FedRAMP Digital Identity Requirements

Version **1.1**

February 21, 2018

FedRAMP

DOCUMENT REVISION HISTORY

DATE	VERSION	PAGE(S)	DESCRIPTION	AUTHOR
1/31/2018	1.0	All	Initial document	FedRAMP PMO
2/21/2018	1.1	3	Updated links in Appendix A, which changed as a result of migration of the FedRAMP web site.	FedRAMP PMO

ABOUT THIS DOCUMENT

This document provides revised guidance and requirements on digital identity capabilities in support of achieving and maintaining a Federal Risk and Authorization Management Program (FedRAMP) security authorization. FedRAMP-authorized systems must be fully compliant **by July 1, 2018**.

This document is not a FedRAMP template – there is nothing to fill out in this document.

This document uses the term *authorizing official* (AO). For systems with a Joint Authorization Board (JAB) provisional authorization to operate (P-ATO), AO refers primarily to the JAB unless this document explicitly says Agency AO. For systems with a FedRAMP Agency authorization to operate (ATO), AO refers to each leveraging Agency's AO.

WHO SHOULD USE THIS DOCUMENT?

This document is intended to be used by Cloud Service Providers (CSPs), Third Party Assessor Organizations (3PAOs), government contractors working on FedRAMP projects, and government employees working on FedRAMP authorizations.

HOW TO CONTACT US

Questions about FedRAMP or this document should be directed to info@fedramp.gov.

For more information about FedRAMP, visit the website at http://www.fedramp.gov.

TABLE OF CONTENTS

LIST OF TABLES

1. PURPOSE

On June 22, 2017, the National Institute of Standards and Technology (NIST) published Revision 3 of Special Publication (SP) 800-63, *Digital Identity Guidelines* (formerly titled *Electronic Authentication Guidelines*). The differences in the new revision that most impact FedRAMP authorizations include emphasis on federation, new password guidance, and options for easing restrictions on in-person identity validation for even High assurance authorizations.

This document establishes revised guidance and requirements on digital identity capabilities, which CSPs must implement **by July 1, 2018** for FedRAMP-authorized systems.

2. BACKGROUND

Since NIST last revised these guidelines, security measures and threats have evolved. Further, the marketplace and business model for providing identity management has changed. Revision 3 focuses on how identity management can be comprised of multiple independent capabilities, each of which relies on diverse digital identity measures across identification, authentication, and possibly federation. Thus, NIST decided to depart from the static one-volume structure and instead to release Revision 3 as a flexible four-volume format that allows entities to componentize their security in a way that reflects their own business structure.

NIST's requirements for digital identification, authentication, and federation are critical to FedRAMP authorizations; therefore, CSP compliance will be enforced by FedRAMP.

3. DIGITAL IDENTITY REQUIREMENTS

The FedRAMP Program Management Office (PMO) is adopting a static alignment between Federal Information Processing Standards (FIPS) 199 system categorization levels and the new NIST 800-63 assurance levels, as depicted in Table 1 below.

Table 1. Mapping FedRAMP Levels to NIST SP 800-63 R3 Assurance Levels

FEDRAMP SYSTEM CATEGORIZATION	IDENTITY ASSURANCE LEVEL (IAL)	AUTHENTICATOR ASSURANCE LEVEL (AAL)	FEDERATION ASSURANCE LEVEL (FAL)
High	IAL3: In-person, or supervised remote identity proofing	AAL3: Multi-factor required based on hardware-based cryptographic authenticator and approved cryptographic techniques	FAL3: The subscriber (user) must provide proof of possession of a cryptographic key, which is referenced by the assertion. The assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it
Moderate	IAL2: In-person or remote, potentially involving a "trusted referee"	AAL2: Multi-factor required, using approved cryptographic techniques	FAL2: Assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it
Low	IAL1: Self-asserted	AAL1: Single-factor or multi-factor	FAL1: Assertion is digitally signed by the identity provider
FedRAMP Tailored LI-SaaS	IAL1: Self-asserted	AAL1: Single-factor or multi-factor	FAL1: Assertion is digitally signed by the identity provider

FedRAMP continues to interpret "approved cryptographic techniques" as FIPS 140-2 Validated cryptographic modules, which aligns with prior FedRAMP guidance.

CSPs must review SP 800-63-3, use its decision trees to obtain an overview of all digital identity requirements, and read the applicable 800-63 volumes to determine specific requirements that apply to their cloud offerings. The FedRAMP PMO is requiring or recommending the following in alignment with the 800-63, Revision 3 changes for all FedRAMP-authorized systems:

1. Systems with a federated identity management solution must comply with *NIST SP 800-63C, Digital Identity Guidelines: Federation and Assertions*. This does not apply to systems with no federated identity management.
2. Agencies and CSPs may adopt the supervised remote identity proofing requirements up to FedRAMP High (IAL level 3), as described in *NIST 800-63A, Digital Identity Guidelines: Enrollment & Identity Proofing*. This change can reduce travel time and money spent in order to authorize individuals for work on Moderate and High sensitivity systems.
3. Agencies and CSPs may adopt the "trusted referee" requirements to operate on a person's behalf to provide identity proofing at the Moderate level – IAL2, as described in *NIST 800-63A, Digital Identity Guidelines: Enrollment & Identity Proofing*. Like supervised remote identity proofing, this is added to ease burdens on agencies and CSPs.
4. Agencies and CSPs are permitted and encouraged to lower password requirements as allowed by *NIST 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management*. This sets lower complexity requirements for memorized secrets so that CSPs have more flexibility in enforcement; however, this does not prevent agencies and CSPs from imposing further limitations, if desired.

   NOTE: At the time of this document's publication, FedRAMP Moderate and High controls IA-5 (g) and IA-5 (1) (a,d) are known to be more restrictive than the new password requirements in 800-63B, AAL2 and AAL3 respectively. FedRAMP recommends Agency AOs accept compliance with NIST's guidance that is most up-to-date and consistent with current cyber security threats. This may be done using an implementation status of "Alternative Implementation."

4. TRANSITION PLAN

The requirements described in this document are effective immediately, and each FedRAMP system must be fully compliant with NIST SP 800-63-3 **by July 1, 2018**. This FedRAMP compliance deadline matches the NIST enforcement requirement date of one year after publication release and maintains FedRAMP compliance with the Federal Information Security Management Act (FISMA) requirements.

By March 31, 2018, each CSP must provide written notification to their AO identifying when their cloud service offering will be fully compliant with NIST SP 800-63-3 requirements.

If the CSP anticipates being unable to meet the July 1, 2018 deadline, the written communication must also include a justification and a plan of action detailing how and when the CSP will fully comply with NIST SP 800-63-3 requirements. Where full implementation is not possible, the CSP must work with their AO on a mitigation plan. The AO must review and approve the CSP's implementation or mitigation plan.

For systems with a JAB P-ATO, the CSP should post the plan to OMB MAX and send an email notification to info@fedramp.gov, or discuss an alternative arrangement with their FedRAMP POC. For systems with an Agency AO, please coordinate with the AO's office for an appropriate delivery mechanism.

For systems with a JAB P-ATO, FedRAMP will track the SP 800-63-3 compliance transition status as part of monthly continuous monitoring activities and include this status in the monthly ConMon Report. For systems with a FedRAMP Agency ATO, the CSP must consult with their Agency AOs regarding implementation status tracking. Agency AOs will likely require the CSP to track implementation via an entry to the system's Plan of Actions and Milestones (POA&M).

Compliance with SP 800-63-3 will be a FedRAMP requirement moving forward; therefore, any CSP not yet authorized should plan to address these requirements as part of their authorization activities.

APPENDIX A: FedRAMP ACRONYMS

The *FedRAMP Master Acronyms & Glossary* contains definitions for all FedRAMP publications, and is available on the FedRAMP website Documents page under Program Overview Documents.

(https://www.fedramp.gov/documents/)

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.