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 (NFSMS) 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;
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 forwarded to the AAIOSPP.
      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 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:

- Continued reliability of the PIV Card Issuer (PCI) and its offered services;
- Ongoing monitoring of the management and quality assurance controls;
- 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.

David A. Saleeba  
Assistant Administrator  
Office of Security and Program Protection
EXHIBIT F
1. H-37, SECURITY, paragraph (a)(2)(v)(A) is revised as follows:

"(v) Chapter 6 is incorporated into the contract with the following understandings:

(A) Through Contract Modification 32, the Parties incorporated FAR Clause 52.204-9, "Personal Identity Verification (PIV) of Contractor Personnel." Through contract Modification 39, the Government incorporated the Personal Identity Verification Issuance Procedures referenced in Procurement Procedures PIC 06-01. Notwithstanding Modification 39, the Parties further hereby agree: