Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn and is provided solely for historical purposes. It has been followed by the document identified below.

Withdrawal Date August 21, 2024

Original Release Date December 16, 2022

The attached draft document is followed by:

Status Second Public Draft (2pd)

Series/Number NIST SP 800-63A-4 2pd

Title Digital Identity Guidelines: Identity Proofing and Enrollment

Publication Date August 2024

DOI https://doi.org/10.6028/NIST.SP.800-63A-4.2pd

CSRC URL https://csrc.nist.gov/pubs/sp/800/63/a/4/2pd

Additional Information https://www.nist.gov/identity-access-management/nist-special-publication-800-63-digital-identity-guidelines

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication
NIST SP 800-63A-4 ipd

Digital Identity Guidelines

Enrollment and Identity Proofing

Initial Public Draft

David Temoshok
Christine Abruzzi
Yee-Yin Choong
James L. Fenton
Ryan Galluzzo
Connie LaSalle
Naomi Lefkovitz
Andrew Regenscheid

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63a-4.ipd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication
NIST SP 800-63A-4 ipd

Digital Identity Guidelines

Enrollment and Identity Proofing

Initial Public Draft

David Temoshok
Ryan Galluzzo
Connie LaSalle
Naomi Lefkovitz
Applied Cybersecurity Division
Information Technology Laboratory

Yee-Yin Choong
Information Access Division
Information Technology Laboratory

Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

Christine Abruzzi
Cacapon Cyber Solutions

James L. Fenton
Altmode Networks

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63a-4.ipd

December 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies

Copyright, Fair Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History

Approved by the NIST Editorial Review Board on YYYY-MM-DD [will be added upon final publication]

How to Cite this NIST Technical Series Publication

Temoshok D, Abruzzi C, Fenton JL, Choong YY, Galluzzo R, LaSalle C, Lefkovitz N, Regenscheid A (2022) Digital Identity Guidelines: Enrollment and Identity Proofing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63A-4 ipd. https://doi.org/10.6028/NIST.SP.800-63a-4.ipd

Author ORCID iDs

David Temoshok: 0000-0001-6195-0331
Christine Abruzzi: 0000-0001-8904-930X
Yee-Yin Choong: 0000-0002-3889-6047
James L. Fenton: 0000-0002-2344-4291
Ryan Galluzzo: 0000-0003-0304-4239
Connie LaSalle: 0000-0001-6031-7550
Naomi Lefkovitz: 0000-0003-3777-3106
Andrew Regenscheid: 0000-0002-3930-527X

Public Comment Period

December 16, 2022 - ~~March 24~~ April 14, 2023

Submit Comments

mailto:dig-comments@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

These guidelines provide technical requirements for federal agencies implementing digital identity services and are not intended to constrain the development or use of standards outside of this purpose. This guideline focuses on the enrollment and verification of an identity for use in digital authentication. Central to this is a process known as identity proofing in which an applicant provides evidence to a credential service provider (CSP) reliably identifying themselves, thereby allowing the CSP to assert that identification at a useful identity assurance level. This document defines technical requirements for each of three identity assurance levels. This publication will supersede NIST Special Publication (SP) 800-63A.

Keywords

authentication; credential service provider; electronic authentication; digital authentication; electronic credentials; digital credentials; identity proofing; federation.

Note to Reviewers

The rapid proliferation of online services over the past few years has heightened the need for reliable, equitable, secure, and privacy-protective digital identity solutions.

Revision 4 of NIST Special Publication 800-63, Digital Identity Guidelines, intends to respond to the changing digital landscape that has emerged since the last major revision of this suite was published in 2017 — including the real-world implications of online risks. The guidelines present the process and technical requirements for meeting digital identity management assurance levels for identity proofing, authentication, and federation, including requirements for security and privacy as well as considerations for fostering equity and the usability of digital identity solutions and technology.

Taking into account feedback provided in response to our June 2020 Pre-Draft Call for Comments, as well as research conducted into real-world implementations of the guidelines, market innovation, and the current threat environment, this draft seeks to:

1. **Advance Equity:** This draft seeks to expand upon the risk management content of previous revisions and specifically mandates that agencies account for impacts to individuals and communities in addition to impacts to the organization. It also elevates risks to mission delivery – including challenges to providing services to all people who are eligible for and entitled to them – within the risk management process and when implementing digital identity systems. Additionally, the guidance now mandates continuous evaluation of potential impacts across demographics, provides biometric performance requirements, and additional parameters for the responsible use of biometric-based technologies, such as those that utilize face recognition.
2. **Emphasize Optionality and Choice for Consumers:** In the interest of promoting and investigating additional scalable, equitable, and convenient identify verification options, including those that do and do not leverage face recognition technologies, this draft expands the list of acceptable identity proofing alternatives to provide new mechanisms to securely deliver services to individuals with differing means, motivations, and backgrounds. The revision also emphasizes the need for digital identity services to support multiple authenticator options to address diverse consumer needs and secure account recovery.
3. **Deter Fraud and Advanced Threats:** This draft enhances fraud prevention measures from the third revision by updating risk and threat models to account for new attacks, providing new options for phishing resistant authentication, and introducing requirements to prevent automated attacks against enrollment processes. It also opens the door to new technology such as mobile driver's licenses and verifiable credentials.
4. **Address Implementation Lessons Learned:** This draft addresses areas where implementation experience has indicated that additional clarity or detail was required to effectively operationalize the guidelines. This includes re-working the federation assurance levels, providing greater detail on Trusted Referees, clarifying guidelines on identity attribute validation sources, and improving address confirmation requirements.

NIST is specifically interested in comments on and recommendations for the following topics:

Identity Proofing and Enrollment

- NIST sees a need for inclusion of an unattended, fully remote Identity Assurance Level (IAL) 2 identity proofing workflow that provides security and convenience, but does not require face recognition. Accordingly, NIST seeks input on the following questions:

178 – What technologies or methods can be applied to develop a remote, unattended
179 IAL2 identity proofing process that demonstrably mitigates the same risks as
180 the current IAL2 process?

181 – Are these technologies supported by existing or emerging technical standards?

182 – Do these technologies have established metrics and testing methodologies to
183 allow for assessment of performance and understanding of impacts across user
184 populations (e.g., bias in artificial intelligence)?

185 • What methods exist for integrating digital evidence (e.g., Mobile Driver's Licenses,
186 Verifiable Credentials) into identity proofing at various identity assurance levels?

187 • What are the impacts, benefits, and risks of specifying a set of requirements
188 for CSPs to establish and maintain fraud detection, response, and notification
189 capabilities?

190 – Are there existing fraud checks (e.g., date of death) or fraud prevention
191 techniques (e.g., device fingerprinting) that should be incorporated as baseline
192 normative requirements? If so, at what assurance levels could these be
193 applied?

194 – How might emerging methods such as fraud analytics and risk scoring be
195 further researched, standardized, measured, and integrated into the guidance in
196 the future?

197 – What accompanying privacy and equity considerations should be addressed
198 alongside these methods?

199 • Are current testing programs for liveness detection and presentation attack
200 detection sufficient for evaluating the performance of implementations and
201 technologies?

202 • What impacts would the proposed biometric performance requirements for identity
203 proofing have on real-world implementations of biometric technologies?

204 **General**

205 • Is there an element of this guidance that you think is missing or could be expanded?

206 • Is any language in the guidance confusing or hard to understand? Should we add
207 definitions or additional context to any language?

208 • Does the guidance sufficiently address privacy?

209 • Does the guidance sufficiently address equity?

210 – What equity assessment methods, impact evaluation models, or metrics
211 could we reference to better support organizations in preventing or detecting
212 disparate impacts that could arise as a result of identity verification
213 technologies or processes?

- What specific implementation guidance, reference architectures, metrics, or other supporting resources may enable more rapid adoption and implementation of this and future iterations of the Digital Identity Guidelines?
- What applied research and measurement efforts would provide the greatest impact on the identity market and advancement of these guidelines?

Reviewers are encouraged to comment and suggest changes to the text of all four draft volumes of of the NIST SP 800-63-4 suite. NIST requests that all comments be submitted by 11:59pm Eastern Time on March 24, 2023. Please submit your comments to dig-comments@nist.gov. NIST will review all comments and make them available at the NIST Identity and Access Management website. Commenters are encouraged to use the comment template provided on the NIST Computer Security Resource Center website.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: mailto:dig-comments@nist.gov.

Table of Contents

List of Tables

List of Figures

Acknowledgments

The authors would like to thank their fellow collaborators on the current revision of this special publication, Sarbari Gupta, Diana Proud-Madruga, and Justin P. Richer, as well as Kerrianne Buchanan and Greg Fiumara for their contributions and review. The authors would like to also acknowledge the past contributions of Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Emad A. Nabbus, Paul A. Grassi, Kristen Greene, Mary Theofanos, Jamie M. Danker, Adam Cooper, Alastair Treharne, Julian White, Tim Bouma, Kaitlin Boeckl, Joni Brennan, Ben Piccarreta, Ellen Nadeau, and Danna Gabel O'Rourke.

1. Purpose

This section is informative.

This publication and its companion volumes, [SP800-63], [SP800-63B], and [SP800-63C], provide technical guidelines to organizations for the implementation of digital identity services.

This document provides requirements for the identity proofing of individuals at each Identity Assurance Level (IAL) for the purposes of enrolling them into an identity service or providing them access to online resources. It applies to the identity proofing of individuals over a network or in person. Verifying the identities of people calling into a customer support service or a call center is out of scope for this document.

2. Introduction

This section is informative.

One of the challenges of providing online services is being able to associate a set of activities with a single, specific individual. While there are situations where this is not necessary - such as when anonymity or pseudonymity is desirable - there are other situations where it is important to reliably establish an association with a real-life subject. Examples of this include accessing some government services or executing financial transactions. There are also situations where association with a real-life subject is required by regulations (e.g., the financial industry's 'Know Your Customer' requirements) or to establish accountability for high-risk actions (e.g., changing the release rate of water from a dam).

This guidance defines identity proofing as the process of establishing, to some degree of certainty or assurance, a relationship between a subject accessing online services and a real-life person. This document provides guidance for Federal Agencies, third-party Credential Service Providers (CSP), and other organizations that provide identity proofing services.

The following list states which sections of this document contain normative language and which contain non-normative, informative language. Where needed to help clarify specific requirements, normative sections often include informative explanations. See the "Requirements Notation and Conventions" section of this document for clarification on which statements are normative and which are not.

- 1 Purpose *Informative*
- 2 Introduction *Informative*
- 3 Definitions and Abbreviations *Informative*
- 4 Identity Assurance Level Requirements *Normative*
- 5 Identity Resolution, Validation, and Verification *Normative*
- 6 Subscriber Accounts *Normative*
- 7 Threats and Security Considerations *Informative*
- 8 Privacy Considerations *Informative*
- 9 Usability Considerations *Informative*
- 10 Equity Considerations *Informative*

2.1. Expected Outcomes of Identity Proofing

The expected outcomes of identity proofing include:

- **Identity resolution**: determine that the claimed identity corresponds to a single, unique individual within the context of the population of users the CSP serves;
- **Evidence validation**: confirm that all supplied evidence is genuine, authentic, and unexpired;
- **Attribute validation**: confirm the accuracy of core attributes;
- **Identity verification**: verify that the claimed identity is associated with the real-life person supplying the identity evidence; and
- **Fraud Prevention**: mitigate attempts to gain fraudulent access to benefits, services, data, or assets.

2.2. Identity Assurance Levels

Assurance in a subscriber's identity is described using one of the following Identity Assurance Levels (IAL). Each successive IAL builds on the requirements of lower IALs in order to achieve greater assurance.

No identity proofing (IAL0): There is no requirement to link the applicant to a specific, real-life identity. Any attributes provided in conjunction with the subject's activities are self-asserted and are treated as self-asserted. Self-asserted attributes at IAL0 are neither validated nor verified.

IAL1: The identity proofing process supports the real-world existence of the claimed identity. Core attributes are obtained from identity evidence or asserted by the applicant. All core attributes are validated against authoritative or credible sources and steps are taken to link the attributes to the person undergoing the identity proofing process.

IAL2: IAL2 adds additional rigor to the identity proofing process by requiring the collection of stronger types of evidence and a more rigorous process for validating the evidence and verifying the identity.

IAL3: IAL3 adds the requirement for a trained CSP representative to interact directly with the applicant during the entire identity proofing session, either in person or via a supervised remote identity proofing session.

3. Definitions and Abbreviations

This section is informative

See [SP800-63] Appendix A for a complete set of definitions and abbreviations.

4. Identity Resolution, Validation, and Verification

This section is normative.

This section provides and overview of the identity proofing and enrollment process as well as requirements to support the resolution, validation, and verification of the identity claimed by an applicant. It also provides guidelines on additional aspects of the identity proofing process. These requirements are intended to ensure that the claimed identity exists in the real world and that the applicant is the individual associated with that identity. Collectively, the elements of the identity proofing process are designed to ensure that attacks against a CSP's identity service that affect a large number of enrolled subscribers require greater time and cost than the value of the data being protected.

Additionally, these guidelines provide for multiple methods by which resolution, validation, and verification can be completed as well as multiple types of identity evidence that may support the identity proofing process. To the extent practical, CSPs and organizations **SHOULD** enable optionality when implementing their identity proofing services and processes to promote access for those with different means, capabilities, and technology access. At a minimum, this **SHOULD** include accepting multiple types and combinations of identity evidence, supporting multiple data validation sources, enabling multiple methods for verifying identity (e.g., use of trusted referees), multiple channels for engagement (e.g., in-person, remote), and offering assistance mechanisms for applicants (e.g., applicant references).

4.1. Identity Proofing and Enrollment

This document describes the common pattern in which an applicant undergoes an identity proofing and enrollment process whereby their identity evidence and attributes are collected, uniquely resolved to a single identity within a given population or context, then validated and verified. See [SP800-63] for details on how to choose the most appropriate IAL. A CSP can then bind these attributes to an authenticator (described in [SP800-63B]).

The objective of identity proofing is to ensure, to a stated level of certainty, the applicant is who they claim to be. Identity proofing is not conducted to determine suitability or entitlement to benefits. The identity proofing process involves the presentation and validation of the minimum attributes necessary to accomplish identity proofing. There can be many different sets of attributes that suffice as the minimum, so CSPs choose this set by considering applicants' privacy and the usability, as well as the likely attributes needed in future uses of the digital identity. For example, such attributes, to the extent they are the minimum necessary, could include:

1. Full name
2. Date of birth
3. Home address

462 This document also provides requirements for CSPs collecting additional information
463 used for purposes other than identity proofing.

4.1.1. Process Flow

This section is informative.

Figure 1 outlines the basic flow for identity proofing and enrollment.

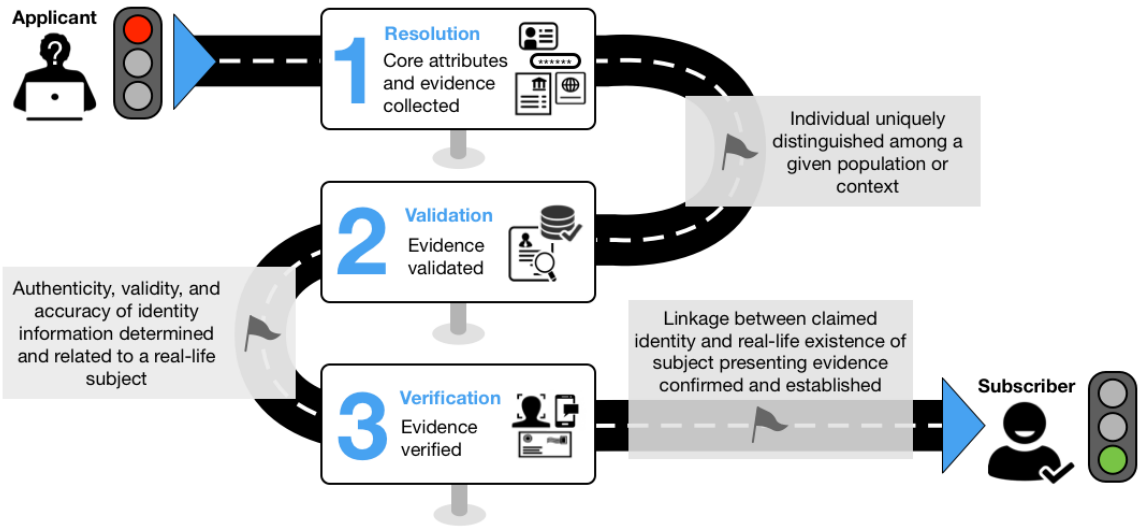

Figure 1. Identity Proofing Process

The following provides an example of how a CSP and an applicant might interact during a remote identity proofing process at IAL2:

1. **Resolution**
   a) The CSP collects attributes from the applicant, such as name, address, date of birth, email, and phone number.
   b) The CSP also collects one or more pieces of identity evidence, such as a driver's license or a passport.
2. **Validation**
   a) The CSP validates the attributes obtained in steps 1a by checking them against authoritative or credible sources.
   b) The CSP validates the authenticity, accuracy, and currency of the presented evidence.
3. **Verification**
   a) The CSP asks the applicant to take a photo of themself, with liveness checks.
   b) The CSP compares the pictures on the license and the passport to the photo of the live applicant's photo from the previous step and determines they match.

c) The CSP sends an enrollment code to the validated phone number of the applicant, the applicant provides the enrollment code to the CSP, and the CSP confirms they match, verifying they the applicant is in possession and control of the validated phone number.

d) The applicant has been successfully identity proofed and can be enrolled into a subscriber account.

4.2. Identity Resolution

The goal of identity resolution is to use the smallest set of attributes to uniquely distinguish an individual within a given population or context. While identity resolution is the starting point in the overall identity proofing process, to include the initial detection of potential fraud, it in no way represents a complete and successful identity proofing transaction.

4.3. Identity Validation and Identity Evidence Collection

The goal of identity validation is to collect the most appropriate identity evidence and attribute information from the applicant and determine it is authentic, accurate, current, and unexpired. Identity validation is made up of three process steps: 1) collecting the appropriate identity evidence; 2) confirming the evidence is authentic; and, 3) confirming key data contained on the identity evidence is valid, current, and related to a real-life subject.

Identity evidence collection supports the identity validation process and consists of two steps: 1) presentation of identity evidence by the identity proofing applicant to the CSP and 2) determination by the CSP that the presented evidence is acceptable. Evidence can be presented as a physical document or a copy, photograph, or scan of a document, or as a digital record. The characteristics for acceptable physical (documentary) identity evidence are presented in Sec. 4.3.1 and the characteristics for acceptable digital evidence are provided in Sec. 4.3.2.

The CSP **SHALL** determine the acceptability of presented identity evidence for identity proofing based on the evidence characteristics in this section.

The characteristics presented in this section are intended to guide CSPs in determining what is acceptable as identity evidence for the identity proofing process and are not an indication of strength of evidence. Once a CSP determines a particular type of evidence is acceptable, a determination must be made as to its strength, as provided in Sec. 4.3.3.

4.3.1. Characteristics of Acceptable Physical Evidence

Acceptable physical evidence **SHALL** contain all of the following characteristics:

1. The presented document contains the printed name of the applicant. (See Sec. 10.1 - Equity and Resolution - for guidance on dealing with a printed name that varies from the applicant's claimed identity.)
2. The presented document contains at least one printed reference number.
3. The presented document contains the printed name of the issuer of the document.
4. The issuer of the document performed identity proofing of the applicant prior to issuing the document.
5. There is reasonable assurance that the document was delivered to the intended person.

4.3.2. Characteristics of Acceptable Digital Evidence

Acceptable digital evidence **SHALL** contain all of the following characteristics:

1. The presented digital evidence contains the name of the applicant as the subject of the digital information or account. (See Sec. 10.1 - Equity and Resolution - for guidance on dealing with a name on digital evidence that varies from the applicant's claimed identity.)
2. The presented digital evidence contains at least one reference (e.g., account number) or sufficient attributes to bind the digital information to the applicant.
3. The presented digital evidence contains the name of the issuer of the digital information.
4. The issuer of the digital evidence performed identity proofing of the applicant prior to issuing the digital evidence.
5. There is reasonable assurance that the digital evidence was delivered or made accessible to intended person.
6. If applicable, the presented digital evidence can be verified through authentication at an AAL or FAL commensurate with the assessed IAL.

4.3.3. Evidence Strength Requirements

This section defines the requirements for identity evidence at each strength. Strength of identity evidence is determined by three aspects: 1) the issuing rigor; 2) the ability to provide confidence in validation, including accuracy and integrity of attributes; and 3) the ability to provide confidence in the verification of the applicant presenting the evidence. Evidence at all levels of strength must be current and unexpired.

4.3.3.1. Fair Evidence Requirements

In order to be considered FAIR, identity evidence **SHALL** meet *all* the following requirements:

1. The issuing source of the evidence confirmed the claimed identity through an identity proofing process.
2. It can be reasonably assumed that the evidence issuing process would result in the delivery of the evidence to the person to whom it relates.
3. The evidence contains at least one reference number, a facial portrait, or sufficient attributes to uniquely identify the person to whom it relates.
4. The evidence has not expired or it expired within the previous six (6) months, or it was issued within the previous six (6) months if it does not contain an expiration date.

4.3.3.2. Strong Evidence Requirements

In order to be considered STRONG, identity evidence **SHALL** meet *all* the following requirements:

1. The issuing source of the evidence confirmed the claimed identity through written procedures designed to enable it to form a reasonable belief that it knows the real-life identity of the person. Such procedures are subject to recurring oversight by regulatory or publicly-accountable institutions. For example, the Customer Identification Program guidelines established in response to the USA PATRIOT Act of 2001 or the [RedFlagsRule], under Sec. 114 of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act).
2. There is a high likelihood that the evidence issuing process would result in the delivery of the evidence to the person to whom it relates.
3. The evidence contains a reference number or other attributes that uniquely identify the person to whom it relates.
4. The evidence contains a facial portrait or other biometric characteristic of the person to whom it relates.
5. The evidence includes physical security features that make it difficult to copy or reproduce.
6. The evidence includes an expiration date and is unexpired.

4.3.3.3. Superior Evidence Requirements

In order to be considered SUPERIOR, identity evidence **SHALL** meet *all* the following requirements:

1. The issuing source of the evidence confirmed the claimed identity by following written procedures designed to enable it to have high confidence that the source knows the real-life identity of the subject. Such procedures are subject to recurring oversight by regulatory or publicly accountable institutions.
2. The issuing source visually identified the applicant and performed further checks to confirm the existence of that person.
3. The issuing process for the evidence ensured that it was delivered into the possession of the person to whom it relates.
4. The evidence contains at least one reference number that uniquely identifies the person to whom it relates.
5. The evidence contains a facial portrait or other biometric characteristic of the person to whom it relates.
6. The evidence includes digital information that is cryptographically signed.
7. The evidence includes physical security features that make it difficult to copy or reproduce.
8. The evidence includes an expiration date and is unexpired.

4.3.4. Identity Evidence and Attribute Validation

The CSP **SHALL** validate all identity evidence collected to meet evidence collection requirements and all core attribute information required by the CSP identity service.

4.3.4.1. Evidence Validation

The CSP **SHALL** validate the authenticity, accuracy, and currency of presented evidence by:

- Confirming the evidence is in the correct format and includes complete information for the identity evidence type.
- Confirming the evidence is not counterfeit and that it as not been tampered with.
- Confirming any security features.

The CSP **SHALL** validate that the evidence is current through confirmation that its expiration date has not passed or that evidence without an expiration date was issued within the previous six (6) months.

The authenticity and accuracy of identity evidence or attribute information that is cryptographically protected can be validated through verification of the digital signature

on the evidence or the attribute data objects. The CSP **SHALL** use the public key of the issuing authority of the evidence to verify digitally signed evidence or attribute data objects.

4.3.4.2. Attribute Validation

All core attributes, whether obtained from identity evidence or applicant self-assertion, must be validated. This subsection provides guidance on acceptable methods for validating evidence and collected attributes.

4.3.4.3. Evidence and Attribute Validation Methods

Acceptable methods for validating presented evidence include:

- Visual and tactile inspection by trained personnel for in-person identity proofing,
- Visual inspection by trained personnel for remote identity proofing,
- Automated document validation processes using appropriate technologies,
- Validation of attributes contained on the evidence with an authoritative or credible source.
- Verification of the digital signature protecting digital evidence or attribute data objects using the public key of the issuing authority of the evidence.

4.3.4.4. Validation Sources

Core attributes that are contained on identity evidence that has been validated according to Sec. 4.3.4.1 can be considered validated, in which case no further validation is required.

An authoritative source is an entity that can provide or validate the accuracy of identity attribute information through one or more of the following characteristics. An authoritative source:

- Is the original source of the identity attribute(s); or
- Is the issuer of identity evidence containing identity attribute information and the issuer confirmed the claimed identity through documented identity proofing processes that are subject to recurring oversight by regulatory or publicly accountable institutions, such as the Customer Identification Program guidelines established under the [PatriotAct]; or
- Collected and validated attribute information through an identity proofing process that can confirm the claimed identity through direct interaction with individuals (either in-person or remotely); or
- Has access to evidence and attribute information that can be traced to the issuing source of a piece of identity evidence.

A credible source is an entity that can provide or validate the accuracy of identity evidence and attribute information through one or more of the following characteristics. A credible source:

- Has access to attribute information that was validated through an identity proofing process; or
- Has access to attribute information that can be traced to an authoritative source; or
- Maintains identity attribute information obtained from multiple sources that is checked for data correlation for accuracy, consistency, and currency.

4.4. Identity Verification

The goal of identity verification is to confirm and establish a linkage between the claimed identity and the real-life existence of the applicant engaged in the identity proofing process.

4.4.1. Identity Verification Methods

The CSP **SHALL** verify the linkage of the claimed identity to the applicant engaged in the identity proofing process through one or more of the following methods, depending on the IAL identity verification requirements presented in Sec. 5.

- **Enrollment code verification** as specified in Sec. 5.1.6.
- **In-person physical comparison**. The CSP operator and applicant interact in person for the identity proofing event. The CSP operator performs a physical comparison of the facial portrait presented on identity evidence to the face of the applicant engaged in the identity proofing event.
- **Remote (attended and unattended) physical facial image comparison**. The CSP operator performs a physical comparison of the facial portrait presented on identity evidence to the facial image of the applicant engaged in the identity proofing event. The CSP operator may interact directly with the applicant during some or all of the identity proofing event (attended) or may conduct the comparison at a later time (unattended) using a captured video or photograph and the uploaded copy of the evidence. If the comparison is performed at a later time, steps are taken to ensure the captured video or photograph was taken from the live applicant present during the identity proofing event.
- **Automated biometric comparison**. Biometric system comparison may be performed for in-person or remote identity proofing events. The facial portrait, or other biometric characteristic, contained on identity evidence is compared by an automated biometric comparison system to the facial image photograph of the live applicant or other biometric live sample submitted by the applicant during the identity proofing event. The automated biometric comparison system uses a mathematical algorithm for the comparison.

- **Control of a digital account**. An individual is able to demonstrate control of a digital account (e.g., online bank account) or signed digital assertion (e.g., verifiable credentials) through the use of authentication or federation protocols. This may be done in person through presentation of the credential to a device or reader, but is more likely to be done during remote identity proofing sessions.

5. Identity Assurance Level Requirements

This section is normative.

This section provides requirements for CSPs that operate identity proofing and enrollment services, including requirements for identity proofing at each of the IALs. This section also includes additional requirements for Federal Agencies regardless of whether they operate their own identity service or use an external CSP.

5.1. General Requirements

The requirements in this section apply to all CSPs performing identity proofing at any IAL.

5.1.1. Identity Service Documentation and Records

The CSP **SHALL** conduct its operations according to a practice statement that details all identity proofing processes as they are implemented to achieve the defined IAL. The practice statement **SHALL** include, at a minimum:

1. A complete service description including the particular steps the CSP follows to identity proof applicants at each offered assurance level;
2. Types of identity evidence the CSP accepts to meet the evidence strength requirements;
3. If applicable, alternative ways for an individual applicant who does not possess the required identity evidence to complete the identity proofing process[1];
4. The attributes the CSP considers to be core attributes. Core attributes include the minimum set of attributes the CSP needs to perform identity resolution as well as any additional attributes the CSP collects and validates for the purposes of identity proofing, fraud mitigation, complying with laws or legal process, or conveying to relying parties (RPs) through attribute assertions;
5. The CSP's policy and process for dealing with identity proofing errors;
6. The CSP's policy and process for identifying and communicating suspected or confirmed fraudulent accounts to RPs and affected individuals;
7. The CSP's policy for managing and communicating service changes (e.g., change in data sources, integrated vendors, or biometric algorithms) to RPs;
8. The CSP's policy for conducting privacy risk assessments, including the timing of its periodic reviews and specific conditions that will trigger an updated privacy risk assessment (see Section 5.1.2);

[1] Options include using a Trusted Referee, with or without an Applicant Representative; see Sec. 5.1.9 for supplemental identity evidence types.

9. The CSP's policy for conducting assessments to determine potential equity impacts, including the timing of its periodic reviews and any specific conditions that will trigger an out-of-cycle review (see Section 5.1.3); and

5.1.1.1. Ceasing Operations

1. The CSP **SHALL** document its policy and plan for when it ceases its operations.
2. This plan **SHALL** include whether the CSP's identity service is subject to retention requirements and how it will protect any sensitive data (including identity attributes, and information contained in subscriber accounts and audit logs) during the period of retention.
3. At the end of any required retention period, the CSP **SHALL** be responsible for fully disposing of or destroying all sensitive data.

5.1.1.2. Fraud Mitigation Measures

1. The CSP **SHOULD** obtain additional confidence in identity proofing using fraud mitigation measures (e.g., examining the device characteristics of the applicant, evaluating behavioral characteristics, and checking vital statistic repositories such as the Death Master File ([DMF]).
2. In the event the CSP uses fraud mitigation measures, the CSP **SHALL** conduct a privacy risk assessment for these mitigation measures.
3. Such assessments **SHALL** include any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography), and be documented per these guidelines.

5.1.2. General Privacy Requirements

The following privacy requirements apply to all CSPs providing identity services at any IAL.

5.1.2.1. Privacy Risk Assessment

1. The CSP **SHALL** conduct and document a privacy risk assessment for the processes used for identity proofing and enrollment.[2] At a minimum, the privacy risk assessment **SHALL** assess the risks associated with:
    a) Any processing of PII for the purpose of identity proofing and enrollment, including identity attributes, biometrics, images, video, scans, or copies of identity evidence;

[2] For more information about privacy risk assessments, refer to the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.

753 b) Any additional steps the CSP takes to verify the identity of an applicant
754 beyond the mandatory requirements specified herein;

755 c) Any processing of PII for purposes outside the scope of identity proofing and
756 enrollment except to comply with law or legal process;

757 d) The retention schedule for identity records and PII; and,

758 e) Any PII that is processed by a third party service on behalf of the CSP.

759 2. Based on the results of its privacy risk assessment, the CSP **SHALL** document the
760 measures it takes to maintain the disassociability, predictability, manageability,
761 confidentiality, integrity, and availability of the PII it processes. In determining
762 such measures, the CSP **SHALL** consult the *NIST Privacy Framework*
763 [NIST-Privacy] and NIST Special Publication [SP800-53].

764 3. The CSP **SHALL** re-assess privacy risks and update its privacy risk assessment any
765 time it makes changes to its identity service that affect the processing of PII.

766 4. The CSP **SHALL** review its privacy risk assessment periodically, as documented
767 in its practice statement, to ensure it accurately reflects the current risks associated
768 with the processing of PII.

769 5. The CSP **SHALL** make a summary of its privacy risk assessment available to any
770 organizations that use its services. The summary **SHALL** be in sufficient detail to
771 enable such organizations to do due dilligence.

772 5.1.2.2. Additional Privacy Protective Measures

773 1. Processing of PII **SHALL** be limited to the minimum necessary to validate the
774 existence of the claimed identity, associate the claimed identity with the applicant,
775 and provide RPs with attributes they may use to make authorization decisions.

776 2. The CSP **MAY** collect the Social Security Number (SSN) as an attribute when
777 necessary for identity resolution, in accordance with the privacy requirements in
778 Sec. 5.1.2. Additionally, CSPs **SHALL** implement privacy protective techniques
779 (e.g., transmitting and accepting derived attribute values rather than full attribute
780 values themselves) to limit the proliferation and retention of SSN data. Knowledge
781 of the SSN **SHALL NOT** be considered identity evidence.

782 3. At the time of collection, the CSP **SHALL** provide explicit notice to the applicant
783 regarding the purpose for collecting attributes necessary for identity proofing,
784 including whether such attributes are voluntary or mandatory to complete the
785 identity proofing process, the specific attributes and other sensitive data that
786 the CSP intends to store in the applicant's subsequent subscriber account, the
787 consequences for not providing the attributes, and the details of any records
788 retention requirement if one is in place.

4. The CSP **SHALL** provide mechanisms for redress of applicant complaints and for problems arising from the identity proofing. These mechanisms **SHALL** be easy for applicants to find and use. The CSP **SHALL** assess the mechanisms for their efficacy in achieving resolution of complaints or problems.

5.1.3. General Equity Requirements

In support of the goal of improved equity, and as part of its overall risk assessment process, the CSP **SHALL** assess the elements of its identity service to identify processes or technologies that can possibly result in inequitable access, treatment, or outcomes for members of one group as compared to others. See Sec. 10 for a non-exhaustive list of identity proofing processes and technologies that may be subject to inequitable access or outcomes.

Note that executive order 13985 [EO13985], *Advancing Racial Equity and Support for Underserved Communities Through the Federal Government*, requires each federal agency to assess whether, and to what extent, its programs and policies perpetuate systemic barriers to opportunities and benefits for people of color and other underserved groups.

When assessing the risk of inequitable access, treatment, or outcomes, the following requirements apply:

1. Based on the results of its risk assessment, the CSP **SHALL** document the measures it takes to mitigate the possibility of inequitable access, treatment, or outcomes.
2. The CSP **SHALL** re-assess the risks to equitable access, treatment, or outcomes any time it makes changes to its identity service that affect the processes or technologies.
3. The CSP **SHALL** re-assess the risks to equitable access, treatment, or outcomes periodically to ensure it accurately reflects the current risks associated with its service.
4. The CSP **SHALL NOT** make applicant participation in these risk assessments mandatory.
5. The CSP **SHALL** make the results of its assessment of risks associated with inequitable access, treatment, or outcomes, and any associated mitigations, available to any organizations or individuals that use its service.
6. The CSP **SHALL** also make the results of its assessment publicly available.

5.1.4. General Security Requirements

1. Each online transaction within the identity proofing process, including transactions that involve third parties, **SHALL** occur over an authenticated protected channel.
2. All PII, in the form of identity attributes, collected as part of the identity proofing process **SHALL** be protected to ensure the confidentiality and integrity of the information.
3. The CSP **SHALL** assess the risks associated with operating its identity service, according to the NIST risk management framework [NIST-RMF], and apply an appropriate baseline security controls.

5.1.5. Additional Requirements for Federal Agencies

The following requirements apply to federal agencies, regardless of whether they operate their own identity service or use an external CSP as part of their identity service:

1. The agency **SHALL** consult with their Senior Agency Official for Privacy (SAOP) to conduct an analysis determining whether the collection of PII, including biometrics, to conduct identity proofing triggers Privacy Act requirements.
2. The agency **SHALL** consult with their SAOP to conduct an analysis determining whether the collection of PII, including biometrics, to conduct identity proofing triggers E-Government Act of 2002 [E-Gov] requirements.
3. The agency **SHALL** publish a System of Records Notice (SORN) to cover such collection, as applicable.
4. The agency **SHALL** publish a Privacy Impact Assessment (PIA) to cover such collection, as applicable.
5. The agency **SHALL** consult with the senior official, office, or governance body responsible for diversity, equity, inclusion, and accessibility (DEIA) for their agency to determine how the identity proofing service should be designed, resourced, and administered to meet the needs of all served populations.
6. The agency **SHOULD** consult with public affairs and communications professionals within their organization to determine if a communications or public awareness strategy should be developed to accompany the roll-out of any new process, or an update to an existing process, including requirements associated with identity proofing. This may include materials detailing information about how to use the technology associated with the service, a Frequently Asked Questions (FAQs) page, prerequisites to participate in the identity proofing process (such as required evidence), webinars or other live or pre-recorded information sessions, or other media to support adoption and provide applicants with a mechanism to communicate questions, issues, and feedback.

7. If the agency uses a third-party CSP, the agency SHALL be responsible for conducting its own privacy risk assessments or doing due diligence before relying on the CSP's privacy risk assessment as part of its PIA process.
8. If the agency uses a third-party CSP, the agency **SHALL** incorporate the CSP's assessment of equity risks into its own assessment of equity risks.

5.1.6. Requirements for Enrollment Codes

Enrollment codes are used to confirm an applicant has access to a validated address. If identity proofing and enrollment are not completed in a single session, an enrollment code can also be used to re-establish an applicant's binding to their enrollment record for the purposes of completing the enrollment process.

The following requirements apply to all CSPs that employ enrollment codes at any IAL:

1. Enrollment codes **SHALL** be sent to a validated address (e.g., postal address, telephone number, or email address).
2. The applicant **SHALL** present a valid enrollment code to complete the identity proofing process.
3. Enrollment codes **SHALL** be comprised of one of the following:
    a) A random six digit number generated by an approved random number generator with at least 20 bits of entropy;
    b) A secure link delivered to a uniquely identified address containing an appropriately constructed session ID (at least 64 bits of entropy); or
    c) A machine readable optical label (such as a QR code) that contains a random secret with at least 20 bits of entropy.
4. Enrollment codes **SHALL** be valid for at most:
    a) 21 days, when sent to a validated postal address within the contiguous United States;
    b) 30 days, when sent to a validated postal address outside the contiguous United States;
    c) 10 minutes, when sent to a validated telephone number (SMS or voice); or
    d) 24 hours, when sent to a validated email address.
5. The enrollment code **SHALL NOT** be used as an authentication factor.

5.1.7. Requirements for Notifications of Identity Proofing

Notifications of proofing are sent to the applicant's validated address notifying them that they have been successfully identity proofed. These notices provide added assurance that the person who underwent identity proofing is the owner of the claimed identity.

The following requirements apply to all CSPs that send notifications of proofing as part of their identity proofing processes at any IAL.

Notifications of proofing:

1. **SHALL** be sent to a validated address (e.g., postal address, telephone number, or email address) of record. Whenever possible, CSPs **SHOULD** send notifications of proofing and enrollment codes to different validated addresses.
2. **SHALL** include details about the identity proofing event, such as the name of the identity service and the date the identity proofing was completed.
3. **SHALL** provide clear instructions, including contact information, on actions to take in the case the recipient repudiates the identity proofing event.
4. **SHOULD** provide additional information, such as how the organization or CSP protects the security and privacy of the information it collects and any responsibilities the recipient has as a subscriber of the identity service.

5.1.8. Requirements for Use of Biometrics

Biometrics is the automated recognition of individuals based on their biological and behavioral characteristics such as, but not limited to, fingerprints, iris structures, or facial features that can be used to recognize an individual. As used in these guidelines, biometric data refers to any analog or digital representation of biological and behavioral characteristics at any stage of their capture, storage, or processing. This includes live biometric samples from applicants (e.g., facial images, fingerprint), as well as biometric references obtained from evidence (e.g., facial image on a driver's license, fingerprint minutiae template on identification cards). As applied to the identity proofing process, CSPs may use biometrics to uniquely resolve an individual identity within a given population or context, verify that an individual is the rightful subject of identity evidence, and/or bind that individual to a new piece of identity evidence or credential.

The following requirements apply to CSPs that employ biometric mechanisms as part of their identity proofing process:

1. CSPs **SHALL** provide clear, publicly available information about all uses of biometrics, what biometric data is collected, how it is stored, and information on how to remove biometric information consistent with applicable laws and regulations.
2. CSPs **SHALL** collect an explicit biometric consent from all applicants before collecting biometric information.

3. CSPs **SHALL** store the biometric consent with the subscriber's account.
4. CSPs **SHALL** have a documented, and publicly available, deletion process and default retention period for all biometric information.
5. CSPs **SHALL** allow individuals to request deletion of their biometric information at any time, except where otherwise restricted by regulation, law, or statute.
6. CSPs **SHALL** have all biometric algorithms tested by an independent entity (e.g., accredited laboratory or research institution) for performance, including performance across demographic groups.
7. Testing of all algorithms **SHALL** be consistent with published ISO/IEC standards for the given modality.
8. CSPs **SHALL** meet the minimum performance thresholds for biometric usage:
    - False match rate: 1:10,000 or better; and
    - False non-match rate: 1:100 or better
9. CSPs **SHALL** employ biometric technologies that provide similar performance characteristics for applicants of different demographic groups (racial background, gender, ethnicity, etc.). If performance differences across demographic groups are discovered, CSPs **SHALL** act expeditiously to provide redress options to affected individuals and to close performance gaps.
10. CSPs **SHALL** make all performance and operational test results publicly available.
11. CSPs **SHALL** assess the performance and demographic impacts of employed biometric technologies in conditions substantially similar to the operational environment and user base of the system. When such assessments include real-world users, participation by users **SHALL** be voluntary.
12. CSPs **SHALL** make all performance and operational test results publicly available.

The following requirements apply to CSPs who collect biometric characteristics from applicants:

1. CSP **SHALL** collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject.
2. When collecting and comparing biometrics remotely, the CSP **SHALL** implement liveness detection capabilities to confirm the genuine presence of a live human being and to mitigate spoofing and impersonation attempts.
3. When collecting biometrics in person, the CSP **SHALL** have the operator view the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process.

5.1.9. Trusted Referees and Applicant References

To increase accessibility and promote equal access to online government services, CSPs provide *trusted referees*. Trusted referees are used to facilitate the identity proofing and enrollment of individuals who are otherwise unable to meet the requirements for identity proofing to a specific IAL. Examples of such individuals and demographic groups include: individuals who do not possess and cannot obtain the required identity evidence; persons with disabilities; older individuals; persons experiencing homelessness; individuals with little or no access to online services or computing devices; persons without a bank account or with limited credit history; victims of identity theft; individuals displaced or affected by natural disasters; and children under 18.

Trusted referees are agents of the CSP or its partners who are trained and authorized to make risk-based decisions to facilitate the identity proofing and enrollment of individuals who are unable to complete the identity proofing process on their own or meet the specified requirements for a given IAL.

Additionally, there may be circumstances that encumber or preclude the active participation of an applicant in the identity proofing process. Such circumstances may be due to physical or mental limitations, disabilities, hospitalization, or other temporary or permanent conditions that make active participation in the identity proofing difficult. An *applicant reference* may vouch for an applicant's particular circumstances and may also actively assist the applicant in the identity proofing process.

Applicant references are individuals who participate in the identity proofing of an applicant in order to assist the applicant in meeting the identity proofing requirements. Such assistance may include vouching for the applicant's circumstances and actively assisting the applicant in completing the identity proofing process. Applicant references are not agents of the CSP but they would typically work in conjunction with a trusted referee to facilitate the identity proofing and enrollment of an applicant. Since information provided by the applicant reference may be used and relied upon in the identity proofing of the applicant, the applicant reference is identity proofed to the same or higher IAL as the applicant. The role of applicant reference is limited to facilitating the identity proofing process and applicant references are not authorized to represent subscribers in transactions with RPs. Persons who simply provide physical, technical, language translation or other similar assistance to an applicant who is otherwise able to meet the requirements for identity proofing to the specified IAL are not considered to be applicant references and do not require identity proofing.

5.1.9.1. Requirements for Trusted Referees

CSPs **SHALL** provide the option for the use of trusted referees for remote identity proofing at IALs 1 and 2.

Where trusted referees are offered, the following requirements apply to their use:

997 1. The CSP **SHALL** establish written policies and procedures for the use of trusted
998 referees as part of its practice statement, as specified in Sec. 5.1.1.
999 2. The CSP **SHALL** train its trusted referees to make risk-based decisions that allow
1000 applicants to be successfully identity proofed based on their unique circumstances.
1001 3. The CSP **SHALL** provide notification to the public of the availability of trusted
1002 referee services and how such services are obtained.

1003 #### 5.1.9.2. Requirements for Applicant References

1004 CSPs **SHOULD** allow the use of applicant references.

1005 The following requirements apply to the use of applicant references at any IAL:

1006 1. The CSP **SHALL** establish written policies and procedures for the use of applicant
1007 references as part of its practice statement, as specified in Sec. 5.1.1.
1008 2. The CSP **SHALL** identity proof an applicant reference to the same or higher IAL
1009 intended for the applicant.
1010 3. If the CSP allows for the use of applicant references, it **SHALL** provide notification
1011 to the public of the allowability of applicant references and any requirements for the
1012 relationship between the reference and the applicant.

1013 ### 5.1.10. Requirements for Interacting with Minors

1014 The following requirements apply to all CSPs providing identity proofing services to
1015 minors at any IAL.

1016 1. The CSP **SHALL** establish written policy and procedures as part of its practice
1017 statement for identity proofing minors who may not be able to meet the evidence
1018 requirements for a given IAL.
1019 2. When interacting with persons under the age of 13, the CSP **SHALL** ensure
1020 compliance with the Children's Online Privacy Protection Act of 1998 [COPPA].
1021 3. CSPs **SHALL** support the use of applicant references when interacting with
1022 individuals under the age or 18.

1023 ## 5.2. Identity Proofing Process

1024 This document provides requirements that apply to several different identity proofing
1025 methods. These possible methods include:

1026 - A fully automated, remote process;
1027 - A CSP operator-assisted remote process;
1028 - A combination of automated and operator-assisted remote process;

- An in-person, physical interaction with the applicant process; and
- An IAL3 Supervised Remote Identity Proofing process.

Identity proofing at IAL1 and IAL2 allow for any of the these processes to be used, while IAL3 requires in-person, physical interaction with the applicant or IAL3 Supervised Remote Identity Proofing.

The following sections provide requirements for identity proofing at each IAL.

5.3. Identity Assurance Level 1

IAL1 permits both remote and in-person identity proofing. Identity proofing processes at IAL1 allow for a range of acceptable techniques in order to detect the presentation of fraudulent identities by a malicious actor while facilitating user adoption and minimizing false negatives and application departures (legitimate applicants who do not successfully complete identity proofing). Notably, the use of biometric matching, such as the automated comparison of a facial portrait to supplied evidence, at IAL1 is optional, providing pathways to proofing and enrollment where such collection may not be viable or where privacy and equity risks outweigh security considerations.

The following requirements apply to all CSPs providing identity proofing and enrollment services at IAL1.

5.3.1. Automated Attack Prevention

The CSP **SHALL** implement a means to prevent automated attacks on the identity proofing process. Acceptable means include, but are not limited to: bot detection, mitigation, and management solutions; behavioral analytics; web application firewall settings; and traffic analysis.

5.3.2. Evidence and Core Attributes Collection Requirements

5.3.2.1. Evidence Collection

For remote or in-person identity proofing, the CSP **SHALL** collect *one* of the following from the applicant:

1. One piece of SUPERIOR evidence, or
2. One piece of STRONG evidence and one piece of FAIR evidence

5.3.2.2. Collection of Additional Attributes

Validated evidence is the preferred source of identity attributes. If the presented identity evidence does not provide all the attributes the CSP considers core attributes, it **MAY** collect attributes that are self-asserted by the applicant.

5.3.3. Evidence and Core Attributes Validation Requirements

The CSP **SHALL** validate the genuineness of each piece of SUPERIOR and STRONG evidence by *one* of the following:

1. Visual inspection by trained personnel
2. The use of technologies that can confirm the integrity of physical security features or detect if the evidence is fraudulent or has been inappropriately modified
3. If present, confirming the integrity of digital security features

The CSP **SHALL** validate the genuineness of each piece of FAIR evidence by visual inspection by trained personnel.

The CSP **SHALL** validate all core attributes by *both*:

1. Validating the accuracy of attributes (such as account or reference number, name, and date of birth) obtained from pieces of evidence by comparison with authoritative or credible sources, and
2. Validating the accuracy of self-asserted attributes by comparison with authoritative or credible sources.

For added assurance, the CSP **SHALL** evaluate the core attributes, as validated by various sources, for overall consistency.

5.3.4. Identity Verification Requirements

The CSP **SHALL** verify the binding of the applicant to the claimed identity by *one* of the following:

1. Physical comparison of the applicant's face or biometric comparison of the facial image of the applicant to the facial portrait included on a piece of SUPERIOR or STRONG evidence, or
2. Demonstrated association with a digital account through an AAL1 authentication or an AAL1 and FAL1 federation protocol, or
3. Verification of the applicant's return of a valid enrollment code Sec. 5.1.6

5.3.5. Notification of Proofing Requirement

Upon the successful completion of identity proofing at IAL1, the CSP **SHOULD** send a notification of proofing to a validated address for the applicant, as specified in Sec. 5.1.7.

5.4. Identity Assurance Level 2

Like IAL1, IAL2 identity proofing allows for both remote and in-person identity proofing processes in order to maximize accessibility while still mitigating against impersonation attacks and other identity proofing errors. Remote IAL2 identity proofing can be accomplished by the CSP via a fully automated process, a CSP operator attended process, or a combination of the two.

5.4.1. Automated Attack Prevention

The CSP **SHALL** implement a means to prevent automated attacks on the identity proofing process. Acceptable means include, but are not limited to: bot detection, mitigation, and management solutions; behavioral analytics; web application firewall settings; and traffic analysis.

5.4.2. Evidence and Core Attribute Collection Requirements

5.4.2.1. Evidence Collection

For remote or in-person identity proofing, the CSP **SHALL** collect *one* of the following from the applicant:

1. One piece of SUPERIOR evidence
2. One piece of STRONG evidence and one piece of FAIR evidence

5.4.2.2. Collection of Attributes

Validated evidence is the preferred source of identity attributes. If the presented identity evidence does not provide all the attributes the CSP considers core attributes, it **MAY** collect attributes that are self-asserted by the applicant.

5.4.3. Evidence and Core Attributes Validation Requirements

The CSP **SHALL** validate the genuineness of each piece of SUPERIOR and STRONG evidence by one of the following:

1. Visual inspection by trained personnel
2. The use of technologies that can confirm the integrity of physical security features or detect if the evidence is fraudulent or has been inappropriately modified
3. If present, confirming the integrity of digital security features

The CSP **SHALL** validate all core attributes by:

1. Validating the accuracy of attributes (such as account or reference number, name, and date of birth) obtained from pieces of evidence by comparison with authoritative or credible sources, and

2. validating the accuracy of self-asserted attributes by comparison with authoritative or credible sources

For added assurance, the CSP **SHALL** evaluate the core attributes, as validated by various sources, for overall consistency.

5.4.4. Identity Verification Requirements

5.4.4.1. Remote Identity Proofing

The CSP **SHALL** verify the binding of the applicant to the claimed identity by *one* of the following:

1. Comparison of a collected biometric characteristic, such as a facial image, to the associated reference biometric contained on a piece of presented SUPERIOR or STRONG evidence
2. Demonstrated association with a digital account through an AAL2 authentication or an AAL2 and FAL2 federation protocol

5.4.4.2. In-person Identity Proofing

The CSP **SHALL** verify the binding of the applicant to the claimed identity by physical or biometric comparison of the facial image of the applicant to the facial portrait contained on a piece of presented SUPERIOR or STRONG evidence.

5.4.5. Notification of Proofing Requirement

Upon the successful completion of identity proofing at IAL2, the CSP **SHALL** send a notification of proofing to a validated address for the applicant, as specified in Sec. 5.1.7.

5.5. Identity Assurance Level 3

IAL3 adds additional rigor to the steps required at IAL2 and is subject to additional and specific processes (including the use of biometric information comparison, collection, and retention) to further protect the identity and RP from impersonation, fraud, or other significantly harmful damages. In addition, identity proofing at IAL3 is performed in person (to include supervised remote identity proofing defined in Sec. 5.5.8).

5.5.1. Automated Attack Prevention

The CSP **SHALL** implement a means to prevent automated attacks on the identity proofing process. Acceptable means include, but are not limited to: bot detection, mitigation, and management solutions; behavioral analytics; web application firewall settings; and traffic analysis.

5.5.2. Evidence and Core Attributes Collection Requirements

5.5.2.1. Evidence Collection

The CSP **SHALL** collect evidence from the applicant according to *one* of the following options:

1. Two pieces of SUPERIOR evidence, or
2. One piece of SUPERIOR evidence and one piece of STRONG evidence, or
3. Two pieces of STRONG evidence and one piece of FAIR evidence

5.5.2.2. Collection of Attributes

Validated evidence is the preferred source of identity attributes. If the presented identity evidence does not provide all the attributes the CSP considers core attributes, it **MAY** collect attributes that are self-asserted by the applicant.

5.5.3. Validation Requirements

5.5.3.1. Evidence Validation Requirements

The CSP **SHALL** validate the genuineness of each piece of SUPERIOR evidence by confirming the integrity of its cryptographic security features and validating any digital signatures.

The CSP **SHALL** validate the genuineness of each piece of STRONG evidence by *one* of the following:

1. Visual inspection by trained personnel
2. The use of technologies that can confirm the integrity of physical security features and detect if the evidence is fraudulent or has been inappropriately modified
3. If present, confirming the integrity of digital security features, including the validity of the issuer's digital signature

5.5.3.2. Core Attribute Validation Requirements

The CSP **SHALL** validate all core attributes by *both*:

1. Validating the accuracy of attributes obtained from pieces of evidence or applicant self-assertion by comparison with authoritative or credible sources
2. Validating the cryptographic features of any presented digital evidence, as described above

For added assurance, the CSP **SHALL** evaluate the core attributes, as validated by various sources, for overall consistency.

5.5.4. Identity Verification Requirements

The CSP **SHALL** verify the binding of the applicant to the claimed identity by *one* of the following:

1. Comparison of a collected biometric characteristic, such as a facial image, to the associated reference biometric characteristic contained on a piece of presented SUPERIOR or STRONG evidence
2. Demonstrated association with a digital account through, at a minimum, an AAL2 authentication or an AAL2 and FAL2 federation protocol

5.5.5. Notification of Proofing Requirement

Upon the successful completion of identity proofing at IAL3, the CSP **SHALL** send a notification of proofing to a validated address for the applicant, as specified in Sec. 5.1.7.

5.5.6. Biometric Collection

The CSP **SHALL** collect and record a biometric sample at the time of proofing (e.g., facial image, fingerprints) for the purposes of non-repudiation and re-proofing.

5.5.7. In-person Proofing Requirements

In-person proofing at IAL3 **SHALL** be conducted in *one* of two ways:

- An in-person interaction between the applicant and a CSP operator, or
- A remote interaction with the applicant, supervised by an operator, based on the requirements in Sec. 5.5.8, *IAL3 Supervised Remote Identity Proofing*.

Regardless of which of the two methods the CSP employs, the following requirements apply to identity proofing at IAL3:

1. The CSP **SHALL** have the operator view the biometric source (e.g., fingers, face) for the presence of any non-natural materials.
2. The CSP **SHALL** collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject.

5.5.8. Requirements for IAL3 Supervised Remote Identity Proofing

IAL3 Supervised Remote Identity Proofing is intended to achieve comparable levels of confidence and security to an in-person interaction with the applicant.

The following requirements apply to all IAL3 Supervised Remote Identity Proofing sessions:

1. The CSP **SHALL** monitor the entire identity proofing session, and **SHALL** ensure the applicant is continuously present during the entire identity proofing session — for example, by a continuous high-resolution video transmission of the applicant.

2. The CSP **SHALL** have a live operator participate remotely with the applicant for the entirety of the identity proofing session.
3. The CSP **SHALL** require all actions taken by the applicant during the identity proofing session to be clearly visible to the remote operator.
4. The CSP **SHALL** require that all digital verification of evidence (e.g., via chip or wireless technologies) be performed by integrated scanners and sensors (e.g., embedded fingerprint reader).
5. The CSP **SHALL** require operators to have undergone a training program to detect potential fraud and to properly perform a supervised remote proofing session.
6. The CSP **SHALL** employ physical tamper detection and resistance features appropriate for the environment in which it is located. For example, a kiosk located in a restricted area or one where it is monitored by a trusted individual requires less tamper detection than one that is located in a semi-public area such as a shopping mall concourse.
7. The CSP **SHALL** ensure that all communications occur over a mutually authenticated protected channel.

5.6. Summary of Requirements

Table 1 summarizes the requirements for each of the identity assurance levels:

Table 1. IAL Requirements Summary

Requirement	**IAL1**	**IAL2**	**IAL3**
Presence	Remote or In-person	Remote or In-person	In-person or Supervised Remote Identity Proofing
Resolution	Minimum attributes to accomplish resolution	Same as IAL1	Same as IAL1
Evidence	1 piece of SUPERIOR or 1 piece of STRONG plus 1 piece of FAIR	1 piece of SUPERIOR or 1 piece of STRONG plus 1 piece of FAIR	2 pieces of SUPERIOR or 1 piece of SUPERIOR plus 1 piece of STRONG or 2 pieces of STRONG plus 1 piece of FAIR
Validation	Evidence is validated for genuineness, accuracy, and currency. All core attributes are validated by authoritative or credible sources	Same as IAL1	Same as IAL1
Verification	Return of an enrollment code or Demonstrated access to a digital account at AAL1 or FAL1	Biometric comparison or Demonstrated access to a digital account at AAL2 or FAL2	Biometric comparison or Demonstrated access to a digital account at AAL2 or FAL2
Biometric Collection	Optional	Optional	Mandatory

6. Subscriber Accounts

This section is normative.

6.1. Subscriber Accounts

With the exception of identity proofing for the purposes of providing one-time access to an online service, or when an applicant declines enrollment into an account, the CSP **SHALL** enroll the applicant as a subscriber into its identity service and establish a unique *subscriber account* for that subscriber following the successful identity proofing of an applicant.

The CSP **SHALL** assign a unique identifier to each subscriber account.

At a minimum the CSP **SHALL** include the following information in each subscriber account:

- Unique identifier established for the subscriber
- A record of the identity proofing steps completed for the subscriber in accordance with Sec. 5.1.1
- Maximum IAL successfully achieved for the identity proofing of the subscriber
- Subscriber consent provided for the processing, retention, or disclosure of any personal or sensitive information maintained in the subscriber account
- All authenticators currently bound to the subscriber account, whether registered at enrollment or subsequent to enrollment
- All attributes that were validated during the identity proofing process or in subsequent transactions to support RP access

The CSP **SHALL** record information in the subscriber account that was collected during the identity proofing process or subsequently updated for each subscriber, including:

- Validated identity evidence
- Validated attribute information
- Attribute information that was collected for enrollment in the CSP identity service that was not validated for identity proofing purposes

The CSP **SHALL** perform a privacy risk assessment for the processing, retention, or disclosure of any personal information maintained in the subscriber account in accordance with Sec. 5.1.2.

6.2. Subscriber Account Access

In order to meet the requirement that accounts containing PII be protected by multi-factor authentication (MFA), the CSP **SHALL** provide a way for subscribers to access the information in their subscriber account through AAL2 or AAL3 authentication processes using authenticators registered to the subscriber account.

The CSP **SHALL** provide the capability for subscribers to change or update the personal information contained in their subscriber account.

6.3. Subscriber Account Lifecycle

6.3.1. Subscriber Account Activity

The CSP **SHALL** establish and maintain a unique subscriber account for each active subscriber in the CSP identity system from the time of enrollment to the time of account closure, as described below. Until the account is closed, the CSP **SHALL** provide for the use of the subscriber account, information contained in the account, and registered authenticators.

6.3.2. Subscriber Account Termination

The CSP **SHALL** terminate the subscriber account and discontinue its use when one of the following occur:

- The subscriber elects to terminate their subscriber account with the CSP.
- The CSP determines, following any due notice period and requirements established by the CSP, that the subscriber account has been compromised.
- The CSP determines, following any due notice period and requirements established by the CSP, that the subscriber has violated the policies or rules for participation in the CSP identity service.
- The CSP determines, following any due notice period and requirements established by the CSP, that the subscriber account is inactive in accordance with the policies or rules established by the CSP.
- The CSP ceases identity system and services operations.

The CSP **SHALL** delete any personal or sensitive information from the subscriber account records following account termination in accordance with the record retention and disposal requirements.

7. Threats and Security Considerations

This section is informative.

Effective protection of identity proofing processes requires the layering of security controls and processes throughout a transaction with a given applicant. To achieve this, it is necessary to understand where and how threats can arise and compromise enrollments. There are three general categories of threats to the identity proofing process:

- **Impersonation**: where an attacker attempts to pose as another, legitimate, individual (e.g., identity theft)
- **False or Fraudulent Representation**: where an attacker may create a false identity or false claims about an identity (e.g., synthetic identity fraud)
- **Infrastructure**: where attackers may seek to compromise confidentiality, availability, and integrity of the infrastructure, data, software, or people supporting the CSPs identity proofing process (e.g., distributed denial of service, insider threats)

This section focuses on impersonation and false or fraudulent representation threats, as infrastructure threats are addressed by traditional computer security controls (e.g., intrusion protection, record keeping, independent audits) and are outside the scope of this document. For more information on security controls, see [SP800-53], *Recommended Security and Privacy Controls for Federal Information Systems and Organizations*.

Table 2. Enrollment and Identity Proofing Threats

Attack/Threat	Description	Example
Automated Enrollment Attempts	Attackers leverage scripts and automated processes to rapidly generate large volumes of enrollments	Bots leverage stolen data to submit benefits claims.
Evidence Falsification	Attacker creates or modifies evidence in order claim an identity	A fake driver's license is used as evidence.
Synthetic Identity fraud	Attacker fabricates evidence of identity that is not associated with a real person	Opening a credit cards in a fake name to create a credit file.
Fraudulent Use of Identity (Identity Theft)	Attacker fraudulently uses another individuals identity or identity evidence	An individual uses a stolen passport.
Social Engineering	Attacker convinces a legitimate applicant to provide identity evidence or complete the identity proofing process under false pretenses	An individual submits their identity evidence to an attacker posing as a potential employer.
False Claims	Attacker associates false attributes or information with a legitimate identity	An individual claims benefits from a state in which they do not reside.

7.1. Threat Mitigation Strategies

Threats to the enrollment and identity proofing process are summarized in Table 2. Related mechanisms that assist in mitigating the threats identified above are summarized in Table 3. These mitigations should not be considered comprehensive but a summary of mitigations detailed more thoroughly at each Identity Assurance Level and applied based on the risk assessment processes detailed in [SP800-63] Sec. 5.

Table 3. Enrollment and Issuance Threat Mitigation Strategies

Threat/Attack	Mitigation Strategies	Normative Reference(s)
Automated Enrollment Attempts	CSP implements Web Application Firewall (WAF) controls and bot detection technology.CSP implements out-of-band engagement (e.g., enrollment codes). CSP implements biometric verification and liveness detection mechanism to determine genuine presence of an applicant. CSP implements traffic and network analysis capabilities to identify indications or malicious traffic	5.3.1, 5.4.1, 5.5.1
Evidence Falsification	CSP validates core attributes with authoritative or credible sources. CSP checks physical or digital security features of the presented evidence.	4.3, 5.3.2, 5.3.3, 5.4.2, 5.4.3, 5.5.2, 5.5.3
Synthetic Identity fraud	CSP collects multiple pieces of identity evidence to support the proofing process. CSP validates core attributes with authoritative or credible sources. CSP verifies identity through biometric comparison of the applicant to validated identity evidence or biometric data provided by an authoritative or credible source.	4.3, 4.3, 5.3.2, 5.3.3, 5.3.4, 5.4.2, 5.4.3, 5.4.4, 5.5.2, 5.5.3, 5.5.4
Fraudulent Use of Identity (Identity Theft)	CSP verifies identity through biometric comparison of the applicant to validated identity evidence or biometric data provide by an authoritative or credible source. CSP implements presentation attack detection measures to confirm the genuine presence of the individual to whom the identity evidence belongs. CSP implements out-of-band engagement (e.g., enrollment codes) and notice of proofing. CSP conducts checks of vital statistics repositories (e.g., Death Master File).CSP implements fraud, transaction, and behavioral analysis capabilities to identify indicators of potentially malicious account establishment.	5.1.1, 5.3.4, 5.4.4, 5.5.4
Social Engineering	CSP conducts training of Trusted Referees to identify indications of coercion or distress. CSP provides out-of-band engagement and notice of proofing to validated address. CSP provides information and communication to end users on common threats and schemes.	5.1.6, 5.1.7, 5.1.9
False Claims	CSP implements geographic restrictions on traffic. CSP validates core attributes and RP requested business attributes with authoritative or credible sources.	5.1.1, 5.3.2, 5.3.3, 5.4.2, 5.4.3, 5.5.2, 5.5.3

7.2. Collaboration with Adjacent Programs

Identity proofing services typically serve as the front door for critical business or service functions. Accordingly, these services should not operate in a vacuum. Close coordination of identity proofing and CSP functions with cybersecurity teams, threat intelligence teams, and program integrity teams can enable a more complete protection of business capabilities while constantly improving identity proofing capabilities.

For example, payment fraud data collected by program integrity teams could provide indicators of compromised subscriber accounts and potential weaknesses in identity proofing implementations. Similarly, threat intelligence teams may receive indications of new tactics, techniques, and procedures that may impact identity proofing processes.

CSPs and RPs should seek to establish consistent mechanisms for the exchange of information between critical security and fraud stakeholders. Where the CSP is external, this may be complicated, but should be considered in contractual and legal mechanisms. All data collected, transmitted, or shared should be minimized and subject to a detailed privacy and legal assessment.

8. Privacy Considerations

This section is informative.

These privacy considerations provide additional information in implementing the requirements set forth in Sec. 5.1.2.

8.1. Collection and Data Minimization

The guidelines permit the collection of only the PII necessary to validate the existence of the claimed identity and associate the claimed identity to the applicant, based on best available practices for appropriate identity resolution, validation, and verification. Collecting unnecessary PII can create confusion regarding why information not being used for the identity proofing service is being collected. This leads to invasiveness or overreach concerns, which can lead to loss of applicant trust. Further, PII retention can become vulnerable to unauthorized access or use. Data minimization reduces the amount of PII vulnerable to unauthorized access or use, and encourages trust in the identity proofing process.

8.1.1. Social Security Numbers

These guidelines permit the CSP collection of the SSN as an attribute for use in identity resolution. However, over-reliance on the SSN can contribute to misuse and place the applicant at risk of harm, such as through identity theft. Nonetheless, the SSN may facilitate identity resolution for CSPs, in particular federal agencies that use the SSN to correlate an applicant to agency records. This document recognizes the role of the SSN as an attribute and makes appropriate allowance for its use. Knowledge of the SSN is not sufficient to serve as identity evidence.

Where possible, CSPs and agencies should consider mechanisms to limit the proliferation and exposure of SSNs during the identity proofing process. This is particularly pertinent where the SSN is communicated to third party providers during attribute validation processes. To the extent possible, privacy protective techniques and technologies should be applied to reduce the risk of an individual's SSN being exposed, stored, or maintained by third party systems. Examples of this could be the use of attribute claims (e.g., yes/no responses from a validator) to confirm the validity of a SSN without requiring it to be unnecessarily transmitted and stored by the third party. As with all attributes in the identity proofing process, the value and risk of each attribute being processed is subject to a privacy risk assessment and for federal agencies the PIA and SORN. The SSN should only be collected where it is necessary to support resolution associated with the applications assurance and risk levels.

8.2. Notice and Consent

The guidelines require the CSP to provide explicit notice to the applicant at the time of collection regarding the purpose for collecting and maintaining a record of the attributes

necessary for identity proofing, including whether such attributes are voluntary or mandatory in order to complete the identity proofing transactions, and the consequences for not providing the attributes.

An effective notice will take into account user experience design standards and research, and an assessment of privacy risks that may arise from the collection. Various factors should be considered, including incorrectly inferring that applicants understand why attributes are collected, that collected information may be combined with other data sources, etc. An effective notice is never only a pointer leading to a complex, legalistic privacy policy or general terms and conditions that applicants are unlikely to read or understand.

8.3. Use Limitation

The guidelines require CSPs to use measures to maintain the objectives of predictability (enabling reliable assumptions by individuals, owners, and operators about PII and its processing by an information system) and manageability (providing the capability for granular administration of PII, including alteration, deletion, and selective disclosure) commensurate with privacy risks that can arise from the processing of attributes for purposes other than identity proofing, authentication, authorization, or attribute assertion, related fraud mitigation, or to comply with law or legal process [NISTIR8062].

CSPs may have various business purposes for processing attributes, including providing non-identity services to subscribers. However, processing attributes for other purposes than those disclosed to a subject can create additional privacy risks. CSPs can determine appropriate measures commensurate with the privacy risk arising from the additional processing. For example, absent applicable law, regulation or policy, it may not be necessary to get consent when processing attributes to provide non-identity services requested by subscribers, although notices may help subscribers maintain reliable assumptions about the processing (predictability). Other processing of attributes may carry different privacy risks that call for obtaining consent or allowing subscribers more control over the use or disclosure of specific attributes (manageability). Subscriber consent needs to be meaningful; therefore, when CSPs do use consent measures, they cannot make acceptance by the subscriber of additional uses a condition of providing the identity service.

Consult your SAOP if there are questions about whether the proposed processing falls outside the scope of the permitted processing or the appropriate privacy risk mitigation measures.

8.4. Redress

The guidelines require the CSP to provide effective mechanisms for redressing applicant complaints or problems arising from the identity proofing, and make the mechanisms easy

for applicants to find and access.

The Privacy Act requires federal CSPs that maintain a system of records to follow procedures to enable applicants to access and, if incorrect, amend their records. Any Privacy Act Statement should include a reference to the applicable SORN(s) (see Sec. 5.1.2), which provide the applicant with instructions on how to make a request for access or correction. Non-federal CSPs should have comparable procedures, including contact information for any third parties if they are the source of the information.

CSPs should make the availability of alternative methods for completing the process clear to applicants (e.g., in person at a customer service center) in the event an applicant is unable to establish their identity and complete the registration process online.

> Note: If the identity proofing process is not successful, CSPs should inform the applicant of the procedures to address the issue but should not inform the applicant of the specifics of why the registration failed (e.g., do not inform the applicant, "Your SSN did not match the one that we have on record for you"), as doing so could allow fraudulent applicants to gain more knowledge about the accuracy of the PII.

8.5. Privacy Risk Assessment

The guidelines require the CSP to conduct a privacy risk assessment. In conducting a privacy risk assessment, CSPs should consider:

1. The likelihood that the action it takes (e.g., additional verification steps or records retention) could create a problem for the applicant, such as invasiveness or unauthorized access to the information; and
2. The impact if a problem did occur. CSPs should be able to justify any response it takes to identified privacy risks, including accepting the risk, mitigating the risk, and sharing the risk. The use of applicant consent should be considered a form of sharing the risk, and therefore should only be used when an applicant could reasonably be expected to have the capacity to assess and accept the shared risk.

8.6. Agency-Specific Privacy Compliance

The guidelines cover specific compliance obligations for federal CSPs. It is critical to involve your agency's SAOP in the earliest stages of digital authentication system development to assess and mitigate privacy risks and advise the agency on compliance requirements, such as whether or not the PII collection to conduct identity proofing triggers the Privacy Act of 1974 [PrivacyAct] or the E-Government Act of 2002 [E-Gov] requirement to conduct a Privacy Impact Assessment. For example, with respect to identity proofing, it is likely that the Privacy Act requirements will be triggered and require coverage by either a new or existing Privacy Act system of records due to the

collection and maintenance of PII or other attributes necessary to conduct identity proofing.

The SAOP can similarly assist the agency in determining whether a PIA is required. These considerations should not be read as a requirement to develop a Privacy Act SORN or PIA for identity proofing alone; in many cases it will make the most sense to draft a PIA and SORN that encompasses the entire digital identity lifecycle or includes the identity proofing process as part of a larger, programmatic PIA that discusses the program or benefit to which the the agency is establishing online access.

Due to the many components of the digital identity lifecycle, it is important for the SAOP to have an awareness and understanding of each individual component. For example, other privacy artifacts may be applicable to an agency offering or using proofing services such as Data Use Agreements, Computer Matching Agreements, etc. The SAOP can assist the agency in determining what additional requirements apply. Moreover, a thorough understanding of the individual components of digital authentication will enable the SAOP to thoroughly assess and mitigate privacy risks either through compliance processes or by other means.

9. Usability Considerations

This section is informative.

Note: In this section, the term "users" means "applicants" or "subscribers."

This section is intended to raise implementers' awareness of the usability considerations associated with enrollment and identity proofing (for usability considerations for typical authenticator usage and intermittent events, see [SP800-63B] Sec. 10.

[ISO/IEC9241-11] defines usability as the "extent to which a system, product, or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use." This definition focuses on users, goals, and context of use as the necessary elements for achieving effectiveness, efficiency, and satisfaction. A holistic approach considering these key elements is necessary to achieve usability.

The overarching goal of usability for enrollment and identity proofing is to promote a smooth, positive enrollment process for users by minimizing user burden (e.g., time and frustration) and enrollment friction (e.g., the number of steps to complete and amount of information to track). To achieve this goal, organizations have to first familiarize themselves with their users.

The enrollment and identity proofing process sets the stage for a user's interactions with a given CSP and the online services that the user will access; as negative first impressions can influence user perception of subsequent interactions, organizations need to promote a positive user experience throughout the process.

Usability cannot be achieved in a piecemeal manner. Performing a usability evaluation on the enrollment and identity proofing process is critical. It is important to conduct usability evaluation with representative users, realistic goals and tasks, and appropriate contexts of use. The enrollment and identity proofing process should be designed and implemented so it is easy for users to do the right thing, hard to do the wrong thing, and easy to recover when the wrong thing happens.

From the user's perspective, the three main steps of enrollment and identity proofing are pre-enrollment preparation, the enrollment and proofing session, and post-enrollment actions. These steps may occur in a single session or there could be significant time elapsed between each one (e.g., days or weeks).

General and step-specific usability considerations are described in sub-sections below.

Guidelines and considerations are described from the users' perspective.

Accessibility differs from usability and is out of scope for this document. [Section508] was enacted to eliminate barriers in information technology and require federal agencies to make their electronic and information technology public content accessible to people with disabilities. Refer to Section 508 law and standards for accessibility guidance.

9.1. General User Considerations During Enrollment and Identity Proofing

This sub-section provides usability considerations that are applicable across all steps of the enrollment process. Usability considerations specific to each step are detailed in Secs. 9.2 to 9.4.

- To avoid user frustration, streamline the process required for enrollment to make each step as clear and easy as possible.
- Clearly communicate how and where to acquire technical assistance. For example, provide helpful information such as a link to online self-service feature, chat sessions, and a phone number for help desk support. Ideally, sufficient information should be provided to enable users to answer their own enrollment preparation questions without outside intervention.
- Clearly explain who is collecting their data and why. Also indicate the path their data will take, in particular where the data is being stored.
- Ensure all information presented is usable.
  - Follow good information design practice for all user-facing materials (e.g., data collection notices and fillable forms).
  - Write materials in plain language and avoid technical jargon. If appropriate, tailor language to the literacy level of the intended population. Use active voice and conversational style, logically sequence main points, use the same word consistently rather than synonyms to avoid confusion, and use bullets, numbers, and formatting where appropriate to aid readability.
  - Consider text legibility, such as font style, size, color, and contrast with surrounding background. The highest contrast is black on white. Text legibility is important because users have different levels of visual acuity. Illegible text will contribute to user comprehension errors or user entry errors (e.g., when completing fillable forms). Use sans serif font styles for electronic materials and serif fonts for paper materials. When possible, avoid fonts that do not clearly distinguish between easily confusable characters (such as the letter “O” and the number “0”). This is especially important for enrollment codes. Use a minimum font size of 12 points, as long as the text fits the display.
- Perform a usability evaluation for each step with representative users. Establish realistic goals and tasks, and appropriate contexts of use for the usability evaluation.

9.2. Pre-Enrollment Preparation

This section describes an effective approach to facilitate sufficient pre-enrollment preparation so users can avoid challenging, frustrating enrollment sessions. Ensuring

users are as prepared as possible for their enrollment sessions is critical to the overall success and usability of the enrollment and identity proofing process.

Such preparation is only possible if users receive the necessary information (e.g., required documentation) in a usable format in an appropriate timeframe. This includes making users aware of exactly what identity evidence will be required. Users do not need to know anything about IALs or whether the identity evidence required is scored as "fair," "strong," or "superior," whereas organizations need to know what IAL is required for access to a particular system.

To ensure users are equipped to make informed decisions about whether to proceed with the enrollment process, and what will be needed for their session, provide users:

- Information about the entire process, such as what to expect in each step.
  - Clear explanations of the expected timeframes to allow users to plan accordingly.
- Explanation of the need for — and benefits of — identity proofing to allow users to understand the value proposition.
- Information on the monetary amount and acceptable forms of payment, and if there is an enrollment fee. Offering a larger variety of acceptable forms of payment allows users to choose their preferred payment operation.
- Information on whether the user's enrollment session will be in-person or in-person over remote channels, and whether a user can choose. Only provide information relevant to the allowable session option(s).
  - Information on the location(s), whether a user can choose their preferred location, and necessary logistical information for in-person or in-person over remote channels session. Note that users may be reluctant to bring identity evidence to certain public places (bank versus supermarket), as it increases exposure to loss or theft.
  - Information on the technical requirements (e.g., requirements for internet access) for remote sessions.
  - An option to set an appointment for in-person or in-person over remote channels identity proofing sessions to minimize wait times. If walk-ins are allowed, make it clear to users that their wait times may be greater without an appointment.
    - Provide clear instructions for setting up an enrollment session appointment, reminders, and how to reschedule existing appointments.
    - Offer appointment reminders and allow users to specify their preferred appointment reminder format(s) (e.g., postal mail, voicemail, email, text message). Users need information such as date, time, location, and a description of required identity evidence.

- Information on the allowed and required identity evidence and attributes, whether each piece is voluntary or mandatory, and the consequences for not providing the complete set of identity evidence. Users need to know the specific combinations of identity evidence, including requirements specific to a piece of identity evidence (e.g., a raised seal on a birth certificate). This is especially important due to potential difficulties procuring the necessary identity evidence.
  - Where possible, implement tools to make it easier to obtain the necessary identity evidence.
  - Inform users of any special requirements for minors and people with unique needs. For example, provide users with the information on whether applicant reference and/or trusted referee processes are available and information necessary to use those processes (see Sec. 5.1.9).
  - If forms are required:
    * Provide fillable forms before and at the enrollment session. Do not require users to have access to a printer.
    * Minimize the amount of information users must enter on a form, as users are easily frustrated and more error-prone with longer forms. Where possible, pre-populate forms.

9.3. Enrollment and Proofing Session

Usability considerations specific to the enrollment session include:

- At the start of the identity proofing session, remind users of the procedure. Do not expect them to remember the procedures described during the pre-enrollment preparation step. If the enrollment session does not immediately follow pre-enrollment preparation, it is especially important to clearly remind users of the typical timeframe to complete the proofing and enrollment phase.
- Provide rescheduling options for in-person or in-person over remote channels.
- Provide a checklist with the allowed and required identity evidence to ensure users have the requisite identity evidence to proceed with the enrollment session, including enrollment codes, if applicable. If users do not have the complete set of identity evidence, they must be informed regarding whether they can complete a partial identity proofing session.
- Notify users regarding what information will be destroyed, what, if any, information will be retained for future follow-up sessions, and what identity evidence they will need to bring to complete a future session. Ideally, users can choose whether they would like to complete a partial identity proofing session.

- Set user expectations regarding the outcome of the enrollment session as prior identity verification experiences may drive their expectations (e.g., receiving a driver's license in person, receiving a passport in the mail).
- Clearly indicate whether users will receive an authenticator immediately at the end of a successful enrollment session, if users have to schedule an appointment to pick it up in person, or if users will receive it in the mail and when they can expect to receive it.
- During the enrollment session, there are several requirements to provide users with explicit notice at the time of identity proofing, such as what data will be retained on record by the CSP (see Sec. 5.1 and Sec. 8 for detailed requirements on notices). If CSPs seek consent from a user for additional attributes or uses of their attributes for any purpose other than identity proofing, authentication, authorization or attribute assertions, per 4.2 requirement (5), make CSPs aware that requesting additional attributes or uses may be unexpected or may make users uncomfortable. If users do not perceive benefit(s) to the additional collection or uses, but perceive extra risk, they may be unwilling or hesitant to provide consent or continue the process. Provide users with explicit notice of the additional requirements.
- If an enrollment code is issued:
  - Notify users in advance that they will receive an enrollment code, when to expect it, the length of time for which the code is valid, and how it will arrive (e.g., physical mail, SMS, landline telephone, email, or physical mailing address).
  - When an enrollment code is delivered to a user, include instructions on how to use the code, and the length of time for which the code is valid. This is especially important given the short validity timeframes specified in Sec. 5.1.6.
  - If issuing a machine-readable optical label, such as a QR Code (see Sec. 5.1.6), provide users with information on how to obtain QR code scanning capabilities (e.g., acceptable QR code applications).
  - Inform users that they will be required to repeat the enrollment process if enrollment codes expire or are lost before use.
  - Provide users with alternative options as not all users are able to access and use technology equitably. For example, users may not have the technology needed for this approach to be feasible.
- At the end of the enrollment session,
  - If enrollment is successful, send users confirmation regarding the successful enrollment and information on next steps (e.g., when and where to pick up their authenticator, when it will arrive in the mail).

  - If enrollment is partially complete (due to users not having the complete set of identity evidence, users choosing to stop the process, or session timeouts), communicate to users:
    * what information will be destroyed;
    * what, if any, information will be retained for future follow-up sessions;
    * how long the information will be retained; and
    * what identity evidence they will need to bring to a future session.
  - If enrollment is unsuccessful, provide users with clear instructions for alternative enrollment session types, for example, offering in-person proofing for users that can not complete remote proofing.
- If users receive the authenticator during the enrollment session, provide users information on the use and maintenance of the authenticator. For example, information could include instructions for use (especially if there are different requirements for first-time use or initialization), information on authenticator expiration, how to protect the authenticator, and what to do if the authenticator is lost or stolen.
- For both in-person and remote identity proofing, additional usability considerations apply:
  - At the start of the enrollment session, operators or attendants need to explain their role to users (e.g., whether operators or attendants will walk users through the enrollment session or observe silently and only interact as needed).
  - At the start of the enrollment session, inform users that they must not depart during the session, and that their actions must be visible throughout the session.
  - When biometrics are collected during the enrollment session, provide users clear instructions on how to complete the collection process. The instructions are best given just prior to the process. Verbal instructions with corrective feedback from a live operator are the most effective (e.g., instruct users where the biometric sensor is, when to start, how to interact with the sensor, and when the biometric collection is completed).
- Since remote identity proofing is conducted online, follow general web usability principles. For example:
  - Design the user interface to walk users through the enrollment process.
  - Reduce users' memory load.
  - Make the interface consistent.

1682 – Clearly label sequential steps.
1683 – Make the starting point clear.
1684 – Design to support multiple platforms and device sizes.
1685 – Make the navigation consistent, easy to find, and easy to follow.

1686 9.4. Post-Enrollment

1687 Post-enrollment refers to the step immediately after enrollment but prior to typical usage
1688 of an authenticator (for usability considerations for typical authenticator usage and
1689 intermittent events, see [SP800-63B], Sec. 10. As described above, users have already
1690 been informed at the end of their enrollment session regarding the expected delivery (or
1691 pick-up) mechanism by which they will receive their authenticator.

1692 Usability considerations for post-enrollment include:

1693 • Minimize the amount of time that users wait for their authenticator to arrive.
1694 Shorter wait times will allow users to access information systems and services
1695 more quickly.
1696 • Inform users whether they need to go to a physical location to pick up their
1697 authenticators. The previously identified usability considerations for appointments
1698 and reminders still apply.
1699 • Along with the authenticator, give users information relevant to the use and
1700 maintenance of the authenticator; this may include instructions for use, especially
1701 if there are different requirements for first-time use or initialization, information on
1702 authenticator expiration, and what to do if the authenticator is lost or stolen.

10. Equity Considerations

This section is informative.

This section is intended to provide guidance to CSPs for assessing the risks associated with inequitable access, treatment, or outcomes for individuals using its identity services, as required in Sec. 5.1.3. It provides a non-exhaustive list of potential areas in the identity proofing process that may be subject to inequities, as well as possible mitigations that can be applied. CSPs can use this section as a starting point for considering where the risks for inequitable access, treatment, or outcomes exist within its identity service. It is not intended that the below guidance be considered a definitive, all-inclusive list of associated equity risks to identity services.

In assessing equity risks, a CSP starts by considering the overall user population served by its identity proofing and enrollment service. Additionally, the CSP further identifies groups of users within the population whose shared characteristic(s) can cause them to be subject to inequitable access, treatment, or outcomes when using that service. CSPs are encouraged to assess the effectiveness of any mitigations by evaluating their impacts on the affected user group(s). The usability considerations provided in Sec. 9 should also be considered when applying equity risk mitigations to help improve the overall usability and equity for all persons using an identity service.

10.1. Equity and Identity Resolution

Identity resolution involves collecting the minimum set of attributes to be able to distinguish the claimed identity as a single, unique individual within the population served by the identity service. Attributes are obtained from presented identity evidence, applicant self-assertion, and/or back-end attribute providers.

This section provides a set of possible problems and mitigations with the inequitable access, treatment, or outcomes associated with the identity resolution process:

Description: The identity service design requires an applicant to enter their name using a Western name format (e.g., first name, last name, optional middle name).

Possible mitigations include:

1. Analyzing possible name configurations and determine how all names can be accurately accommodated using the name fields
2. Providing easy-to-find and use guidance to users on how to enter all names using the name fields

Description: The identity service cannot accommodate applicants whose name, gender, or other attributes have changed and are not consistently reflected on the presented identity evidence or match what is in the attribute verifier's records.

Possible mitigations include:

1. Providing Trusted Referees (Sec. 5.1.9.1) who can make risk-based decisions based on the specific applicant circumstances
2. Allowing for the use of Applicant References (Sec. 5.1.9.2) who can vouch for the difference in attributes

10.2. Equity and Identity Validation

Identity evidence and core attribute validation involves confirming the genuineness, currency, and accuracy of presented identity evidence and the accuracy of any additional attributes. These outcomes are accomplished by comparison of the evidence and attributes against data held by authoritative or credible sources. When considered together with the identity resolution phase, the result of successful validation phase is the confirmation, to some level of confidence, that the claimed identity exists in the real world.

This section provides a set of possible problems and mitigations with the inequitable access, treatment, or outcomes associated with the evidence and attribute validation process:

Description: Certain user groups do not possess the necessary minimum evidence to meet the requirements of a given IAL.

Possible mitigations include:

1. Providing Trusted Referees (Sec. 5.1.9.1) who can make risk-based decisions based on the specific applicant circumstances
2. Allowing for the use of Applicant References (Sec. 5.1.9.2) who can vouch for the applicant

Description: Records held by authoritative and credible sources (e.g., mobile network operators and phone number verifiers) are insufficient to support the validation of core attributes or presented evidence for applicants belonging to certain user groups.

Possible mitigations include:

1. Providing Trusted Referees (Sec. 5.1.9.1) who can make risk-based decisions based on the specific applicant circumstances
2. Employing alternative authoritative or credible sources

Description: Records held by authoritative and credible sources may include inaccurate or false information about persons who are the victims of identity fraud.

Possible mitigations include:

1. Providing Trusted Referees (Sec. 5.1.9.1) who can make risk-based decisions based on the specific applicant circumstances
2. Allowing for the use of Applicant References (Sec. 5.1.9.2) who can vouch for the difference in attributes

10.3. Equity and Identity Verification

Identity verification involves proving the binding between the applicant undergoing the identity proofing process and the validated, real-world identity established through the identity resolution and validation steps. It most often involves collecting a picture (facial image capture) of the applicant taken during the identity proofing event and comparing it a photograph contained on a presented and validated piece of identity evidence.

This section provides a set of possible problems and mitigations with the inequitable treatment or outcomes associated with the identity verification phase:

Description: Image capture technologies lack the ability to capture certain skin tones or facial features of sufficient quality to perform a comparison.

Possible mitigations include:

1. Employing robust image capture technologies that are able to accommodate different skin tones, facial features, and lighting situations
2. Conducting operational testing to determine if the image capture technologies have introduced unintentional biases
3. Providing risk-based alternative processes that compensate for residual bias and technological limitations

Description: Facial coverings worn for religious purposes impede the ability to capture a facial image of an applicant.

Possible mitigations include:

1. Providing Trusted Referees (Sec. 5.1.9.1) who can make risk-based decisions based on the specific applicant circumstances.
2. Providing alternative ways to accomplish identity verification, such as an in-person proofing.

Description: When using 1:1 facial image comparison technologies, biased facial comparison algorithms may result in false non-matches.

Possible mitigations include:

1. Using algorithms that are independently tested for consistent performance across demographic groups and image types
2. Supporting alternative processes to compensate for residual bias and technological limitations
3. Conducting ongoing quality monitoring and operational testing to identify performance variances are identified across demographic groups and implementing corrective actions as needed (e.g., updated algorithms, machine learning, etc.)

Description: When employing physical facial image comparison performed by CSP operators, human biases and inconsistencies in making facial comparisons may result in false non-matches.

Possible mitigations include:

1. Defining policy and procedures aimed at reducing/eliminating the inequitable treatment of applicants by CSP operators/agents
2. Rigorously training and certifying of operators
3. Conducting ongoing quality monitoring and taking corrective actions when biases, or inequitable treatments or outcomes, are identified

10.4. Equity and User Experience

The Usability Considerations section of this document (Sec. 9) provides CSPs with guidance on how to provide applicants with a smooth, positive identity proofing experience. In addition to the specific considerations provided in Sec. 9, this section provides CSPs with additional considerations when considering the equity of their user experience.

Description: Lack of access to needed technology (e.g. connected mobile device or computer), or difficulties in using required technologies, unduly burdens some user groups.

Possible mitigations include:

1. Allowing the use of helpers who assist applicants, who are otherwise able to meet the identity proofing requirements, in the use of the required technologies and activities
2. Allowing the use of publicly-available devices (e.g., computers or tablets) and providing online help resources for completing the identity proofing process on a non-applicant-owned computer or device
3. Providing in-person proofing options

Description: The remote or in-person identity proofing process presents challenges for persons with disabilities.

Possible mitigations for remote identity proofing include:

1. Providing Trusted Referees (Sec. 5.1.9.1) who are trained to communicate and assist people with a variety of needs or disabilities (e.g., fluent in sign language)
2. Allowing for the use of Applicant References (Sec. 5.1.9.2)
3. Supporting the use of accessibility and other technologies, such as audible instructions, screen readers and voice recognition technologies

Possible mitigations for in-person identity proofing include:

1. Providing trained operators who are trained to communicate and assist people with a variety of needs or disabilities (e.g., fluent in sign language)
2. Choosing equipment and workstations that can be adjusted to different heights and angles
3. Selecting locations that are convenient and comply with ADA accessibility guidelines

References

This section is informative.

General References

[A-130] OMB Circular A-130, *Managing Federal Information as a Strategic Resource*, July 28, 2016, available at: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

[COPPA] *Children's Online Privacy Protection Act of 1998 ("COPPA")*, 15 U.S.C. 6501-6505, 16 CFR Part 312, available at: https://www.law.cornell.edu/uscode/text/15/chapter-91.

[EO13985] Executive Order 13985, *Executive Order On Advancing Racial Equity and Support for Underserved Communities Through the Federal Government*, January 20, 2021, available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/20/executive-order-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government/.

[DMF] National Technical Information Service, *Social Security Death Master File*, available at: https://www.ssdmf.com/Library/InfoManage/Guide.asp?FolderID=1.

[E-Gov] *E-Government Act of 2002* (includes FISMA) (P.L. 107-347), December 2002, available at: https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.

[FBCACP] *X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)*, Version 2.30, October 5, 2016, available at: https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FBCA_CP.pdf.

[FBCASUP] *FBCA Supplementary Antecedent, In-Person Definition*, July 16, 2009.

[FEDRAMP] General Services Administration, *Federal Risk and Authorization Management Program*, available at: https://www.fedramp.gov/.

[GPG45] UK Cabinet Office, Good Practice Guide 45, *Identity proofing and verification of an individual*, December 3, 2014, available at: https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual.

[M-03-22] OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003, available at: https://georgewbush-whitehouse.archives.gov/omb/memoranda/m03-22.html.

[M-04-04] OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 16, 2003, available at: https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy04/m04-04.pdf.

[NISTIR8062] NIST Internal Report 8062, *An Introduction to Privacy Engineering and*

Risk Management in Federal Systems, January 2017, available at: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.

[NIST-Privacy] *NIST Privacy Framework*, available at: https://www.nist.gov/privacy-framework.

[NIST-RMF] *NIST Risk Management Framework*, available at: https://csrc.nist.gov/Projects/risk-management/about-rmf.

[PatriotAct] *Patriot Act of 2001*, available at: https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf.

[PrivacyAct] *Privacy Act of 1974* (P.L. 93-579), December 1974, available at: https://www.justice.gov/opcl/privacy-act-1974.

[RedFlagsRule] 15 U.S.C. 1681m(e)(4), Pub. L. 111-319, 124 Stat. 3457, *Fair and Accurate Credit Transaction Act of 2003*, December 18, 2010, available at: https://www.ftc.gov/sites/default/files/documents/federal_register_notices/identity-theft-red-flags-and-address-discrepancies-under-fair-and-accurate-credit-transactions-act/071109redflags.pdf.

[Section508] Section 508 Law and Related Laws and Policies (January 30, 2017), available at: https://www.section508.gov/manage/laws-and-policies/.

Standards

[Canada] Government of Canada, *Guideline on Identity Assurance*, available at: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678&section=HTML.

[ISO9241-11] International Standards Organization, ISO/IEC 9241-11 *Ergonomic requirements for office work with visual display terminals (VDTs) — Part 11: Guidance on usability*, March 1998, available at: https://www.iso.org/standard/16883.html.

[OIDC] Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, *OpenID Connect Core 1.0 incorporating errata set 1*, November, 2014. Available at: https://openid.net/specs/openid-connect-core-1_0.html.

NIST Special Publications

NIST 800 Series Special Publications are available at: < https://csrc.nist.gov/publications/sp800>. The following publications may be of particular interest to those implementing these guidelines.

[SP800-53] NIST Special Publication 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020 (includes updates as of Dec.

10, 2020), https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

[SP800-63] NIST Special Publication 800-63-4, *Digital Identity Guidelines*, November 2022, https://doi.org/10.6028/NIST.SP.800-63-4.ipd.

[SP800-63B] NIST Special Publication 800-63B-4, *Digital Identity Guidelines: Authentication and Lifecycle Management*, November 2022, https://doi.org/10.6028/NIST.SP.800-63b-4.ipd.

[SP800-63C] NIST Special Publication 800-63C-4, *Digital Identity Guidelines: Assertions and Federation*, November 2022, https://doi.org/10.6028/NIST.SP.800-63c-4.ipd.

[SP800-157] NIST Special Publication 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, December 2014, https://dx.doi.org/10.6028/NIST.SP.800-157.

Appendix A. Change Log

This appendix is informative.

This appendix provides a high-level overview of the changes to SP 800-63A since its initial release.

- Adds requirements for a new IAL1 for lower-risk applications
- Swaps the content in sections 4 and 5 to facilitate the introduction of identity proofing concepts before providing related requirements
- Provides guidance and requirements for characteristics of acceptable identity evidence, including physical documents and digital evidence
- Decouples the collection of identity attributes from the collection of identity evidence
- Introduces the concept of core attributes
- Expands acceptable evidence and attribute validation sources to include credible sources
- Adds requirements for CSP-specific privacy risk assessments and considerations for integrating the results into agency PIAs
- Adds new guidance and requirements for the consideration of equity risks associated with identity proofing processes
- Provides guidance and requirements for the use of Trusted Referees and Applicant References