Directive 12 (HSPD-12)

h. NASA Procedural Requirements (NPR) 1600.1, Security Program Procedural Requirement

i. NPR 1382.1, NASA Privacy Procedural Requirements

j. NPR 2810.1, Security of Information Technology

k. NASA Grant Information Circular (GIC) 06-02, September 22, 2006

l. NIST Special Publication (SP) 800-79, Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations

m. NIST SP 800-104, A Scheme for PIV Visual Card Topography

n. Office of Management and Budget (OMB) Memo M-05-24, of August 5, 2005, "Implementation of Homeland Security Presidential Directive (HSPD) 12 -Policy for a Common Identification Standard for Federal Employees and Contractors"

o. Privacy Act of 1974, U.S. Public Law 93-579, 1974.

p. X.509 Certificate Policy for the U.S. Federal Public Key Infrastructure (PKI) Common Policy Framework, v2.5 16 OCT 2006

P.5 MEASUREMENT/VERIFICATION

To determine compliance with this NID, the 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 Office of Management and Budget (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. 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.

b. NASA Memorandum (NM) 1600-46, Security Identification System Requirements.

c. NM 1600-50, Photo Identification Color-Coding Requirements.

d. NM 1600-52, Personal Identity Verification Policy and Procedures.

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

CHAPTER 1. Introduction

1.1 Overview

1.1.1 In recent years, increasing emphasis has also been placed by the Federal Government on improving the physical security of the hundreds of thousands of facilities that the Federal Government owns and leases to support the diverse mission work of Federal agencies like NASA. 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. GAO has also outlined the need for standard performance metrics to evaluate the effectiveness of physical security protections.

1.1.2 This NID establishes the policies and high-level procedures that shall be used throughout NASA to achieve these improvements in physical security protections. 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 existing weaknesses within the NASA's physical security infrastructure.

1.1.3 Identity management and credential management are important not only to an effective physical security program but also to effective cyber security. In addition to complex cyber and physical security threats, NASA faces significant challenges in being able to carry out its mission activities in a manner that fulfills the needs of its business partners and the American public and appropriately leverages current information technology capabilities to enable electronic service delivery. These challenges lie in being able to verify the identity of an individual in the digital realm and to establish trust in the use of that identity in conducting business. Even low-risk employees possess access behind physical and locical safeguards that can give them unprecedented access to critical information and systems. As a result, strong, consistent and reliable ICAM capabilities throughout NASA are a critical factor in the success of all NASA's mission work. A common, standardized, trusted basis for electronic identity and access management within the NASA is needed to provide a consistent approach to deploying and managing appropriate identity assurance, credentialing, and access control services.

1.1.4 Despite a complex set of challenges, the NASA has made significant progress regarding ICAM in recent years. The Homeland Security Presidential Directive 12 (HSPD-12) program provides a common, standardized identity credential that enables secure, interoperable online transactions. This document codifies the policies and procedures that are necessary to sustain and maintain this capability.

1.2 Identity, Credential, and Access Management (ICAM) Governance

1.2.1 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.

1.3 Scope

1.3.1 The policies and procedures identified within this document define the approved processes for NASA to manage personal identities and the issuance to those identities 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 temporary badges. Non-PIV logical access tokens are not covered in this document. The policies and procedures for vetting an identity are covered in NID 1600, Personnel Security Procedural Requirements. 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 necessary to properly manage identity, credential, and access management (ICAM) services as an integrated end-to-end service to improve security, efficiency, and inter-Center collaboration are covered in NPR 2841.1 Identity, Credential, and Access Management Services.

1.4 Waivers and Exceptions

1.4.1 Centers may occasionally experience difficulty in meeting specific requirements established in the series of NASA Security Program NPRs, and so 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 CCS shall justify the exception request through security risk analysis: i.e., 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; inability of the CCS to perform its missions and goals, etc.

(1) Justification must 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 Center Chief of Security and the Center Chief Information Officer. The Center Director then either recommend approval or return the exception request to the CCS for further study or closure. The Center Director forwards concurrence to the Mission Support Directorate Associate Administrator at NASA Headquarters.

c. The Mission Directorate Associate Administrator shall forward exception requests to the Assistant Administrator (AA) for Protective Services at Headquarters or return proposals to the Center Director for further study or closure.

d. The AA for Protective Services shall return the exception request to the appropriate Center Director with an approved exception, for further study, or denial and closure.

CHAPTER 2. Roles and Responsibilities

2.1 Overview

2.1.1 All NASA employees and contractor employees as well as NASA tenants and contractors for NASA tenants will be required to comply with this Directive. Commercial or private entities and their contractors (all tiers) and employees needing physical or logical access per Economy Act, Space Act, Commercial Space Competitiveness Act (CSCA), Commercial Space Launch Act (CSLA) agreements also must comply with this directive. The Assistant Administrator, Office of Protective Services (OPS), is the system owner of all systems used to manage identities and to issue NASA PIV credentials. The Assistant Administrator, Office of Protective Services also has overall responsibility for ensuring uniformity of credential issuance policies and procedures throughout the Agency. All NASA organizational components shall adhere to the policies and procedures herein and promulgate implementing regulations, as required, consistent with the policies and procedures set forth herein. Center Directors, through their Center Office of Protective Services (OPS), supported by the Center Office of the Chief Information Officer (OCIO), Center Human Resources Office (HRO), Procurement Office, and other offices as necessary, shall 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 Card Issuer (PCI) Senior Authorizing Official (SAO) - The Assistant Administrator for the Office of Protective Services shall be the PCI Senior Authorizing Official (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 Personal Identity Verification Card Issuer (PCI) Designated Accreditation Authority (PCI DAA), Personal Identity Verification Card Issuer (PCI) Assessor, and the 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 Agency Identity Management Official (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 is 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 is 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 Protective Services 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 shall 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 shall have the appropriate skills, resources, and competencies to perform certifications of the Agency. The PCI Assessor conducts the PIV Certification and Accreditation (C&A), per NIST SP 800-79-1

2.2.5 NASA Enterprise Applications Competency Center (NEACC) - 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.

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 servant employee serving as the Center Chief of Security (CCS), Chief of the Protected 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 validates the individuals at the Center who perform the roles of PIV requester and PIV sponsor. The PIF Manager 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 reviews I-9 document discrepancies and provides determinations for the acceptance of the documents.

2.3.2 PIV Applicant - Per FIPS 201-1, the PIV Applicant is the individual to whom a PIV credential needs to be issued. The PIV applicant shall be a prospective or current NASA employee (e.g., either a civil servant or a federal contractor), requiring access to NASA facilities

and/or IT resources. The PIV applicant is responsible for providing demographic 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 C: Subscriber Agreement. The PIV applicant shall 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 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 PIV requester shall be an individual one of the following categories depending on the applicant affiliation:

a. Manager or authorized administrator of a specific NASA program or contract;

b. NASA Human Resources (HR) for prospective or current NASA employees;

c. NASA grant provider for grantees; or

d. International Visits Coordinator (IVC) for foreign nationals.

2.3.3.2 The PIV requester creates the initial request for a PIV applicant to receive a NASA federal credential.

2.3.4 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 federal civil servant 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). The PIV sponsor modifies, as necessary, incorrect or missing information in the credential issuance request. The PIV sponsor is an individual from the identified entity for the following applicant affiliation:

a. HR specialist for NASA civil servant 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 Enrollment Official - The PIV Enrollment Official is 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 completion of the background checks. The role of 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 I-9 identity source documents for authenticity, captures copies and/or scans of the I-9 documents, compares the name and demographic data in the PIV credential request and the I-9 documents, and determines whether any discrepancies exist on an applicant's I-9.

2.3.6 PIV Authorizer - The PIV Authorizer covers the portions of the PIV Registrar 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 shall be a Federal employee. The PIV authorizer shall hold no other role in the identity management or credential issuance process for a given identity. The PIV authorizer shall hold no role other than applicant in the issuance of their credential. The PIV authorizer must be trained in adjudication by an accredited provider of adjudication training. The PIV authorizer reviews the PIV credential request, the PIV sponsor's endorsement, and confirms that 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 Office of Personnel Management's (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 results of the fingerprint check and background investigation results and approves or denies NASA PIV credential issuance. The 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 NPR 1600.X2 NASA Personnel Security Procedural Requirements.

2.3.7 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 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 check and background investigation as they are received;

f. recording results of the fingerprint check;
g. updating PIV applicant information when necessary; and

h. rejecting a PIV applicant's application when necessary.

2.3.8 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 maintain records and controls for PIV credential stock to ensure that stock is only used to issue valid credentials. The role of PIV issuance official shall be performed by personnel authorized by the Center Chief of Security. The PIV issuance official issues NASA PIV credentials to approved PIV applicants. The PIV issuance official encodes and prints the NASA PIV credential 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 - According the FIPS 201-1 the PIV Digital Signatory is the entity that digitally signs the PIV biometrics and CHUID.

2.3.10 PIV Authentication Certification Authority (CA) - The PIV Authentication Certification Authority 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 roles of PIV Applicant, PIV Sponsor, PIV Enrollment Official, and Issuer are mutually exclusive. No individual shall hold more than one of these roles in the identity proofing and registration process. The PIV Issuer and PIV Digital Signatory roles may be assumed by one individual or entity.

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 meet the applicable requirements established by the appropriate accreditation process.

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 role involved in the PIV issuance process. Re-certification is required each year to ensure training is up-to-date and conducted with the most recent system updates. Training records are

maintained by the SATERN computer based training system or subsequent/succeeding system(s). End-user training is provided on an as-required basis to Agency personnel. Technical and user training are available through computer based training or on-site "desk-side coaching" sessions on an as-needed basis. Day-to-day operations' training is provided to system operators and administrators to ensure that they have a thorough understanding of the systems and related components being managed.

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

f. E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36)

2.6.2 As prescribed by the Office of the Chief Information Officer, NASA shall conduct and maintain a Privacy Impact Assessment (PIA) of the identity management program. NASA shall 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) shall 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 to limit who has legitimate access to those identity management systems they maintain. NASA shall ensure privacy of applicant information is sustained through all steps of identity management including enrollment and issuance. PIV credential issuance facilities shall 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 website, 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 shall be posted in every enrollment and issuance location, on the applicable NASA website, 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 for those denied a PIV credential or whose PIV credential is revoked; and

c. sanctions for employees violating NASA privacy policies.

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 shall establish procedures for notifying applicants when their PII is lost, damaged, becomes corrupt, or stolen.

2.6.8 NASA shall normally discipline any individuals violating the privacy requirements established in this chapter in compliance with NASA guidelines established in NPR 1382.1 NASA Privacy Procedural Requirements.

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 (2) 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 have 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

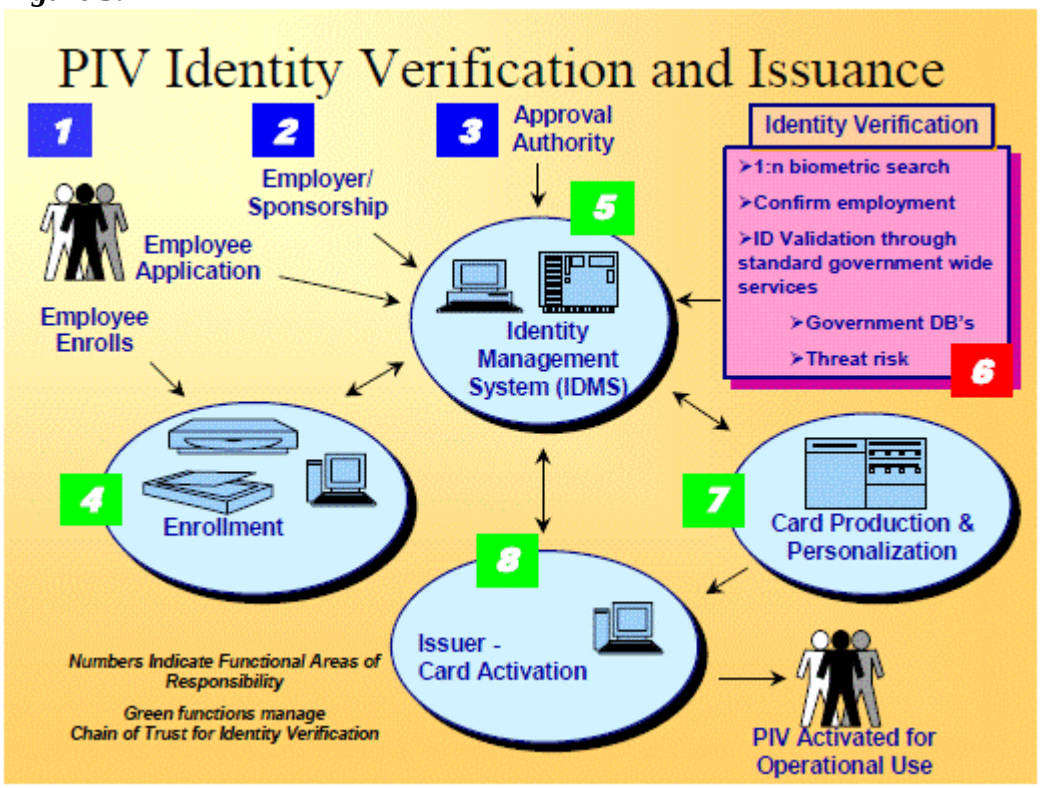
e. any additional documents used in the enrollment and issuance process.

CHAPTER 3. Enrollment and Credential Issuance

3.1 Overview

3.1.1 The NASA Identity Management and Credential Management Process are designed to conform to the system-based model for identity proofing, registration and issuance process that is described in NIST FIPS 201-1and is represented diagrammatically in that 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 granted via NASA PIV Credentials. NASA PIV Credentials allow physical only, logical only, and both physical and logical access to resources at NASA. Each NASA credential is linked to an established identity and must go through the appropriate issuance steps as outlined in this chapter. NPR 2810.1, Security of Information Technology for policy and procedures regarding NASA non-PIV credentials that allow access to only logical systems. NASA visitor badges are NASA non-PIV badges which allow only physical access to NASA Centers. For short-term visitors, Centers are authorized to issue Center-specific badges (i.e. NASA non-PIV badges) for physical access to that Center based on a risk-based determination documented as part of the permanent record. 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 issued to all persons who have been deemed as needing access to NASA Centers, Facilities, and IT systems and resources for a period exceeding 179 days in a 365-day period. These persons include all NASA employees, all NASA contractors, agreement partners,as well as non-NASA tenants in NASA facilities. NASA PIV credentials shall be issued to both U.S. citizens and foreign nationals. NASA PIV credentials shall be issued following the complete identity-proofing, registration, and issuance processes defined in this document for the management of identities of all new and current employees, contractors, and affiliates including foreign nationals. NASA PIV credentials shall not be issued without, at a minimum, completion of a FBI fingerprint check and subsequent completion of a National Agency Check with inquires (NACI) background investigation. NASA PIV credentials shall have an expiration date set for a period not to exceed 5 years from the Card Production Request (CPR) generation date. NASA PIV credentials shall not be issued to individuals holding a federal PIV credential issued by another federal entity or to individuals holding a PIV-I credential issued by an organization whose PIV-I credentials conform to the federal PIV-I standard. Exceptions to this policy may be made only when the exception has been formally documented and approved via the process described in section 1.4 of this document. The exception request must specifically explain why non-NASA credential is not usable in the NASA ICAM services.

3.3.3 Any person (i.e., NASA employee, NASA contract personnel, non-NASA tenant, or other category of individuals such as volunteers, guest researchers, interns, grantees, etc.) who will be affiliated with NASA and its Centers or Facilities for a period of 179 days or less shall be issued a NASA non-PIV badge (i.e., a NASA temporary badge). The 179-day period begins the first day of affiliation and ends 179 calendar days later regardless of the work schedule. If an individual's affiliation extends past 179 days in a 365-day period, the individual must be issued a NASA PIV credential if the individual is a NASA employee (either a civil servant or a federal contractor employee). All other individuals (volunteers, guest researchers, interns, grantees, etc.) may be from the 179-day limit on use of a NASA non-PIV badge consistent with risk-based assessments by CCS/CPS. Issuance of NASA non-PIV badges requires at minimum a favorable adjudication of a National Crime Information Center (NCIC) name query and completion of steps 1-4 of section 3.5, On-Site Enrollment and Issuance Procedures. Escort requirements for

individuals with a NASA non-PIV badge shall be based on risk-determination by the Center Chief of Security.

3.3.4 NASA visitor badges may be issued to individuals requiring access to a NASA Center for a period not to exceed 29 days in any single visit and not more that a cumulative total of 29 days in a 365-day period. Individuals needing access beyond 29 days must be issued a NASA Non-PIV Temporary badge. Issuance of NASA visitor badges requires completion of steps 1-3 of section 3.5, Enrollment and Issuance, and shall include capture of the visitor's photograph section 3.5.4, Step 4: Enrollment Process. Visitors requiring access to a NASA Center for more than 5 days shall undergo a minimum of a National Crime Information Center name query. Escort requirements for individuals with visitor badges shall be based on risk-determination by the Center Chief of Security.

3.3.5 NASA Center-specific badges may be issued to accommodate unique situations of the Center not otherwise accommodated by NASA PIV credentials, NASA non-PIV badges, and NASA visitor badges. All NASA Center-specific badge Templates shall have the approval of the Agency Identity Management Official prior to their creation and utilization. NASA Center-specific badges shall be issued upon completion of a minimum FBI fingerprint check. Issuance of these badges shall be based on a risk-based access determination by the Center Chief of Security. NASA Center-specific badges may be issued to individuals who hold a PIV credential issued by another federal government agency or department if their current non-NASA PIV credential does not work at the NASA Center. This may include contractors from another NASA Center in the event that electronic verification of a need to be on the NASA Center is not available at a point of entry. Issuance of NASA Center-specific badges requires completion of 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.

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

3.4 Applicant Types

3.4.1 NASA employees are Federal civil servants employed and paid by NASA. NASA Employees also includes individuals employed and paid by another entity but working for NASA under an Interagency 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 contractors are individuals working under contract with the responsibility to perform activities for NASA.

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

3.4.4 Detailees are either Federal employees from other-Federal Agencies, or U. S. military personnel, or non-Federal employees working at NASA through an Intergovernmental Personnel Act (IPA) assignment. Any badges issued to a Detailee shall be designated with an affiliation of "NASA" and shall appear as a federal employee badge. The Center PIF Manager shall 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 temporary badge by NASA.

3.4.5 International Partners are individuals, working for agencies or organizations of foreign governments, foreign education institutions, foreign companies, or international organizations, engaged in a program of international cooperation in work done pursuant to a Space Act Agreement as defined by NPD 1050.1H, Authority To Enter Into Space Act Agreements. A signed international agreement must 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. There may or may not be a "Formal" agreement associated with a tenant (example: Credit Union). The tenant may require logical access to certain NASA applications. A tenant may work for another government agency as either a civil servant or contractor and may have a PIV badge from this other agency. Tenants include those entities and their contractors and employees under Economy Act, Space Act, Commercial Space Competitiveness Act (CSCA) or Commercial Space Launch Act (CSLA) agreements are those individuals needing physical or logical access based on the above authorities. The tenant may work for a company that is leasing space on a NASA facility but does not work on a NASA-related project.

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

3.5.1 Step 1: Credential Request - A requester completes a credential request within IdMAX for an applicant. The requester submits the request to the sponsor via IdMAX. The information submitted includes the following:

a. Name of the applicant;

b. Date of Birth of the applicant;

c. Position of the applicant;

d. Contact information for the applicant;

e. Name of the requester;

f. Organization of the requester; and

g. Contact information for the requester.

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

3.5.3 Step 3: Check for Background Investigation - The authorizer or Investigation Reviewer validates the receipt of the request from the sponsor. The authorizer and supporting staff review the Office of Personnel Management (OPM) and other federal databases and take appropriate steps to validate the applicant's investigation status with regard to a current investigation.

a. 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.

b. 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.

3.5.4 Step 4: Enrollment Process - The Enrollment Official validates the receipt of the request from the authorizer. The sponsor advises the applicant that they must appear in-person before the Enrollment Official and present two forms of identity source documents in original form. The applicant appears in-person before the authorized Enrollment Official and presents two forms of identity source documents in original form per Form I-9, one of which must 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.

a. Enrollment fingerprints - The applicant’s fingerprints are captured. If the applicant currently has a background investigation on file or in progress, only flat fingerprints are required to be captured. If no background investigation is on file or in progress, both flat and rolled fingerprints are required to be captured. In cases where there is difficulty in collecting fingerprints due to damage, injury or deformity, NASA shall perform authentication using asymmetric cryptography for authentication. The facial image collected from the applicant during enrollment can also be used for authenticating badge holders covered under Section 508 of the Rehabilitation Act.

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

reasons may be obtained by written application to the AA for Protective Services who may refer the matter for a recommendation to a NASA Headquarters Access Appeals Panel.

c. Enrollment I-9 Documentation - The Enrollment Official obtains and maintains a legible photocopy or scan copy of the original I-9 documentation. Any document that appears invalid (e.g., absence of security hologram, or other known security features, on a State issued driver's license; security features on a birth certificate or passport; smeared ink, etc.) is to be rejected by the Enrollment Official and reported to the proper authority for review. Photocopies of rejected documents are to be made and retained for a period not to exceed one year, or until any appeal process is completed. I-9 documents that do not pass electronic examination, if available, are rejected and another approved I-9 document must 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 shall be used to update the applicant identity record.

d. Enrollment Subscriber Agreement - The Enrollment Official provides the applicant with the Subscriber Agreement, Appendix C, Subscriber Agreement, and obtains 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 are 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 may use the results of a NCIC to process the PIV credential request. The authorizer makes a determination based upon receipt of the fingerprint check results, or evidence of an acceptable existing background investigation (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 submits a PIV credential issuance request to authorize the creation and issuance of a PIV credential In instances where a badge is to be issued, the authorizer notifies the sponsor and requester that the badge issuance has been authorized. Final adjudication of the record is performed in compliance with NASA personnel security policies.

3.5.6 Step 6: Badge Production Process - The Issuance Official validates the receipt of the issuance request from the authorizer. The Issuance Official initiates a badge printing. If the badge is to be printed remotely at a commercial facility or a shared service provider, the necessary information is included in a batch card creation request. The initialized and printed badges are returned to NASA and forwarded to the appropriate Issuance Officials where the credentials shall be held in a secure location. If the badge is to be produced locally, the Issuance Official prints the identity information onto the card and compares the photo to the identity database. The badge shall be encoded with the identity and biometric data of the applicant. The encoded badge shall be tested. The applicant shall 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 printed in a batch job or previously printed on-site, the Issuance Official obtains the card stock from storage. If the badge is to be printed on-site, the Issuance Official obtains a blank badge from storage, verifies the identity of the applicant against the database, and prints the badge. The Issuance Official checks the printed badge to verify the identity of the applicant, conducts a biometric match and encodes the badge with an applicant entered PIN number. Upon completion of the badge printing and encoding, the badge is officially released to the applicant. An approved electronically shielded badge holder shall be offered to the applicant in order to protect the badge and the privacy of information on the badge.

CHAPTER 4. Foreign Nationals

4.1 Overview

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 shall have identity proofing and vetting accomplished in the same manner as U.S. Citizens.

4.1.1 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. Sponsorship for the foreign national shall be determined. If a foreign national is not under a contract where a COTR has been officially designated, the foreign national shall provide information directly to their visit/assignment host, and the host shall fulfill the duties of the sponsor as required herein; and

c. Pre-visit identity vetting shall be conducted.

4.1.2 This Chapter outlines the requirements that NASA personnel shall follow in granting access by foreign nationals to NASA physical or information technology resources for any purpose other than a tour of facilities that is or would normally be conducted for the general public The sub-sections outline the processes, procedures and authorizations necessary to successfully obtain required access permissions in a timely manner. These requirements apply to foreign national civil servants, contractors, researchers, international partners as defined via International Space Act Agreements (ISAA), as well as high-level protocol visitors (HLPV), 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.

4.1.3 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 International Visit Coordinator (IVC). In the event that 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 Office of Protective Services for review and approval (see section 1.4 of this document). Suggestions for process improvements are welcome and should be addressed to the NASA Office of Protective Services, Headquarters Office, Washington, DC 20546.

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 information technology 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 be conducted in conformance with Agency and national policies and regulations, including U.S. national security, nonproliferation and foreign policies, and export control laws and regulations.

4.2.2 Visits and other access for the purpose of implementing a mutually agreed program or project must be conducted in accordance 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 must be limited to information which has been approved for release 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 web page at http://oiir.hq.nasa.gov/nasaecp) are coordinated initially through the Center IVC, then shall be forwarded to NASA Headquarters External Relations, Export Control and Program Points-of-Contact (as necessary) for review and final approval. Only after final approval shall a foreign national be provided access to NASA physical or information technology assets.

4.3 Processing On-Site Visit Requests

4.3.1 SA 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 for any purpose. All foreign national access requests other than for public tour shall undergo an identity vetting process based on visit type, foreign national residency, and country affiliation. The Center IVC shall approve the requests for foreign nationals from non-designated countries. Requests for foreign nationals from designated countries shall be forwarded and approved by Headquarters Office of External Relations for review and approval before final approval by the Center IVC.

4.3.2 If the visit is for the purpose of 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 should 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 has been previously approved for release to the general public. All identity proofing and vetting for foreign nationals from non-designated countries shall be performed at the Center. The requirement to forward all IT access requests to Headquarters is

rescinded. This eliminates steps (thus time) in the process and does not create new processes for the Centers. All current Center review processes shall continue as they do now at each Center's discretion.

4.3.3 Only NASA personnel holding active PIV credentials shall be allowed to escort foreign nationals.

4.3.4 Centers shall accept 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 one is from a Designated country, shall be processed as from a Designated country.

4.3.6 NASA Center personnel will 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 3 years or more a background investigation (i.e. NACI or equivalent) must be initiated after employment authorization is appropriately verified through e-Verify (or immigration status is appropriately verified for those individuals not working for NASA through the USCIS Systematic Alien Verification for Entitlements (SAVE) system).

a. For foreign nationals in the U.S. or a U.S. territory for less than three years, NASA Center personnel will delay the background investigation until the individual has been in the U.S. or a U.S. territory for three years. 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 must be verified and an FBI fingerprint based criminal history check must be completed. Center personnel will request an FBI Investigations Files (name check search), a name check against the Terrorist Screening Database, and a USCIS Check against SAVE. Some of these database checks may be requested directly from OPM or through automated tools such as NCIC and Visual Compliance

b. 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 an automated tool,

(1) Visual Compliance Unverified List

(2) Entities List

(3) Denied Persons List

(4) Debarred Parties List

(5) Specially Designated Nationals

(6) Terrorist database

4.3.7 Foreign national non-PIV credentials shall be issued for a maximum period of three years, 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, 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. Foreign nationals on visa waivers shall present their current passport/visa 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 For foreign nationals in the U.S. greater than three years to receive a PIV credential, they MUST 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 will be allowed to access all Center perimeters without additional identity proofing or vetting. Additional access (physical or IT) shall be determined by the physical or IT asset owner and coordinated through the Center's International Visits Coordinator prior to the foreign national's arrival at the receiving Center. For Centers who use Physical Access Control Plans, they must be valid and accurate. Technology Transfer Control Plans (TTCP), as required by Export Control, must 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 IT Remote Access ONLY will be enabled by the IVC after approval in IdMAX. There is no Federal requirement for Identity vetting for foreign national Remote IT Only Access. NASA collects basic information that allows us to approximate level of assurance for user ID/password and/or RSA token access to IT assets. 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. 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, assure the following:

a. Where fingerprints are captured at a location other than the Center Security Office, the transmission of those fingerprints to the Center Security Office must be from a valid law enforcement agency or other accredited fingerprint provider.

b. To ensure a chain of trust, the fingerprint cards shall be delivered to the Center Security Office by the entity that took the fingerprints.

c. Any foreign national having access to NASA data must 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 in the form of 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 must be performed annually.

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 shall 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 shall 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 that may be necessary while the foreign national is at a NASA facility.

4.4.2 To expeditiously process the request, the sponsor shall provide the following information 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) Social security number (if one is available)

(h) Foreign national number (if no SSN is available)

(i) Contact information

(j) Sponsor name

(k) Physical access requirements

(l) Information technology access requirements (on-site and/or remote)

(m) Export control data access requirements (including license requirements)

(n) NASA affiliation (civil servant, contractor, partner, etc.)

(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 shall 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 Technology Transfer Control Plan (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 information technology access requirements. Determine circumstances whereby escort only status shall be applied. Review and approve TTCP, if accessing NASA physical resources.

(d) The Center Security Office shall begin the background investigation based on visit type, foreign national residency, and country affiliation and commensurate with risk levels outlined in the TTCP.

(e) The Counterintelligence/Counterterrorism Office shall perform their background investigation (as needed) and report results back to the Center Security Office.

(f) With the Export Control Office, 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 information technology resources.

(g) With the Information Technology Security Manager (ITSM), review information technology access requirements (on-site and remote), and make risk-based determination on access protocols. Review and approve TTCP, if accessing NASA information technology 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 External Relations (if the individual is part of the NASA Exchange Visitor Program), obtain endorsement from the appropriate Enterprise/Functional Office at

NASA Headquarters. Review and approve TTCP for physical and information technology 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 information technology 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 shall provide the final approval.

4.6.2 Centers or Programs may specify restrictions regarding physical or information technology (IT) access privileges or escort requirements that are more restrictive than those documented in this NID.

4.6.3 If a foreign national will be accessing multiple Centers, it will be incumbent on the foreign national's sponsor and Center IVC to collaborate with affected Centers to determine which access and escort restrictions apply at which Center.

4.6.4 If a foreign national will be accessing an information technology resource from multiple locations (including remote), it will be incumbent on the foreign national's sponsor and system owner to determine how that access will be provisioned at multiple locations.

4.6.5 The IVC shall coordinate input for identity vetting, physical access, and information technology 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 shall forward all information to the Headquarters Export Control Office, External Relations Desk Officer and (as required by the Program), the Headquarters Program Point-of-Contact for review and approval. The Headquarters Export Control Office, External Relations Desk will then forward the approval back 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 shall provide the final approval.

4.7 Implementation

4.7.1 Once all approvals have been received, the IVC shall report back to the foreign national's sponsor the terms and conditions of the on-site assignment. The sponsor shall assure implementation of the foreign national's access credentials. The sponsor shall assure 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 provide the sponsor with the Appeals process.

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 shall be escalated to the Agency Identity Management Official (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" shall be performed. In instances where a NACI cannot be rendered, a determination shall be made between the Program Manager and the Chief for Center Security 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 shall expire at the end of the program/project or contract term. Investigation status information shall be updated annually. Access to information technology resources will be administered with a non-PIV credential.

4.8.2 If a foreign national is working for 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 for "Foreign National Works at Overseas NASA Location."

4.8.3 If a foreign national is coming to NASA periodically as an accredited news media representative, the IVC shall coordinate with the Center Public Affairs Office to obtain requisite information. Once the IVC has determined that agreement has been reached on requirements, the IVC shall coordinate with the Chief for Center Security 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 shall be issued. Investigation status information shall be updated annually. Access to information technology resources will be administered with a non-PIV credential.

4.8.4 If a foreign national is coming to 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 shall forward all information to the Headquarters External Relations Desk Officer and Export Control (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 coming to 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 assure that the foreign national is part of an existing International Space Act Agreement (ISAA) partnership. Once the IVC has determined that agreement has been reached on

requirements, including completion of the TTCP (if necessary), the IVC shall forward all information to the Headquarters External Relations Desk Officer and Export Control (if TTCP was created) for review and approval.

4.8.7 No NASA funding is provided to the foreign national under the NASA Visitor Exchange Program. All funding must come from the foreign sponsor or from personal funds, and NASA must assess if the funds being made 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 NPR 2810.1, computer and network access.

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

4.9.2 U.S. citizens 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. If a U.S. citizen is found to have committed espionage (i.e., giving/selling data to a foreign entity), they will be prosecuted as a U.S. citizen. The minimum identity vetting process for a full-time civil servant or contractor working at a NASA facility is the National Agency Check with written 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 IdMAX versus the Foreign National Management System (FNMS). The credential provided to LPRs shall be the blue stripe LPR credential. This credential shall conform to the color coding requirements for Zone 15 described in NIST Special Publication 800-104. The letters “LPR” shall be displayed superimposed on the NASA logo in the lower right hand corner of the front of the 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 shall be issued an LPR proximity credential only following the requirements described in section 3.4.6.

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

4.10.1 Foreign nationals who have been resident in the U.S. for less than three years shall undergo the following identity vetting process:

(a) A Visual Compliance database check that reveals no violations or derogatory information

(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 proximity credential (foreign national Blue) shall be issued. The term of issue will be the length of assignment or time in which the foreign national is resident in the U.S. for three years whichever is shorter.

4.10.3 Foreign nationals who have been resident in the U.S. for three years 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 a 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 shall require a minimum annual revalidation of the Visual Compliance database search along with an NCIC check. The foreign national blue credential shall be issued based on the results of the identity vetting revalidation. 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 is 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. FBI finger print check (foreign national must be escorted until favorable finger print results are returned). Foreign nationals may then be issued a Center-specific temporary foreign national visitor credential.

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 apply. 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 are applicable:

a. If foreign national 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. If foreign national has resided in the U.S. for less than 36 months, must undergo identity vetting 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 Office of Management and Budget (OMB) Circular A-130, and NPR 2810.1, NASA has established security requirements and procedures to assure an adequate level of protection for NASA Information Technology (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 handle and the risk of magnitude of loss or harm that could be caused by the individual.

4.12.2 Foreign national access to "limited privileged" IT systems shall be allowed only if the foreign national is involved in a program member under an International Space Act Agreement (ISAA). The sponsor shall verify that an ISAA is in place. The sponsor has accountability for assuring the security of IT system data being accessed by the foreign national.

4.12.3 IT Remote Access ONLY 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. 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, assure the following:

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

4.12.5 Any foreign national having access to NASA data must 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 in the form of 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 must be performed annually.

4.12 Escort Requirements

4.12.1 Identity vetting requirements established here do not preclude each Center Security Office from enacting their requirements regarding access to the Center, buildings, or other secured areas. Access requirements for foreign nationals are outlined in the TTCP.

4.12.2 It is incumbent on the IVC to 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 abide by those requirements.

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 imbedded 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 (MMM YYYY format), and the second to the right of the applicant photograph, below the Agency identifier, and over the Agency logo (YYYYMMMDD format);

(4) the NASA Agency identifier logo;

(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;

(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; and

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 imbedded chip. Temporary badges shall not resemble the NASA PIV credential.

a. Temporary badges 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 photograph of the applicant;

b. the legal name of the applicant;

c. the full name of the issuing Center; and

d. 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 shall not contain technologies that allow for physical (beyond recognition by Center security) or logical access. Center-specific badges shall contain the following printed information:

a. the photograph of the applicant;

b. the legal name of the applicant;

c. the name of the issuing Center (Center name may be common abbreviation, e.g., ARC, DFRC, et alia, as appropriate).

5.1.5 Visual Color Coding for Employee Type - NASA PIV and temporary 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 temporary 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 temporary badges as described in Table 5.1.5:

Table 5.1.5

Employee Type	**Color Coding**
Federal Employee	A plain white color band
Contractor Employee	Contractors shall 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.
Contractors at the NASA Jet Propulsion Laboratory (JPL)	Contractors at the NASA Jet Propulsion Laboratory (JPL) who are United States (U.S.) citizens shall be recognized by the addition of a solid silver color below the green contractor color band.
Interagency Personnel Agreement (IPA) Employee	A plain white color band. The lower right corner on the front of the badge the label "LPR" shall appear in black letters.
Foreign Nationals	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.

Employee Type	Color Coding
International Partners	International Partners shall 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.
Emergency Response Officials	Emergency Response Officials shall 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 Emergency Response Official (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 may 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 continuity of operations 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 National Incident Management System (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 NFLET 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 Center Chief of Protective Services/Center Chief of Security 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 will be issued 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 temporary badges:

Table 5.1.8

Employee Type	**Color Coding**
Contractor	Temporary contractors shall be recognized by a dark blue lower section. Temporary contractors at JPL who are U.S. citizens shall be recognized by a silver lower section with red lettering for the "JPL" Center designation.
Foreign Nationals	Temporary Foreign Nationals shall be recognized by an orange lower section.
Detailees	Temporary Detailees shall be recognized by a green lower section.
Interns and Grantees	Interns and grantees shall be recognized by a temporary badge with a purple lower section.

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 temporary badge. U.S. press corps shall be further recognized by a brown lower section. Foreign national press shall 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 consists of:

a. Name (Last Name, First name and middle initial);

b. Photo;

c. Affiliation (Civil Servant, Detailee, Contractor, Grantee, or Foreign National, etc.);

d. Badge Expiration Date;

e. Badge Number consisting of a three (3) 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 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.
a. 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:

(1) Federal Agency Smart Credential Number (FASC-N) composed of:

(2) NASA Agency Code;

(3) System code identifying the original issuing Center

(4) A credential number; and

(5) PIV credential holder's UUPIC.

(6) Expiration Date

b. Digital Certificates

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

(2) 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.

c. 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.

d. 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.

e. 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.

f. 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. Section 6.7, PIV Credential PIN Reset details requirements for resetting a PIN.

5.3. The Universal Uniform Personal Identification Code (UUPIC)

5.3.1 UUPIC System Management - The UUPIC system shall be owned by OPS, working in concert with the OCIO, to ensure proper functioning, assignment, use, and protection of the UUPIC system. OPS is responsible for administrative identity management in the UUPIC system. The UUPIC system shall be treated as a high confidentiality, integrity, and reliability system. Access to the UUPIC system shall be controlled by two-factor authentication, firewalls, and encryption techniques. The UUPIC may not be used as a login identifier or user account name for any information systems, databases, web sites, et al. The UUPIC system may not be used for identification purposes outside those needed for positive identification of individuals within information systems without the concurrence of the Agency Identity Management Official, with the exception of account initiation in the identity management system. System owners requiring access to the UUPIC system must submit a signed Service Level Agreement (SLA) and/or Memorandum of Understanding (MOU) to OPS.

5.3.2 Approval to Access the UUPIC System - The system owner requiring access to the UUPIC system must 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 Agency Identity Management Official. 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 will only be issued through the population of seed data (name, Social Security Number or Foreign National visitor number for foreign nationals without a Social Security Number, 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 a UUPIC will be initiated via an approved work flow method. The UUPIC database will auto-populate the IdMAX, 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 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 will serve as a replacement for the Social Security Number 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, et al. With the exception of account initiation in the Identity Management System, 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 Agency Identity Management Official. The UUPIC may never be posted on any Internet accessible web site. Any deviation from this policy must be coordinated with OPS through OCIO in advance. Requests for a UUPIC must 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. It is the property of the U.S. Government. All personnel are responsible for appropriately safeguarding issued credentials, immediately reporting the loss or false use of a PIV credential, challenging uncredentialed personnel, notifying the proper authority of a name change, properly displaying a PIV credential when on Center, and surrendering a PIV credential upon resignation, retirement, or the direction of the issuing authority.

6.1.2 Reciprocity. PIV credentials issued by other 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 1 year, or both, and may further result in termination of employment and access to NASA resources.

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

6.1.4 Stock protection. Unprinted or unfinalized credentials shall be shipped directly to a Center by the PIV credential manufacturer. The PIV credential Issuing Facility Manager or other appropriate authority shall designate a point of contact who is responsible for receipt of, signing for, and inventory and storage of PIV credential stock. PIV credential stock shall 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 shall 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 are 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 stored in secure area protected by guard(s), key lock(s), and/or card reader(s).

6.2.2 Credentials which are lost, stolen, or unaccounted while in storage shall be reported immediately to the PIV credential Issuing Facility Manager and in a timeframe not to exceed 24 hours 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 shall forward a report

outlining all pertinent facts to the OPS Security Management Division Director no later than 2 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 shall record the defective PIV credential identification number and the defective status in the PIV credential storage log. A new PIV credential shall 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 or logical access control systems (PACS or 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 NID.

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 20 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 to determine if the results of the investigation are favorable or unfavorable. This adjudication shall 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 shall be set to indicate background investigation completion. When background investigation results are unfavorable, the authorizer shall update the applicant's record to reflect unfavorable determination of the background investigation result. The authorizer shall revoke all physical and logical access rights associated with the PIV credential. The PIV credential shall be immediately confiscated. The requester and sponsor shall be notified of the denial decision.

6.3.3 The PIV credential holder shall be provided the opportunity to appeal, pursuant to NPR 1600.2 NASA Personnel Security Procedural Requirements. If the PIV credential holder does not appeal or appeal is denied, the confiscated PIV credential shall be terminated.

6.4 PIV Credential Usage: Display, Protection and Proper Usage

6.4.1 NASA shall provide an electromagnetically opaque badge holder selected from an approved products list in order 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 must be properly displayed and worn at all times while the bearer is on a NASA Center or Component Facility. They shall be worn above the waist on the outermost garment; and with the side 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 shall be accepted at all Centers for access to public areas and IT resources at that Center. Access to non-public areas at each Center shall 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 shall be accepted at all NASA Centers. Contractor PIV credentials from another Center may be accepted following a risk-based decision at the visited Center. Tenant credentials and foreign national PIV credentials will only be accepted at the Center from which they were issued. Foreign national PIV credentials from other Centers must be accompanied by an approved visit request.

6.4.3 NASA temporary badges shall only be used for access to the Center or facility from which it was issued. NASA temporary 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 3.4.6, NASA Visitor Badges. The visitor badge shall be returned at the end of the visit and individuals issued a visitor badge shall be escorted by NASA PIV or NASA temporary badge holders based on risk-determination at the Center.

6.4.5 A Center Chief of Security may establish Center-specific temporary badges for the following purposes:

a. Providing access for relatives or next of kin requiring access to wellness facilities (child care, health care, etc.);

b. To provide visual verification in the absence of electronic verification for PIV credentials issued by other federal agency and department; and

c. Recognition of retirees and other individuals previously affiliated with NASA (such as ex-astronauts) who no longer requires 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. The DOD Transition CAC (tCAC) satisfies HSPD-12 as a PIV compatible credential and shall therefore be accepted as an appropriate identity credential for DOD personnel working on NASA facilities. The tCAC does not identify that the individual is authorized to access NASA facilities. Centers shall 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 shall be accepted for the purpose of identity verification at a Center. Access shall 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 registration process. PIV credential holders may apply for a renewal starting six weeks prior to the expiration date on their PIV credential. The PIV credential holder shall coordinate with the sponsor, who ensures personnel records are accurate and current before the issuance of a new PIV credential. 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 shall approve the renewal and coordinate the request for a new background investigation to be performed.

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 shall undergo the entire registration and issuance process. PIV credential re-issuance shall 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, etc.) or employee status.

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

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

6.7 PIV Credential PIN Reset

6.7.1 Credentials that are disabled or locked-out due to a maximum of 15 consecutive invalid PIN entry attempts shall have their PIN reset. It is the responsibility of the 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 shall 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.

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

a. the PIV credential holder's 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 24 hours of discovery of the loss/theft. The PIV credential holder shall, within five

business days of reporting the loss/theft, appear in person at the badging office and provide their Social Security Number (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 shall 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 shall 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 shall obtain a visitor or temporary PIV credential and NPR 2810.1, Security of Information Technology for logical access credentials.

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 (2) Credentials after which the PIV credential holder must 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 PIV credential to the PIV credential holder with verification of identity through an 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

6.11.1 Credentials shall be set to "suspended," temporarily disabled, when the PIV credential has been misplaced and the PIV credential holder knows the current location of the PIV credential. Lost or stolen credentials shall be handled pursuant to section 6.9, Lost and Stolen Credentials. The PIV credential holder shall appear at the badging office, no later than 24 hours after discovery of the misplacement, and file a report stating the PIV credential has been misplaced and the location of the PIV credential is known. Until the PIV credential is recovered or declared lost or stolen, the PIV credential holder shall obtain a visitor or temporary PIV

credential and NPR 2810.1, Security of Information Technology for logical access credentials. PIV credential holders shall 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 shall adhere to section 6.9, Lost and Stolen Credentials. Credentials that are found shall be set to "active" upon report of the PIV credential being found and visual confirmation of the PIV credential. Any temporary or visitor badge issued shall be returned.

6.12 PIV Credential Return

6.12.1 Credentials are to 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 shall be responsible for recording receipt of the PIV credential that are returned and properly storing the PIV credential until destruction. Credentials are not allowed to be kept as souvenirs. The responsibility of PIV credential return oversight shall 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

6.13.1 Credentials returned to the badging office that do not meet any of the requirements previously established in this chapter and are to be terminated shall have all data, certificates, and access privileges invalidated, revoked, and/or disabled. Credentials that are to be terminated shall have their status set to "terminated" and a reason shall be supplied for the termination. Deactivation of a PIV credential and associated identity shall be completed within 18 hours of notification of the need for PIV credential termination. Terminated Credentials shall 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, deposit into a burn bag for burning, or more rigorous methods.

APPENDIX A: DEFINITIONS

A.1 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, border crossing entrances.

A.2 Access Control. The process of granting or denying specific access requests.

A.3 Accreditation. Formal declaration by a Designated Approving Authority (DAA) that an information technology 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.

A.4 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.

A.5 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.

A.6 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.

A.7 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.

A.8 Center Chief of Security (CCS) - The senior Center security official who is responsible for management of the Center security program.

A.9 Certification - Used under two separate contexts in this NID:
a. 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.

b. A formal process implemented at the CCS level to ensure a room, vault, or security container meets minimum structural and physical security attributes necessary to ensure adequate protection of CNSI. Certified Tempest Technical Authority (CTTA) - Designated official responsible for performing Tempest countermeasures cost and security analyses prior to the implementation of Tempest countermeasures.

A.10 Component Facilities - NASA-owned facilities not located on any NASA Center (e.g., Michoud Assembly Facility, Wallops Flight Facility, White Sands Test Facility, NASA IV&V).

A.11 Contractor - For the purpose of this NID, any non-NASA entity or individual working on a NASA installation or accessing NASA information technology.

A.12 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.

A.13 Debarment - Official determination made in writing by the Center Director or Center Chief of Security that bars, for cause, an individual from accessing NASA property.

A.14 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.

A.15 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.

A. 16 Executive Order (EO) - Official documents, numbered consecutively, through which the President of the United States manages the operations of the Federal Government.

A.17 Foreign National - For the purpose of general security protection, considerations of national security, and access accountability: Any person who is not a citizen of the United States. Includes lawful permanent resident (i.e., holders of green cards) or persons admitted with refugee status to the United States. See definition of Lawful Permanent Resident (LPR) in this Chapter.

A.18 Foreign Person - Any person 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 United States, as well as any international organizations, any foreign governments and any agency or subdivision of foreign governments (e.g., diplomatic missions).

A.19 Grant Recipient - Organization (Universities, nonprofits, etc.) or individual that has received official designation and funding to perform specific research on behalf of NASA.

A.20 I-9 document – one of the documents listed on the OMB Form I-9, Employment Eligibility Verification

A.21 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.

A.22 Identity Proofing. The process for providing sufficient information (e.g., identity history, credentials, documents) to a Registration Authority (RA) when attempting to establish an identity or issue a credential.

A.23 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

A.24 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.

A.25 International Partners - Foreign nationals or U. S. citizen representatives of foreign governments, who are involved in a particular international program or project under an International Space Act Agreement (ISAA).

A.26 Lawful Permanent Resident (LPR) - Replaces the term "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 classified national security information. (NOTE: LPR's are not prohibited from accessing export controlled commodities but must still have a work related "need-to-know" and are still considered Foreign nationals under immigration laws. See definitions for “foreign national”, “foreign persons”, and “U.S. persons” in this chapter).

A.27 Logical Access. Access to information records, data, information technology systems and applications.

A.28 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.

A.29 NASA PHOTO-ID - refers to the NASA photo-ID that has any number of imbedded and external technology 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.

A.30 NASA National Agency Check - Conducted electronically by NASA Security Offices of the files of the Federal Bureau of Investigation (including fingerprint files), Office of Defense Central Index of Investigations (DCII), the Office of Personnel Management, or other Government agencies, as appropriate. The files of the Bureau of Immigration and Customs Enforcement (BICE), the Central Intelligence Agency, 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.

A.31 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.)

A.31 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.

A.32 Non-designated Country - Country with which the United States has favorable diplomatic relations.

A.33 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 classified national security information. (NOTE: PRA's are not prohibited from accessing export controlled commodities but must still have a work related "need-to-know" and are still considered Foreign nationals under immigration laws.)

A.34 Protected Persons - A non-U.S. citizen allowed into the country under "refugee," "displaced person," "religious," or "political" persecution status.

A.35 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.

A.36 Risk Acceptance - An official acknowledgement by a management officials that they accept the risk posed by not implementing a recommendation, or requirement, designed to reduce or mitigate the risk.

A.37 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.

A.38 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

A.39 U.S. Person (non-U.S. Citizen) - For the purpose of implementing protection and accountability under the ITAR; A person who is a lawful permanent resident (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 United , States. It also includes any governmental (federal, state, or local) entity. It does not include any foreign person as defined in this chapter.

A.40 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

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

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

NAFA – Non-Appropriated Funds Activity

NEACC – NASA Enterprise Applications Competency Center

NFLET – National Federal Law Enforcement Training

NCIC - National Crime Information Center

NID -NASA Interim Directive

NIMS – National Incident Management System

NIST - National Institutes of Standards and Technology

NM – NASA Memorandum

NPD – NASA Policy Directive

NPR - NASA Procedural Requirement

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 Unique Personal Identification Code

APPENDIX C: NASA PHOTO IDENTIFICATION BADGE STANDARDS

Table C-1

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. PO Box	Black-Helvetica	6 pt. Upper & lower case. Bottom centered.

2. NASA PHOTO-ID STANDARDFEATURES	**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	GOLD
b. Consultant/Contractor	BLUE
c. Military/Other Agency (Detailee)	GREEN
d. Interns/CO-Ops, Summer Students	VIOLET
e. U.S. National Press	BROWN
f. Foreign National (Non-Designated/Press)	ORANGE
g. Foreign National (Designated)	RED
h. Jet Propulsion Laboratory	SILVER

4. CENTER	CENTER ALPHA DESIGNATOR
a. Ames Research	ARC
b. Dryden Flight Research Center	DFRC
c. Glenn Research Center	GRC
d. Goddard Space Flight Center	GSFC
e. NASA Headquarters	HQS
f. Jet Propulsion Laboratory	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

General - Pursuant to Public Law 93-579, Privacy Act of 1974, as amended (5 U.S.C. 552a), 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.

Authority - This information is collected under the authority of the National Aeronautics and Space Act, as amended, 51 U.S.C. § 20113(a), and Executive Order 9397.

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.

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 a law enforcement or administrative inquiry or investigation shall be disclosed to NASA contractors, subcontractors, or grantees. Disclosure shall 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 shall be disclosed in the course of presenting evidence or during pretrial discovery. NASA shall disclose information to the Department of Justice or other agencies in connection with such a proceeding.

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 shall result in various undesired actions such as disqualification for employment or access

APPENDIX D: SUBSCRIBER AGREEMENT

NASA Public Key Infrastructure (PKI) Subscriber Agreement (HSPD 12 Compliant badge) (version 1.0, August 2007):

YOU MUST 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.

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:

a. 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;

b. use your badge exclusively for authorized NASA business such as to gain access to NASA facilities and/or systems; - take reasonable precautions to protect your badge from loss, disclosure, modification, or unauthorized use;

c. inform NASA within 24 hours of the loss of your badge; - 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. 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.

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**.**

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.

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.

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)

Statement:

I hereby certify that the information provided by me is true and correct to be 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.