



NASA Procedural Requirements

NPR 1600.4Effective Date: August 01,
2012Expiration Date: August 01,
2017**COMPLIANCE IS MANDATORY**[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](#) | [ALL](#) |

Chapter 1. Introduction

1.1 Overview

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

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

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

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

1.2 Scope

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

2841.1.

1.2.2 The terms "PIV credential" and "non-PIV credential" are used frequently in this document. The term "PIV credential" refers to the credential which is issued to civil service and contractor employees who need physical or logical access to NASA facility and IT systems for 180 days or more. NASA's procedures for issuing PIV credentials must conform to HSPD-12. All other credentials issued by NASA are referred to as "Non-PIV" credentials. Non-PIV credentials include such things as: visitor badges, Center-specific badges, RSA tokens, etc.

1.3 Waivers and Exceptions

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

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

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

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

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

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

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

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