Standard PR.AC: Digital Identity

February 9, 2021

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to
OCIO_IAS@ed.gov

APPROVAL

Steven Hernandez Digitally signed by Steven Hernandez Date: 2021.02.09 17:24:11 -05'00'

_____ _____

Steven Hernandez **Date**

Director, IAS/Chief Information Security Officer (CISO)

Revision History

The table below identifies all changes that have been incorporated into this document.

Version	Draft Date	Summary of Changes
1.0	8/9/2019	Initial draft
1.1	12/9/2019	Underwent annual policy review for accuracy and timeliness and to incorporate updates to NIST SP 800-53 Rev. 4. No updates were required as of December 2019.
1.2	2/9/2021	Underwent annual policy review for accuracy and timeliness, updated risk acceptance/policy exceptions section, updated standard to align with updated CSAM fields.

Table of Contents

1 INTRODUCTION 1

1.1 Purpose 1

1.2 Applicability 1

1.3 System Stakeholders 1

1.4 Compliance Approach 2

2 IDENTITY ASSURANCE 2

3 AUTHENTICATOR ASSURANCE 3

4 FEDERATION ASSURANCE 3

5 ONGOING COMPLIANCE ASSESSMENTS 3

6 RISK ACCEPTANCE/POLICY EXCEPTIONS 3

7 APPENDIX A: Identity Assurance Level Decision Chart 4

8 APPENDIX B: Authenticator Assurance Level Decision Chart 5

9 APPENDIX C: Federated Assurance Level Decision Chart 6

10 APPENDIX D: Resources and References 7

1 INTRODUCTION

This document establishes the Department of Education (ED) standard for all systems and applications that are required to implement digital identity services. Specifically, this standard defines and establishes technical requirements in the areas of user identity proofing, registration, management processes, authentication protocols, federation, and related assertions as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, *Digital Identity Guidelines*.

1.1 Purpose

The goal of establishing this Standard is to ensure that all ED systems have in place at a minimum:

- Processes and tools for effective and continuous assessment of assurance levels for each system/application role
- Robust, effective, secure and well-documented user onboarding and offboarding processes, including identity proofing and validation for all system users and support personnel
- Processes for the implementation of all necessary controls and solution(s), providing authenticator lifecycle services (such as issuance, validation and verification, renewal, reissuance and others) including a process for mapping the appropriate authenticator type for each system/application role.
- Processes for implementing Federated Identity Authentication and Authorization services, to allow systems and applications to leverage existing Credential Service Provider offerings from within the Department, from other Government entities, or from trusted third-party commercial federation services; or provide such services to others.

1.2 Applicability

The policies established in this document apply to all systems operated or maintained by ED or on behalf of ED; internal users (employees, contractors, business partners); and external users authorized to access ED systems or information. Further, this Standard applies to all *transactions* for which digital identity/identity proofing or authentication are required, regardless of the constituency. Transactions not covered by this guidance include those associated with national security systems as defined in 44 U.S.C. § 3542(b)(2).

1.3 System Stakeholders

For the purposes of this document, the term “System Stakeholder” refers to any individual with a responsibility relevant to ensuring that an ED System or Application successfully implements its required digital identity services in compliance with all Department

policies. Examples of System Stakeholders include but are not limited to Information System Owners (ISO) and Information System Security Officers (ISSO).

1.4 Compliance Approach

NOTE: While the full digital identity implementation process lifecycle consists of five phases and sub-processes, shown below for context, the scope of this Standard is limited to the **Preparation (I)** and **Assessment (II)** phases. For lifecycle Phases III through V, System Stakeholders should follow established ED solution implementation processes.

I. Preparation
1. Define each System/Application
2. Conduct a Risk Profile Assessment for each System/Application

II. Assessment
1. Conduct an Identity Assurance Level (IAL) assessment for each role and enter system values into the CSAM Digital Identity screen

III. Solution Analysis and Selection
1. Conduct a market analysis
2. Conduct an Analysis of Alternatives
3. Select a solution
4. Conduct an Enterprise Solution review and approval

IV. Implementation
1. Procure a solution
2. Deploy a solution

V. Ongoing Compliance Assessment
1. Conduct an annual re-evaluation
2. Conduct a compliance reassessment
3. Update values in CSAM Digital Identify screen, as required

2 IDENTITY ASSURANCE

Within an identity-proofing scenario, there are three different Identity Assurance Levels (IAL) used to assess false identity risks (IAL1, IAL2, IAL3). In parallel with each user role being defined in the System Security Plan (SSP), each user role must be evaluated and assigned an applicable IAL ranking (as defined in NIST SP 800-63A). Using the highwater mark, values must be entered in the CSAM Digital Identity screen.

NOTE: *The decision chart in* ***Appendix A*** *can be used in determining an IAL for each identity or operational role defined within a System/Application.*

3 AUTHENTICATOR ASSURANCE

The strength of an authentication transaction is ranked by Authenticator Assurance Level (AAL), as defined by NIST SP 800-63B. Each defined user role must be evaluated and assigned an appropriate Authenticator Assurance Level (AAL1, AAL2, AAL3). Using the high watermark, values must be entered into the CSAM Digital Identity screen.

NOTE: *The decision chart in* ***Appendix B*** *can be used in determining an AAL for each identity or operational role defined within a System/Application. Agencies and Cloud Service Providers are permitted and encouraged to lower password requirements as allowed by NIST 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management.*

4 FEDERATION ASSURANCE

Federation allows users to establish a digital identity with an identity provider and to use that identity with multiple relying parties unrelated to the identity provider. Each system role must be evaluated and assigned an appropriate Federation Assurance Level (FAL1, FAL2, FAL3) per NIST SP 800-63C. Using the high watermark, values must be entered into the CSAM Digital Identity screen.

NOTE: *The decision chart in* ***Appendix C*** *can be used in determining an FAL for each identity or operational role defined within a System/Application.*

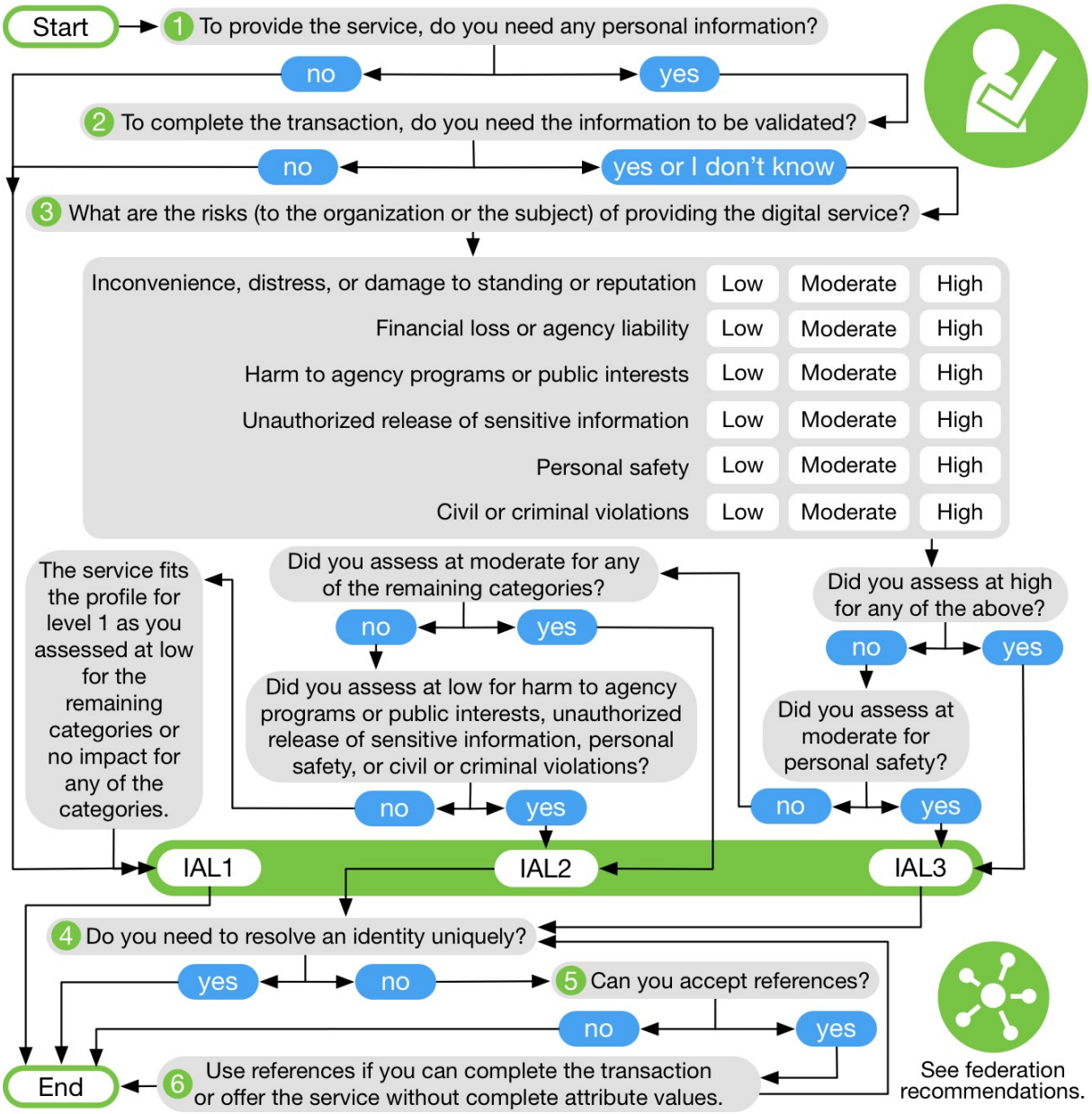
5 ONGOING COMPLIANCE ASSESSMENTS

Stakeholders must re-evaluate assurance level assessments annually in accordance with NIST SP 800-63-3, update the "Digital Identity" screen in CSAM and upload supporting artifact(s). Changes in system/application design, related to user roles, entitlements, or risk profiles must trigger a full Assurance Level re-evaluation process as defined in this document.

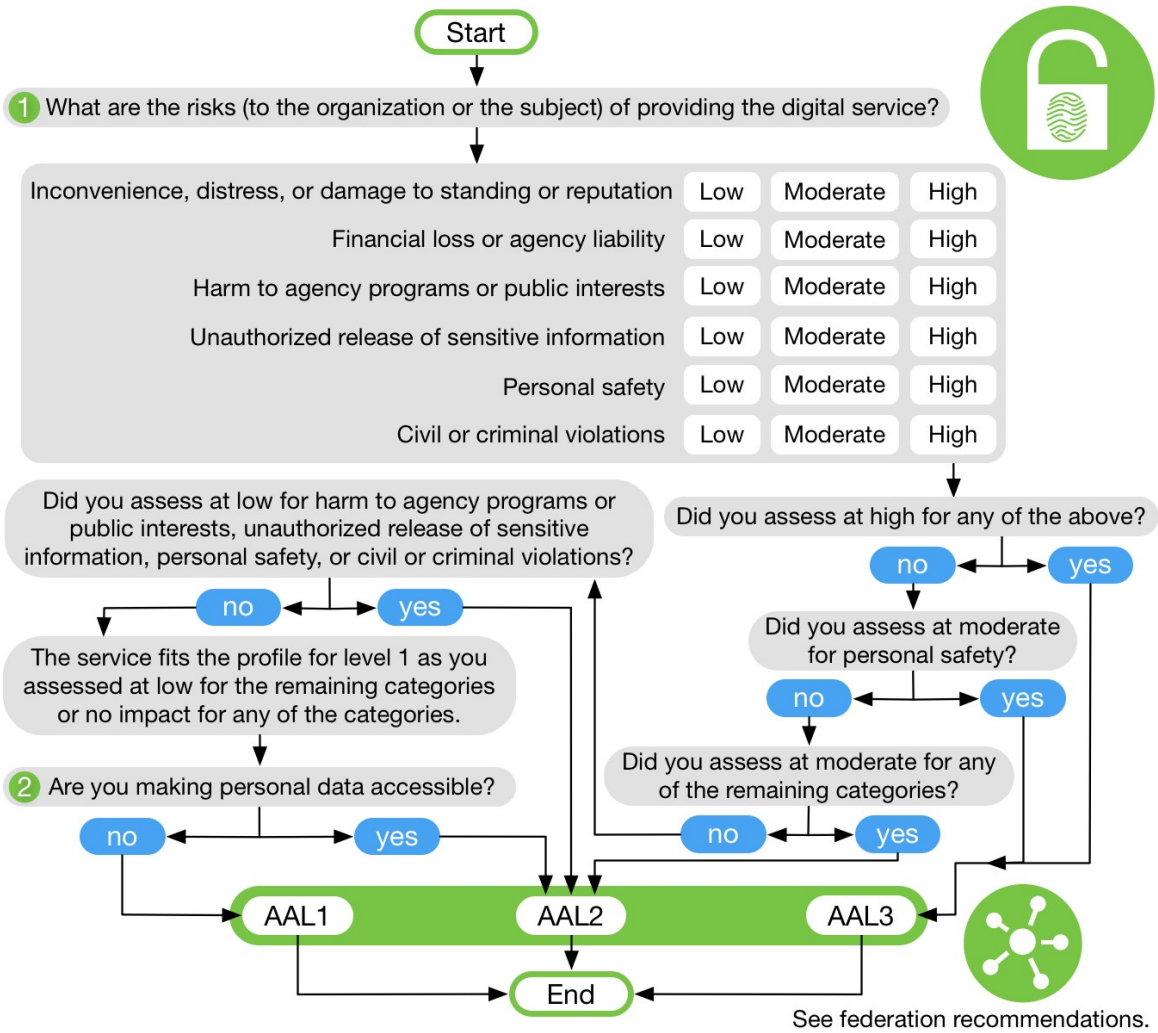
6 RISK ACCEPTANCE/POLICY EXCEPTIONS

Deviations from the Department policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department's Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).

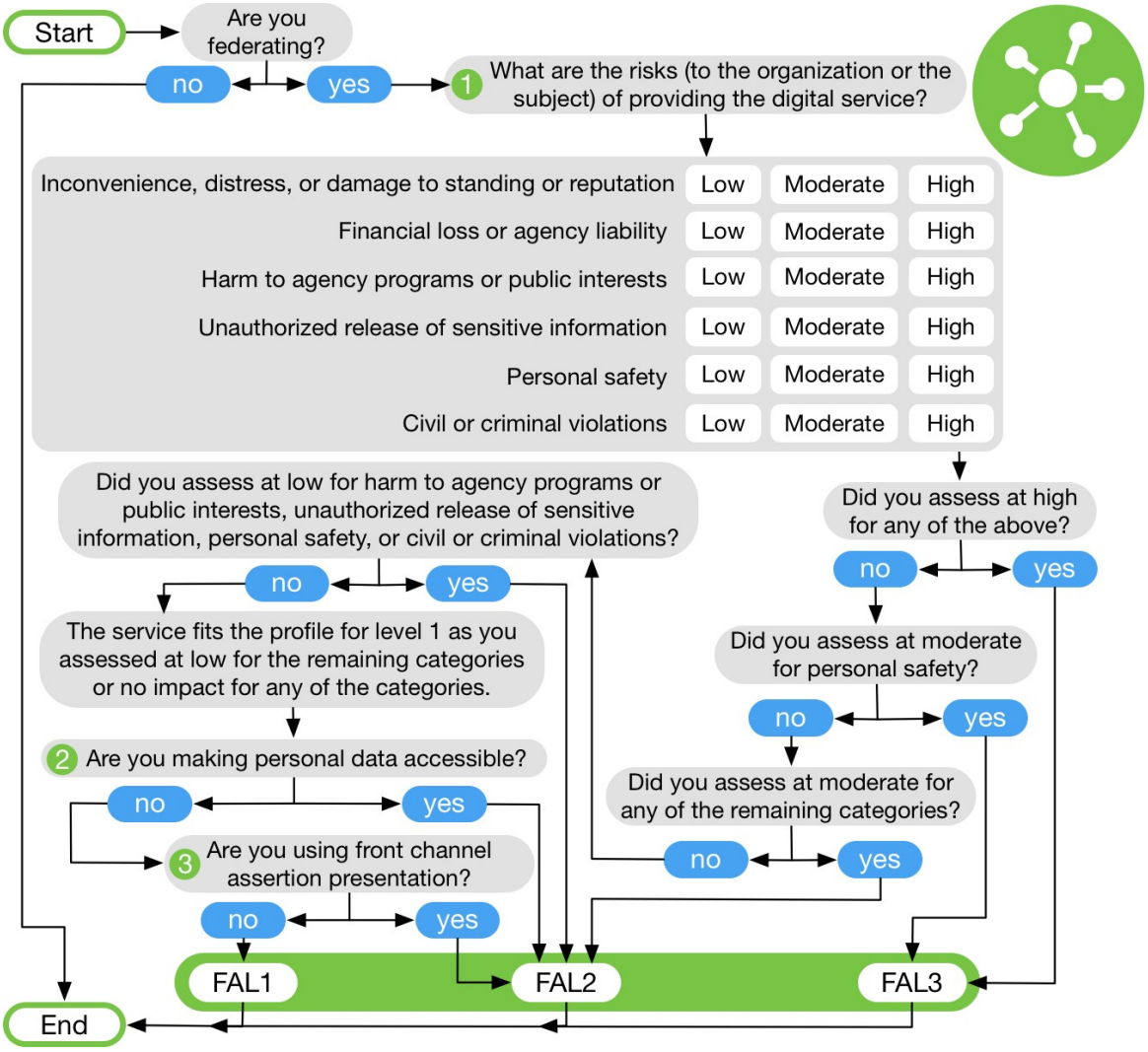
7 APPENDIX A: Identity Assurance Level Decision Chart



8 APPENDIX B: Authenticator Assurance Level Decision Chart



9 APPENDIX C: Federated Assurance Level Decision Chart



10 APPENDIX D: Resources and References

#	Reference Description
1	NIST SP 800-63-3, *Digital Identity Guidelines* - https://pages.nist.gov/800-63-3/sp800-63-3.html
2	SP 800-63A, *Enrollment & Identity Proofing* - https://pages.nist.gov/800-63-3/sp800-63a.html
3	SP 800-63B, *Authentication & Lifecycle Management* - https://pages.nist.gov/800-63-3/sp800-63b.html
4	SP 800-63C, *Federation & Assertions* - https://pages.nist.gov/800-63-3/sp800-63c.html
5	NIST SP 800-39, *Managing Information Security Risk* - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
6	Executive Order 13681, *Improving the Security of Consumer Financial Transactions*, October 17, 2014 - https://www.federalregister.gov/d/2014-25439
7	OMB M-11-11
8	OMB M-19-17