

Attachment J-7

Personal Identity Verification (PIV) for Contractor Personnel

NASA Interim Directive (NPR-1600.1)

Date: May 24, 2007

Office of Security and Program Protection

Personal Identity Verification (PIV) Policy and Procedures

1. Purpose

This requirements document establishes an Agency-wide policy for the creation and issuance of federal credentials at NASA.

2. Scope

The policies and procedures identified within this document cover the only approved processes for NASA to issue federal credentials pursuant to Federal Information Processing Standards Publication Number 201-1 (FIPS 201), and Homeland Security Presidential Directive (HSPD) 12.

3. Applicability

This policy applies to all NASA facilities, organizational components, employees, contractors, personnel completing work through Space Act Agreements or Memorandums or Agreement/Understanding, those assigned or detailed under the Intergovernmental Personnel Act, partners and visitors, where appropriate, in achieving NASA missions, programs, projects, and institutional requirements. Contractors, as used in this Directive, are defined to include contractor organizations and employees or subcontractors, recipients of grants and cooperative agreements and employees or sub-recipients, and all other organizations or employees that are reimbursed by NASA through appropriated funds. This NID augments NPR1600.1 and will be in effect for one year or until NPR 1600.1 is revised, whichever occurs first.

4. Authority

1. 42 U.S.C. § 2473(c)(1), Section 203(c)(1) of the National Aeronautics and Space Act of 1958 as amended.

5. References

1. Homeland Security Presidential Directive 12 (HSPD-12)
2. Federal Information Processing Standards Publication 201 (FIPS-201)
3. NASA Procedural Requirement (NPR) 1600.1
4. 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"
5. Federal Acquisition Regulation Clause 52.204-9, Personal Identity Verification of Contractor Personnel
6. Executive Order 12968 of August 2, 1995
7. X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, v2.5 16 OCT 2006
8. 5 CFR Section 731.202; 5 Code of Federal Regulations Section 731.501
9. NIST Special Publication 800-79, Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations
10. Executive Order 10450 of April 17, 1953
11. Federal Information Security Management Act of 2002 (FISMA 2002) P.L. 100-235
12. Privacy Act, 5 U.S.Code section 552a.

6. Responsibilities

All NASA employees and contractor employees will be required to comply with this Directive, and the implementing Directives of their respective Centers consistent with Homeland Security Presidential Directive 12 and with the Privacy Act, 5 U.S. Code section 552a. As more fully detailed herein, all Applicants will have their information protected by applicable provisions of the Privacy Act. See also section 10 of this Directive. The Assistant Administrator, Office of Security and Program Protection (AA/OSPP), is the system owner of the Common Badging and Access Control System (CBACS) which is used to issue Personal Identity Verification (PIV) credentials, hereinafter "Badge," and has overall responsibility for ensuring uniformity of federal credential issuance policies and procedures throughout the agency.

All NASA organizational components shall adhere to the policies and procedures herein and promulgate implementing regulations (but no lower than the Center level) consistent with the policies and procedures set forth herein.

In accordance with this NID and other applicable regulations, Center Directors, through their Chiefs of Center Security (CCS), supported by the Center Human Resources Office (HRO), Procurement Office, Chief Information Office (CIO) and other offices as necessary, shall ensure that local operating procedures and execution conform to the policies and procedures herein. Center Directors shall ensure the Personal Identity Verification Card Issuance (PCI) chain of trust and card control is maintained. To support

the integration of PIV procedures, Center Directors¹ are to adhere to the principle of separation of duties as provided herein to ensure clearly that no single individual has the capability to issue a Badge without the cooperation of another authorized person. PIV Authorizers and Enrollment Officials making suitability, security and/or access determinations must be members of the Federal civil servant workforce.

6.1 PIV Oversight of Roles and Responsibilities

HSPD-12 and FIPS 201 define specific roles and responsibilities as follow:

6.1.1 Agency Official for Privacy (AOP)

As identified in FIPS 201, the AOP oversees privacy-related matters in the PIV system and works with the PIV System Owner to ensure that the rights of Applicants and PIV Subscribers are protected in accordance with applicable law and regulation. The Agency Chief Information Officer (ACIO) serves this function.

6.1.2 PIV Card Applicant Representative

The PIV Card Applicant Representative acts as a point-of-contact for Applicants in adhering to prescribed processes to properly obtain Badges. This function is performed by a Human Resources (HR) specialist for Government Employees or a Contracting Officers Technical Representative (COTR) or other federal civil service technical personnel responsible for work requirements for contractor employees.

The PIV Card Applicant Representative serves the following roles:

1. Acts as a point-of-contact for current or prospective Federal employees, contractors, or foreign nationals in providing the necessary documents, and in properly obtaining a Badge.
2. Adheres to this NID and other pertinent directives in protecting personal privacy of Applicants; also acts as a point-of-contact for an Applicant who is denied a Badge because of missing or incorrect information in an Identity Source document, or whose application is otherwise held in abeyance.
3. As authorized in this Directive, may act on behalf of (as a surrogate for) an Applicant who is not available for performing required actions.

6.2 Badge Issuance Roles and Responsibilities

The following roles and responsibilities are to be followed during the issuance and card life-cycle management process:

6.2.1 Applicant

The Applicant is the individual to whom a Badge is to be issued. Badges are issued to all individuals who require physical or logical access to designated NASA resources for a period of greater than 179 days. Applicants may be prospective and current NASA employees (i.e., civil servants), contractors, grantees (grants, academics, and cooperative

¹ For HQ NASA, this function is accomplished by the Deputy Assistant Administrator for Headquarters Operations.

program personnel) and foreign nationals. Applicants are responsible for: providing basic demographic data for the PIV request; submitting their photograph and fingerprints; presenting valid identity documents during enrollment; and proper handling and use of the Badge once issued. Until their own PIV request is approved, and a Badge properly issued, an individual Applicant cannot perform any other role during their processing for a Badge.

6.2.2 Requestor

The Requestor is the individual, designated by implementing regulations under this Directive, who creates the initial request for an Applicant to receive a Badge, and who performs initial entry of Applicant demographic data into the system as part of the PIV badge request. The Requestor role for a given Applicant may be held by a manager of a specific program, contract or grant. The Requestor is HR for prospective NASA employees, the Contractor organization for Contractors, and the Grant Provider for Grantees. Foreign Nationals must first be processed through the NASA Foreign National Management System (NFMMS) for review and approval by the center's International Visits Coordinator, or the NASA Foreign National Management System (NFMMS) Administrator as appropriate, before requesting a Badge. An individual who holds the Requestor role may also perform the role of Sponsor, but cannot perform the roles of Enrollment Official, Issuance Official, or PIV Authorizer.

6.2.3 Sponsor

The Sponsor is the designated government official who establishes and approves the request for the Applicant's physical or logical access to NASA facilities. The Sponsor is authorized to modify, approve, or disapprove the Requestor's request for issuance of a Badge. Generally, the Sponsor role is held by an HR specialist for NASA employees, a Contracting Officer's Technical Representatives (COTR) or other federal civil service technical personnel responsible for work requirements for contractor employees, or a grants technical official for grantees. An individual who holds the Sponsor role may also perform the role of Requestor, but cannot perform the roles of the Enrollment Official, Issuance Official, or PIV Authorizer.

6.2.4 Enrollment Official

The Enrollment Official collects, establishes, and verifies identity information from an Applicant. The Enrollment Official captures fingerprints and photographs, (for background investigation and placement on the credential); checks I-9 identity source documents for authenticity and scans them into the Identity Management System (IDMS) system; compares name and demographic data between the system and I-9 documents; and determines whether the any discrepancies on an Applicant I-9 during proofing are valid. This role is generally fulfilled by personnel in the Center Security Office. An individual who holds the Enrollment Official role may also perform the role of Issuance Official, but cannot perform the roles of Requestor, Sponsor or PIV Authorizer for the same PIV application.

6.2.5 PIV Authorizer

The PIV Authorizer is a NASA federal employee in the Center Security Office who records final results of adjudicated investigations, and on favorable adjudications,

authorizes production and issuance of a Badge for a given Applicant. The PIV Authorizer, either directly or through supporting staff, manages the Applicant's background investigation submission process through the Office of Personnel Management's Electronic Questionnaire for Investigation Processing (e-QIP); reviews the PIV badge request, the Sponsor's approval, and the results of the I-9 validation; checks for existing background investigation and if there is none, issues a request for a background investigation; reviews the results of the National Agency Check (NAC) if required; based on investigation results, authorizes credential issuance through the PIV workflow; and updates authorization once a NACI or higher investigation results are received. An individual who holds the PIV Authorizer role must be a government employee and can perform no other role in the PIV issuance process (when the PIV Authorizer is going through their issuance or reissuance process, they shall not serve as their own PIV Authorizer).

6.2.6 Issuance Official

The Issuance Official issues the Badge to an approved Applicant. The Issuance Official verifies the Applicant's identity with a 1:1 biometric verification to the IDMS; encodes the Badge with the appropriate identity information; ensures the Applicant has selected a Personal Identification Number (PIN); secures and accounts for Badges prior to issuance to the Applicant; and delivers the card to the Applicant, completing the PIV issuance process. This role is generally fulfilled by the Center Security Office. An individual who holds the Issuance Official role may also perform the role of Enrollment Official, but cannot perform the roles of Requestor, Sponsor or PIV Authorizer for the same PIV applicant.

The above roles must be performed by separate individuals, unless otherwise noted. Combining of these duties is not permitted.

7. Training

Each of the roles described herein are unique and have their own requirements. Training will be provided to ensure that each role functions properly. Individuals who are designated for the roles identified above require training in two areas:

1. NASA-specific processes and procedures (processes and procedures unique to NASA), and;
2. PIV-specific processes and procedures (processes and procedures unique to the PIV identity-proofing process).

NASA will provide end-user training on the card life-cycle management system to agency personnel as required. Training will be both formal and informal, consisting of on-site "desk-side coaching" sessions, instruction and web-based training modules. Both technical training and user training will be available. Day-to-day operations training will be provided to system operators and administrators to ensure that they have a thorough understanding of the systems and related components they will be responsible for managing.

8. Discussion

On August 27, 2004, the President signed Homeland Security Presidential Directive 12 (HSPD-12) entitled "Policy for a Common Identification Standard for Federal Employees and Contractors," applicable to all Executive Branch departments and agencies. HSPD-12 states that, *"secure and reliable forms of identification" for purposes of this directive means identification that:*

1. *Is issued based on sound criteria for verifying an individual employee's identity;*
2. *Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;*
3. *Can be rapidly authenticated electronically; and*
4. *Is issued only by providers whose reliability has been established by an official accreditation process."*

HSPD-12 charged the Secretary of Commerce with the promulgation of a "Federal standard for secure and reliable forms of identification." As a result the Secretary of Commerce published Federal Information Processing Standards Publication 201-1 (FIPS PUB 201-1) titled "Personal Identity Verification (PIV) of Federal Employees and Contractors." (Hereinafter, FIPS 201). HSPD-12 directed that the Department of Commerce promulgate uniform standards to satisfy stated control objectives. The HSPD-12 control objectives include, *"secure and reliable forms of identification" for purposes of this directive means identification that:*

5. *Is issued based on sound criteria for verifying an individual employee's identity;*
6. *Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;*
7. *Can be rapidly authenticated electronically; and*

Is issued only by providers whose reliability has been established by an official accreditation process."

Accordingly, the Secretary of Commerce published the required standards in Federal Information Processing Standards Publication 201-1 (FIPS PUB 201-1) titled "Personal Identity Verification (PIV) of Federal Employees and Contractors." (Hereinafter, FIPS 201).

FIPS 201 is, *"... to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identify of individuals seeking physical access to Federally controlled government facilities and electronic access to government information systems."*

As required by HSPD-12, the standards provided in FIPS 201 are applicable to identification issued by Federal departments to their employees, contractor employees, and others comprising the agency workforce (foreign national, co-operatives, partners, grantees, recipients of Space Act Agreements, visitors, et al.) Waivers to Federal Information Processing Standards are not allowed. Accordingly, FIPS 201 requires that each federal organization adopt an approved identify proofing and registration process that includes:

1. A minimum of a completed FBI National Criminal History Check (NCHC) , and either the receipt of a completed background investigation or 5 days from submission of the background investigation where no disqualifying information is returned within that 5 day period. This minimum NCHC requires that the individual submit fingerprints.
2. At the time of registration (enrollment), an individual's identity is verified. The Applicant will appear in person and present two forms of identity that are listed on the Form I-9, (OMB No 1115-0136, Employment Eligibility Verification). One document will be a valid State or Federal issued picture identification. Again at the time the credentials are issued a person's identity is verified to match that at registration, usually by biometrics, before a Badge can be issued.
3. Prevent the issuance of a Badge by a single individual without the cooperation of another authorized person.
4. That the Badge is revoked if the results of an investigation warrant.

This Interim Policy Directive provides those processes required for Badge Issuance.

9. Badge Usage

The Badge provides multiple levels of assurance when validating an individual's identity. The only authorized uses of the Badge are for establishing identity for physical and logical access. Establishing identity is a separate function from authorizing access.

1. **Physical Access:** Following proper issuance of a Badge, the Office of Security and Program Protection (OSPP) can provide Badgeholders needing access with physical access to NASA facilities through the Enterprise Physical Common Access Control System (E-PACS).
2. **Logical Access:** Following proper issuance of a Badge, the Office of the Chief Information Officer (OCIO) can provide Badgeholders needing access with logical access to NASA computer and data network systems through Badge card log-on procedures.

9.1 Badge Authentication Methods for Physical Access

The Badge will be used for visual identity authentication by an authorized individual, such as a security guard, or by electronic identity authentication, such as a card reader. The type and factor of authentication will be based on the current threat level, characteristics or profile of the facility, risk management principles, and security posture at the site, as determined by competent authority. Note that proof of identity does not necessarily mean full physical or logical access to NASA facilities, which instead must be separately determined by the CCS.

- 1 **Visual Authentication:** A security guard will perform visual screening of the Badgeholder to ascertain the identified individual should be granted access to the NASA facility. The visual authentication process includes:

- i The security guard at the access control entry point will determine whether the Badge appears to be genuine and has not been altered in any way;
 - ii The security guard will compare the Badgeholder's facial features with the photo on the badge to ensure they match;
 - iii The security guard will check the expiration date on the Badge to ensure it has not expired; and
 - iv One or more of the other data elements on the Badge, such as the name, employee affiliation, or Agency name, will be compared to the individual's appearance or responses, assisting the security official to verify the Badgeholder is whom they purport to be.
- 2. **CHUID Authentication:** A Cardholder Unique Identifier (CHUID) authentication will be used to access NASA and other Federal facilities with FIPS 201 compliant Physical Access Control System (PACS). The CHUID authentication process will include:
 - i The CHUID will be read electronically from the Badge;
 - ii When inserted into the card reader, the security guard will check the expiration date to ensure the badge has not expired;
 - iii One or more of the CHUID data elements (e.g. FASC-N) will be used as input into the electronic authorization check to verify that the Badgeholder should be granted access.
- 3. **PIN Pad Authentication:** This system may be employed for greater security needs, typically for certain limited access facilities at NASA Centers. A PIN input device can be used in tandem with badge readers when a higher level of authentication assurance is required, providing two-factor authentication. The badgeholder presents the Badge and will be required to type in the badge's PIN into the PIN input device. If PIN devices are used, PACS will ensure that each PIN is 6 digits in length.
- 4. **Biometric Authentication:** On an as-needed basis, biometric authentication may be used for two-factor authentication to support access control to physical and logical infrastructure. The Badge hosts a mandatory, signed biometric that can only be read from the badge using a PIN supplied by the badge holder.
- 5. **PIV Asymmetric Cryptography (PKI) Authentication:** The Badge carries an asymmetric authentication private key and corresponding authenticity certificate that is used by other Federal agencies to verify the Badgeholder's identity.

9.2 Badge Authentication Methods for Logical Access

- 1. **PIN Pad Authentication:** A PIN input device can be used with badge readers when a higher level of authentication assurance is required as determined by the CCS, providing two-factor authentication. The badge holder presents the Badge and will be required to type in the badge's PACS PIN into the PIN input device.

2. **Biometric Authentication:** Biometric authentication may be used for two, or three-factor authentication to support access control to physical and logical infrastructure on an as-needed basis, as determined by the CCS. The Badge hosts a mandatory, signed biometric that can only be read from the badge using a PIN supplied by the badge holder.
3. **PIV Asymmetric Cryptography (PKI) Authentication:** The Badge carries a mandatory asymmetric authentication private key and corresponding certificate that is used by other Federal agencies to verify the Badgeholder's identity.

9.3 Authenticating other Agency PIV Cards

The Badges issued by NASA will provide proof of identity to other government agencies. In like manner, other agency PIV credentials will serve as proof of identity to NASA. Note that proof of identity does not necessarily mean full physical or logical access to NASA or other Federal facilities, which instead must be separately determined by the Center Chief of Security (CCS).

10. Privacy

Privacy protection is an essential part of NASA's implementation of HSPD-12. Particular information on HSPD-12 and related privacy issues are discussed in NASA Privacy Impact Assessment (PIA) of July 20, 2006 (See Federal Register System of Record Notice (SORN) NASA 10 SECR, and PIA (http://www.nasa.gov/pdf/154145main_PDFonline.pdf)).

Any and all individuals involved in the PIV issuance process must adhere strictly to the requirements of the PIA and the Privacy Act, 5 U.S.C. sec. 552a, and other implementing regulations. In accordance with the Privacy Act, the PIA sets forth the proper uses of the systems of records concerned. Information that is not authorized to be obtained and maintained shall not be requested or maintained. Any use of unauthorized information from or within PIV systems or subsystems can be the basis for disciplinary actions, including removal, in accordance with existing regulations.

11. Process for Federal PIV Credential Issuance

The following steps reflect the procedures that NASA officials will follow to issue a Federal PIV credential:

Step 1: Badge Request

1. A Requestor requests issuance of a Badge for an Applicant by entering the Applicant's demographic data into the PIV system through the IdMAX Create Identity application. The Requestor is:
 - i HRO for prospective NASA employees; (automated process via the Workforce Transformation Tracking System [WTTS])
 - ii The Contractor organization, COTR or other federal civil service technical personnel responsible for work requirements for Contractors;

- iii The Grant Provider for Grantees; and
- iv The Center's International Visits Coordinator for foreign nationals, only after approval through the NASA Foreign National Management System (NFNMS) (automated process via NFNMS).

Step 2: Sponsorship

2. The Sponsor approves the Requestor's request, establishes the need for a relationship between the Applicant and NASA, and validates the Applicant's need for a Badge by either approving or denying the request.

Step 3: Check for Background Investigation Status

3. Upon receiving the request for a Badge with the Sponsor's approval, the PIV Authorizer and supporting staff review the Office of Personnel Management (OPM) and other federal databases and take appropriate steps to validate the Applicant's investigation status with regard to a current investigation. (If the Applicant has an investigation on file or in progress that meets the investigative and reciprocity requirements, the Applicant proceeds to enrollment steps with only flat (not rolled) fingerprints obtained).
4. The PIV Authorizer authorizes the Enrollment Official to obtain the Applicant's fingerprints, I-9 documents and biometric data.
5. If the review of the federal databases reflects that the Applicant requires further background investigation, the PIV Authorizer and supporting staff:
 - i Provide information to Applicants who do not currently possess the required level of background investigation on completing the appropriate security questionnaire form.
 - a) At a minimum, the background investigation must be a NACI. The appropriate background investigation is determined by the completion of NASA Form 1722 or NASA Form 1760 as appropriate, and will flow automatically from the WTTS into IDMS.
 - ii Initiate an invitation in the OPM Electronic Processing for Investigations Processing (e-QIP) database for the Applicant and provides the Applicant with instructions on accessing and using e-QIP.
 - iii Notify the Applicant and/or Requestor of the need to complete background investigation forms through e-QIP.
 - iv Advise the Applicant that an unsatisfactory determination based on an adverse background investigation could result in denial of access to NASA-controlled facilities and/or information systems.
6. The Sponsor advises the Applicant that they must appear in-person before the Enrollment Official and submit two forms of identity source documents in original form prior to being issued a Badge.
7. The Applicant completes the Standard Form (SF) 85-P/86 (as appropriate), OPM Questionnaire for Non-Sensitive Position found on the e-QIP website, to provide the required background information.

Step 4: Enrollment Process

8. The Applicant appears in-person before the authorized Enrollment Official and submits two forms of identity source documents in original form. The Enrollment Official inspects the source document for genuineness, and if possible, validates the source document with the authority or entity which issued it.
 - i The identity source documents must come from the list of acceptable documents included in Form I-9, Employment Eligibility Verification; one of which must be a Federal or State issued picture identification. The current NASA badge may not be used to fulfill the I-9 requirement.
9. Fingerprints and photo identification pictures are taken, and attached electronically by the Enrollment Official to the OPM questionnaire.
 - i Two of the Applicant's fingerprints are obtained in an electronic format compliant with FIPS 201, to be used on the Applicant's Badge.
10. The Enrollment Official obtains and maintains a legible photo-copy of the original I-9 documentation, or if the technical capability is available, the Enrollment Official electronically scans and submits the documents to IDMS.
 - i 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.
 - ii A photo-copy of any rejected documents are to be made and retained for a period not to exceed one (1) year, or until any appeal process is completed.
 - iii An I-9 document that does not pass electronic examination is rejected and another form of I-9 document must be obtained, and is subjected to electronic scrutiny, if available.
11. A non-PIV government identification badge, including any NASA Photo Identification Badge which has not undergone the PIV-I process, MAY NOT BE USED for the original issuance of a PIV vetted credential or to fulfill the requirement for an I-9 original source document.
12. The Enrollment Official provides Applicant with subscriber agreement [and obtains an electronic signature.
13. Upon the Applicant's presentation of required documentation, the Enrollment Official reviews the information and resolves any discrepancies or omissions with the Applicant as necessary.
 - i The information submitted by the Applicant is used to update the Applicant identity record in IDMS.
14. When the Applicant has appeared in person and completed fingerprints per Step 2 (above) and has submitted complete and correct background information, the PIV Authorizer submits a request for a background investigation to OPM with a request for reply/response on the NAC.
15. OPM records the results of the NCHC in the OPM database.

Step 5: Adjudication Process

16. At a minimum, the PIV Authorizer reviews the results of the NCHC and, if available, the advanced NAC. After 5 days of initial submission of a background investigation to OPM via e-QIP (or 10-working days for paper submission), the PIV Authorizer makes a determination if the applicant is eligible to receive a Badge.

If the Applicant is eligible, the PIV Authorizer authorizes creation and issuance of a Badge and informs the Sponsor and Requestor of the need for the Applicant to report to the Issuance Official for credential issuance and pickup.

- ii If adverse information is developed and the Applicant denied access, the PIV Authorizer notifies both the Sponsor and Requestor of the action.

Step 6: Card Production Process

- 17. The PIV Authorizer directs printing to be done either remotely or on site:
 - i If the Badge is to be printed remotely at a commercial facility or shared service provider, the necessary information is included in a batch card creation request. The initialized Badges are returned to NASA and forwarded to the appropriate Issuance Officials where it is held in a secure location.
 - ii If the Badge is to be produced locally, the Issuance Official prints the identity information onto the card; compares the photo to the identity database; loads the printed card into the card reader; encodes the card with the identity and biometric data; tests the card and logs the successful completion of the encoding process.

Step 7: Issuance Process

- 18. The Applicant appears before the Issuance Official, who establishes whether the Badge was printed with a batch, or is to be printed on-site:
 - i If printed in a batch, the Issuance Official checks the printed Badge to verify the identity of the Applicant, conducts a fingerprint match and encodes the Badge with an Applicant entered PIN number.
 - ii If printed on-site, the Issuance Official verifies the identity of the Applicant against the database, conducts a fingerprint match and encodes the Badge with an Applicant entered PIN number.
- 19. Upon completion, IDMS is updated to indicate the Badge has been issued.
- 20. At this point the Badge issuance process is complete and the badge is officially released to the Applicant.

11.1 Issuance Process for Contractors

- 1. The Contractor's Corporate Security Officer (CSO), Program Manager (PM), or Facility Security Officer (FSO) or equivalent functionary as designated by the Contractor organization, serves as the Requestor for contractors and is granted access to the Create Identity web portal, and initiates a Badge request by entering the Applicant's required information.
- 2. The Contracting Officer's Technical Representative (COTR) or other federal civil service technical personnel responsible for work requirements serves as the Sponsor, approving the Badge request from the contractors for which they are responsible.
- 3. Once these steps are complete, the contractor or foreign national begins the issuance process in Section 11 above, starting at Step 3.

11.2 Issuance Process for Grantees and Recipients

1. A grantee or recipient is granted access to a web-based version of the Create Identity program, and initiates a Badge request by entering the Applicant's required information.
2. The information is transmitted to the cognizant NASA technical officer or grants administrator, who serves as the Sponsor as well as the PIV Card Applicant Representative for grantees.
3. Once these steps are complete, the grantee or recipient begins the PIV Card issuance process in Section 11, starting at Step 3.

11.3 Issuance Process for Foreign Nationals

1. Approval through the NASA Foreign National Management System (NFMMS) must be obtained for the visit or assignment before any processing for a Badge can take place for a foreign national. The current version of NPR 1371.2 will be consulted.
2. If a foreign national is not under a contract where a COTR has been officially designated, the foreign national provides the information directly to their visit/assignment host, and the host Sponsor fulfills the duties of the Sponsor as required herein.
3. A national check of the Bureau of Immigration and Customs Enforcement (BICE) database is also performed.
4. Once these steps are complete, the contractor or foreign national begins the issuance process Section 11 above, starting at Step 1.

11.4 Obtaining Alternative Biometrics

The right and left index finger are the primary and secondary finger for obtaining biometrics. However, if these fingers cannot be imaged, the primary and secondary designations are taken from the following fingers, in decreasing order of priority as follow:

1. Right thumb,
2. Left thumb,
3. Right middle finger,
4. Left middle finger,
5. Right ring finger,
6. Left ring finger,
7. Right little finger,
8. Left little finger.

These card fingerprints are used for 1:1 biometric verification against live samples collected from the PIV Applicant. The card stores both fingerprints recorded, however, a Center may use one or both of them for the purpose of Badgeholder authentication. If only one fingerprint is used for authentication, then the primary finger will be used.

In cases where there was 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 Badgeholders covered under Section 508 of the Rehabilitation Act. The photograph must include the entire face, from natural hairline forward, to the chin, and may not be obscured by dark glasses, coverings, etc. 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 AA/OSPP who may refer the matter for a recommendation to a HQ NASA Access Appeals Panel.

Based on the mandatory topographical features on the front and back of the Badge (i.e., photograph, name, employee affiliation employment identifier, expiration date, agency card serial number, issuer identification, etc.) that support visual identification and authentication, a security official or guard will perform visual identity verification of the cardholder before permitting access to NASA-controlled facilities and/or information systems.

12. Post-Issuance Activities

After badge issuance, four post-issuance activities may occur over the course of the Badge life-cycle prior to termination. For each activity, the badge holder must coordinate with the Issuance Official, Enrollment Official, or Sponsor. The post-issuance activities require badge holders to appear in person at their respective Center – either to receive a new Badge or to have a current badge updated.

12.1 Badge Renewal

Card renewal occurs immediately before a card expires and the card is replaced without the need to repeat the full registration process. Before renewing the card, the center must verify that the cardholder still has an up-to-date background investigation and that the cardholder's security/IDMS records are accurate. Biometric data on file may be reused when issuing the new Badge, but the digital signature must be recomputed and a new certificate created.

FIPS 201 requires that PIV Cards be valid for no more than five years. Badge holders can apply for a renewal starting six weeks prior to the expiration date on their Badge. The Badgeholder coordinates with the Sponsor, who ensures the personnel records are accurate and current before the issuance of a new Badge.

The PIV Authorizer and supporting staff check to see if the background investigation is current and either approves the renewal or requests that a new background investigation be performed, as required.

In cases when the PIV Authorizer approves the card renewal, the cardholder appears before the Issuance Official, who initializes the new card and validates the cardholder's biometrics against the ones on file before releasing the new PIV smart card.

12.2 Badge Reissuance

In the event that a Badge expires before renewal, is compromised, lost, stolen or damaged – or in the event of an employee's status change – the card holder notifies his/her Sponsor and requests issuance of a replacement Badge. Contractor employees will do this through their Requestor. The Sponsor notifies Center Security of the lost, stolen, damaged or expired Badge, so that the old Badge can be revoked, and then enters a request for re-issuance of the Badge. The old Badge is then revoked, as in 12.5.

Before the Badge can be re-issued, the entire registration and issuance process (including fingerprint, facial image and I-9 documentation) must be repeated. This requires the Badge holder to appear before an Enrollment Official again to obtain and verify the biometrics.

The PIV Authorizer reviews the request, ensuring that the employee remains in good standing, that the personnel and security records (ibid.), and background investigation are current before approving the reissuance. If everything is in order, the PIV Authorizer approves reissuance.

If available by applicable contract, the replacement card may be ordered from the manufacturer as part of a batch and received by the Issuance Official in a few days. Alternatively, a blank Badge could be printed locally by the Issuance Official when the Applicant appears to receive their new card. At that time, the Issuance Official requests a new identity credential, initializes the card, verifies the identity of the Applicant, and delivers the replacement card, and retains the old card (if available).

12.3 Badge PIN Reset

In the event that a Badge is disabled or locked-out due to entry of an invalid PIN more than NASA's three entry attempts, it is the badge holder's responsibility to notify the Issuance Official to enable or unlock the badge. After the badge holder's PIN is reset, the Issuance Official must ensure the badge holder's fingerprint matches the template stored on their Badge before providing it back to the badge holder. A new badge does not need to be printed when the PIN is reset.

12.4 Separation

In the event that a Badge is revoked, due to exit on duty, change in need for access, termination of employment, an unfavorable NAC or completed background investigation, or death, the PIV Authorizer follows the following steps:

1. Sets the worker's relationship to "inactive;"
2. Inquires whether the credential has been issued;

- i If a credential has not been issued, the PIV Authorizer proceeds to step 5.
- 3. Authorizes the termination of the credential with a return required;
- 4. Provides instruction to the worker to return their credential;
- 5. Finds out whether an investigation has been initiated or submitted;
 - i If an investigation has not been initiated or submitted, proceeds to step 7.
- 6. Authorizes the cancellation of the investigation;
- 7. Inquires whether or not the worker passed away;
 - i In the case of an Applicant's death, the PIV Authorizer terminates the credential with a return of the credential requested, and proceeds to step 8.
- 8. Notifies the Sponsor of all the previous steps taken.

12.5 Badge Termination

The termination process is used to permanently destroy or invalidate the Badge and the data and keys needed for PIV authentication so as to prevent any further use of the card for PIV authentication.

The Badge must be turned into the Issuance Official before permanent departure from NASA. Once received, the Issuance Official:

- 1. Inspects the credential for authenticity.
- 2. Verify credential life-cycle status as active.
- 3. Sets credential lifecycle status to "terminated," and sets reason for termination
- 4. Revoke certificates.
- 5. Documents the reason for destruction.
- 6. Renders the credential unusable and confirms its physical destruction by authorized means.
- 7. Sets the credential life-cycle status to "destroyed."

12.6 Visitor and Temporary Badging

Visitor and temporary badging is outside the scope of this document and is determined by each Center's security office, consistent with pertinent directives. Usually, a set of temporary visitor badges are held by the Badging Office and issued on an as-needed basis to authorized, temporary, and short-term visitors for appropriate access to NASA facilities. Short-term visitors will not receive access to protected logical data systems and resources. Individuals who require extensive physical or logical access, but for a period less than 6 months will be handled on a case-by-case basis in consultation with the Center Chief of Security. Access by visitor and temporary badges will be for bona fide purposes, and not used to circumvent the requirements of this Interim Directive.

Suitability, Adjudication, Investigation and Appeals

13.1 Unsatisfactory Suitability Results

13.1.1 NASA Employees

If the Badge issuance process yields any derogatory or unfavorable information, the CCS immediately advises the applicant of the information. The applicant has 10-working days to provide information that he/she feels will mitigate the information to the CCS. Upon receipt of the information, the CCS will adhere to NPR 1600.1 section 3.10. If 10-working days expires and the CCS does not receive input from the applicant, the CCS will forward any derogatory information to HRO to aid in their initial employment suitability determination. In compliance with 5 C.F.R. section 731, HRO solely determines employment suitability.

In addition, the PIV Authorizer and supporting staff will determine suitability for access. If a satisfactory determination is made for both employment suitability and access, the PIV Authorizer will continue the credentialing process. If an unsatisfactory suitability determination is rendered, further steps will depend upon the Applicant's employment status. HRO has cognizance over these actions, and for such applicants, the PIV processing suspends or terminates.

If the Applicant has not yet entered on duty, HR notifies the Applicant and the selection official of the decision. All PIV processing activities will terminate. If the Applicant has already entered on duty, appropriate steps begin for determination of continued employment or separation.

13.1.2 Non-NASA Employees

If this process yields unfavorable information requiring that access be denied, the CCS will immediately notify the sponsor of the denial of access, per NPR 1600.1. This NPR should be consulted in full, but requires that the employer not be informed of the basis for the determination. The Sponsor will advise the contractor only that the employee is being denied physical and/or logical access to NASA-controlled facilities and/or information systems.

The substantive criteria set forth at 5 C.F.R. 731.202 will be used to determine physical and/or logical access for all Applicants to any and all NASA Centers/component facilities.

13.2 Investigation Status

Individuals may be issued Badges prior to receipt of the complete NACI report, based on an initial adjudication using the results of the FBI fingerprint and name checks (NAC). A final adjudication is made upon receipt of the complete NACI package. An individual's "NACI status," whether their Badge is authorized based on the initial NAC or completed NACI, can be determined by examining their record in the IDMS database.

13.3 Unfavorable Advanced NAC or Background Investigation

Although an Applicant may be initially determined as eligible based on a successful fingerprint check, the Applicant's continued access is subject to a favorable adjudication following an advance NAC and background investigation. If the advance NAC or background investigation is unfavorably adjudicated, the PIV Authorizer immediately cancels and retrieves the Applicant's Badge and contacts the Sponsor for any further action, including for continued access.

13.4 Applicants with any prior Criminal Record. Applicants with any prior criminal records (except minor traffic), will be considered in accordance with 5 C.F.R. 731.202 and the following criteria.

1. If an Applicant is still under probation/parole for a state or Federal felony conviction, this alone serves as an immediate disqualifying factor for physical/logical access for any period of time. A felony is defined for these purposes as an offense that could have been punished by imprisonment for more than one year (regardless of the sentence actually imposed).
2. Additionally, the PIV Authorizer will suspend further processing if the Applicant is currently incarcerated, awaiting a hearing or trial for any offense (except minor traffic); has been convicted of a crime punishable by imprisonment of six (6) months or longer; or is awaiting or serving a form of pre-prosecution probation, suspended or deferred sentencing, probation, or parole in conjunction with an arrest or criminal charges against the individual for a crime that is punishable by imprisonment of six (6) months or longer. The PIV Authorizer will notify the Sponsor that processing has been suspended.
 - i At such a time as the hearing, trial, criminal prosecution, suspended sentencing, deferred sentencing, probation, or parole has been completed, the Applicant may be resubmitted to the identity verification process to determine eligibility for a NASA credential.
 - ii If, notwithstanding the foregoing considerations, the CCS determines that access may be justified based on compelling mitigating factors, the investigative records and a memorandum signed by the CCS containing a full justification for favorable consideration will be forwarded to the AA/OSPP. Physical or logical access may not be granted until approval is acted upon by the AA/OSPP
3. The AA/OSPP in consultation with the HQ OGC, makes the final determination and forwards the results to the CCS.

13.4 Appeals Process

13.4.1 Federal Civil Service Employees

Certain Federal employees who are denied a Federal Credential may be able to appeal the decision following procedures set forth in 5 CFR section 731.501. This appeal avenue is

not addressed by this Directive and should be consulted directly. Appeals processes set forth below are in addition to, and do not otherwise affect any available appeal procedures including those of 5 C.F.R. 731.501.

3.4.2 Badge Applicants who are Denied a Badge.

General. For all Badge applicants, if derogatory information is identified (consistent with national standards as at 5 CFR 731.202 and section 13.4 above) during any phase of the background investigation process (to include falsified information on the investigative forms/submission), National Criminal History Check (fingerprint check), National Criminal Information Center (NCIC) check, or upon completion of the investigation) requiring resolution, the applicant is advised directly. The applicant is requested to provide any information that the applicant deems pertinent or responsive to the derogatory information. If derogatory information is resolved favorably, processing for PIV continues.

If derogatory information is not resolved favorably, the applicant is afforded the opportunity to be interviewed in person to provide information to clarify or explain the derogatory information. If, upon further inquiry, the derogatory information is favorably resolved, processing for PIV continues.

Unresolved or unfavorable derogatory information and all appropriate mitigating information, including results from interviews shall again be reviewed. If upon the conclusion of the review the decision to deny issuance of a Badge is made, the CCS will send an official letter to the applicant and their sponsor advising them of the unfavorable determination and appeals procedures set forth below. Consistent with the Privacy Act, upon any denial of access, the Contractor organization shall be informed by letter that the individual has been denied access. Unless specifically authorized by the Applicant in writing, the Contractor organization will not be provided with the reason for this determination. As discussed above, contractor employees who are denied access will not have the reason for that determination revealed to their employer.

Appeal. The applicant, either personally or through the PIV Sponsor, may appeal to the CCS, seeking review of the decision only as follows.

a. Within 10 working days of being notified of the denial of clearance, the individual must submit a written request for review of the denial of requested physical or logical access, and include any and all written materials as he desires be considered on that review. An additional 5 working days for an individual's submission shall be granted on written request, but only if the individual has made the initial request within the first 10 working days following notification of the denial of access. If the individual supplies new information, the CCS may augment any written submission on the individual, in accordance with steps above.

b. Upon submission of the individual's written materials, the Center Director shall convene a three (3) person Access Appeals Panel to review the CCS determination. For

HQ NASA, this convening function is held by the Deputy Assistant Administrator for the Headquarter Operations. The Access Appeals Panel shall consist only of Federal employees. It shall include (1) an attorney from the Center Counsel/Office of General Counsel; (2) a disinterested employee from the Center management, and (3) an employee from the Center Office of Security. For HQ NASA, the members will be from analogous offices.

c. The Access Appeals Panel will assess the CCS denial determination in terms of compliance with access standards as promulgated by 5 CFR 731.202 NPR 1600.1, and section 13.4 above. The Panel will submit a written statement briefly setting forth their conclusions and decision. The Panel may (1) uphold the denial of access, (2) reverse the denial of access, or (3) return the matter for additional and specified processing. Returning a matter without specific guidance is discouraged. A minority report may be submitted, and should be succinct as to reasons for disagreement with the majority. The Access Appeals Panel shall accomplish its review within 5 working days of the individual making a written submission. The Center Director may extend the appeal period an additional 5 working days if circumstances warrant.

d. The decision of the Panel is final, and further review of the Access Appeals Panel decision is not provided for. The NASA Administrator, however, reserves the right and authority to direct that any grant or denial of access decision (including subsequent appeal) be held in abeyance pending additional discretionary review by HQ. This reservation of authority by the Administrator does not convey any substantive right to affected individuals.

If the applicant declines to appeal, either through communicating in writing or time for the appeal has expired, the original unfavorable determination will be final and annotated in OPM investigative databases. During this process the individual is not granted access until the case has been resolved.

14. Certification & Accreditation

In accordance with NIST Special Publication 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*, NASA will follow the appropriate certification and accreditation procedures.

Recertification will take place at a minimum, every three years or whenever a PIV policy or process changes.

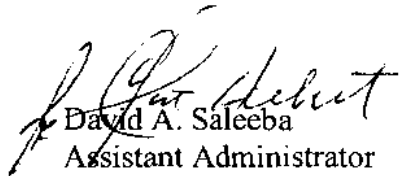
Accreditation is conducted in a manner that ensures:

- i Continued reliability of the PIV Card Issuer (PCI) and its offered services;
- ii Ongoing monitoring of the management and quality assurance controls;
- iii Re-accreditation occurs periodically in accordance with agency policy and whenever a significant change is made to the system or its operational environment

Centers will be reviewed to ensure their compliance with the certified NASA policies and procedures and may be included in future recertification.

Point of Contact

The Deputy Assistant Administrator for the Office of Security and Program Protection is the OSPP point of contact concerning this PCI policy. The DAA/OSPP can be reached at 202-358-2010.

A handwritten signature in black ink, appearing to read "David A. Saleeba", is written over the printed name.

David A. Saleeba
Assistant Administrator
Office of Security and Program Protection