

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

NASA Procedural Requirements

COMPLIANCE IS MANDATORY**NPR 1600.4A**

Effective Date: April 08, 2016

Expiration Date: April 08,
2021[Printable Format \(PDF\)](#)

Request Notification of Change (NASA Only)

Subject: Identity and Credential Management**Responsible Office: Office of Protective Services**[| TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) | [Chapter5](#) | [Chapter6](#) | [AppendixA](#)
| [AppendixB](#) | [AppendixC](#) | [AppendixD](#) | [AppendixE](#) | [ALL](#) |

Chapter 6. PIV Credential Management Lifecycle

6.1 PIV Credential Inventory

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

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

6.1.3 Misuse. Forging, falsifying, or allowing misuse of a PIV credential or other forms of NASA identification in order to gain unauthorized access to NASA physical and logical resources is punishable under 18 U.S.C. 799 by fine or imprisonment for not more than one year, or both, and may further result in termination of employment and access to NASA resources.

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

6.1.5 Stock protection. Unprinted or unfinalized PIV credentials shall be shipped directly to a Center by the PIV credential manufacturer. The PIV credential issuing facility manager or other appropriate authority will designate a point of contact that is responsible for receipt of, signing for, and inventory and storage of PIV credential stock. PIV credential stock will be accessible only by authorized personnel and maintained in a secure manner, pursuant to Section 6.2, PIV Credential Storage and Handling. PIV credential stock will be monitored through the use of a log which includes, at a minimum, the date of check in, the date of check out, and the name of the person(s) performing the PIV credential stock check-ins or check-outs.

6.2 PIV Credential Storage and Handling

6.2.1 Credentials shall be stored using the following minimum requirements:

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

6.2.2 Credentials which are lost, stolen, or unaccounted for while in storage shall be reported immediately or within 24 hours to the PIV credential issuing facility manager after discovery. PIV credential details, including PIV credential identification numbers and status, will be reported to the NEACC within 24 hours of discovery in order to update the card management system. The PIV credential issuing facility manager will forward a report outlining all

pertinent facts to the OPS Security Management Division Director no later than two days after receiving reports of the lost, stolen, or unaccounted for credentials.

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

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

6.2.4.1 PIV credential encoding failures include:

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

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

6.3 Final Adjudication and Subsequent Investigation

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

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

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

6.4 Credential Usage: Display, Protection, and Proper Usage

6.4.1 NASA shall provide an electromagnetically opaque badge holder selected from an approved products list to physically protect the badge and electronically protect the information contained in the badge. Other holders found on the approved products list may be purchased by a Center at their discretion. Such holders are the responsibility of the purchasing Center to ensure that they are electromagnetically opaque. The badge will be properly displayed and worn at all times while the bearer is on a NASA Center or component facility. They will be worn above the waist on the outermost garment with the photograph visible. The use of a permanent-type symbol or the affixing of any device (e.g., tenure pin, decals, etc.) on a PIV credential (or any alteration or modification thereof) is not allowed.

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

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

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

6.4.5 A CCS/CCPS may authorize issuance of alternate Agency credentials for the following purposes:

- a. To provide access for relatives, guardians, or next of kin to wellness facilities (child care, healthcare, etc.).
- b. To provide visual verification in the absence of electronic verification for PIV credentials issued by another

Federal agency and department.

c. To recognize retirees and other individuals previously affiliated with NASA (such as ex-astronauts) who no longer require access for official NASA business.

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

a. Authorized uses of the PIV credential.

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

6.5 PIV Credential Renewal

6.5.1 Credential renewal shall occur prior to PIV credential expiration and facilitate replacement of the PIV credential without the need to repeat the full enrollment and reissuance procedures described in Section 3.5. PIV credential holders may apply for a renewal starting six weeks prior to the expiration date on their PIV credential. The PIV credential holder will coordinate with the sponsor, who ensures personnel records are accurate and current before the issuance of a new PIV credential. New biometrics are collected as described in Section 3.5.4. The old and/or expired PIV credential is to be collected and destroyed at the time of renewal pursuant to Section 6.14, PIV Credential Destruction. If warranted, the authorizer will approve the renewal and coordinate the request for a new background investigation to be performed. If a renewal is in process and is not completed before the enrollment is completed, then the credential must be re-issued as described in Section 6.6.

6.6 PIV Credential Re-issuance

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

a. Has reached its expiration date.

b. Has been compromised.

c. Is lost, stolen, or damaged.

d. Requires a change in printed information (name change, citizenship change, etc.) or card holder's status.

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

6.6.3 PIV credential holders who have officially changed their name shall submit a request for a reissuance of their PIV credential. The PIV credential holder will be required to reenroll and provide approved identity source documentation that reflects the legal 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 will occur prior to the PIV credential being returned to the applicant. PIN reset does not require the reissuance of a PIV credential.

6.8 PIV Credential Revocation

6.8.1 Credentials shall be revoked under the following conditions:

a. Exit on duty.

b. Change in need for access.

- c. Termination of employment.
- d. Unfavorable fingerprint check or background investigation determinations.
- e. Death of the PIV credential holder.

6.8.2 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.
- c. Notification shall be provided to the sponsor of the PIV credential revocation.

6.9 Lost and Stolen Credentials

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

6.9.2 It is the responsibility of NASA Centers to establish policy for the handling of multiple lost and stolen credentials. Centers may adopt one of the below methods for managing PIV credential holders who report their PIV credential as lost or stolen on multiple occasions. The following list is not comprehensive, and additional methods may be chosen by the Center:

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

6.10 Forgotten Credentials

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

- a. Require the PIV credential holder to retrieve the PIV credential.
- b. Allow issuance of a visitor badge to the PIV credential holder with verification of identity through approved identity source documents such as a driver's license.
- 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" and temporarily disabled when the

PIV credential has been misplaced and the PIV credential holder knows the current location of the PIV credential but cannot retrieve it at this time. Lost or stolen credentials will be handled pursuant to Section 6.9, Lost and Stolen Credentials. The PIV credential holder will appear at the badging office, no later than 18 hours after discovery of the misplacement, and file a report stating the PIV credential has been misplaced and provide the location of the PIV credential that was last known. Until the PIV credential is recovered or declared lost or stolen, the PIV credential holder will obtain a visitor or alternate Agency credential. PIV credential holders will report to the badging office within five business days of the original report to update the PIV credential status as being recovered, lost, or stolen. Lost and stolen credentials will adhere to Section 6.9, Lost and Stolen Credentials. Credentials that are found will be set to "active" upon report of the PIV credential being found and visual confirmation of the PIV credential. Any alternate Agency credential or visitor badge that was issued will be returned.

6.12 PIV Credential Return

6.12.1 Credentials shall be returned to NASA once an individual's affiliation with NASA has ended. Credentials

should be returned to the issuing authority no later than the last day of association with NASA. The issuing authority will be responsible for recording receipt of the PIV credentials that are returned and properly storing the PIV credentials until destruction. Credentials are not allowed to be kept as souvenirs. The responsibility of PIV credential return oversight will be:

- a. HR for NASA civil servant.
- b. Contract program manager for contractors.
- c. Grant technical official for grantees.
- 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 will have their status set to "terminated," and a reason will be supplied for the termination. Deactivation of a PIV credential and associated identity will be completed within 18 hours of notification of the need for PIV credential termination. Terminated credentials will be destroyed following the requirements in Section 6.14, PIV Credential Destruction.

6.14 PIV Credential Destruction

6.14.1 Credentials meeting the following criteria shall be destroyed:

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

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

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) | [Chapter5](#) | [Chapter6](#) |
[AppendixA](#) | [AppendixB](#) | [AppendixC](#) | [AppendixD](#) | [AppendixE](#) | [ALL](#) |

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

DISTRIBUTION: **NODIS**

This Document Is Uncontrolled When Printed.

Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>
