



1

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

2

3

# Digital Identity Guidelines

4

Enrollment and Identity Proofing

5

Initial Public Draft

6

David Temoshok

7

Christine Abruzzi

8

Yee-Yin Choong

9

James L. Fenton

10

Ryan Galluzzo

11

Connie LaSalle

12

Naomi Lefkowitz

13

Andrew Regenscheid

14

This publication is available free of charge from:

15

<https://doi.org/10.6028/NIST.SP.800-63a-4.ipd>

16

17  
18  
19  
20  
21  
  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
  
38  
39  
40  
  
41  
42  
43  
  
44  
45

**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*

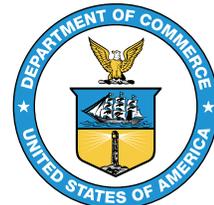
Andrew Regenscheid  
*Computer Security Division*  
*Information Technology Laboratory*

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*

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

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

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

## 61 **Authority**

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

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

## 77 **NIST Technical Series Policies**

78 [Copyright, Fair Use, and Licensing Statements](#)  
79 [NIST Technical Series Publication Identifier Syntax](#)

80 **Publication History**

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

83 **How to Cite this NIST Technical Series Publication**

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

88 **Author ORCID iDs**

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

97 **Public Comment Period**

98 December 16, 2022 - March 24, 2023

99 **Submit Comments**

100 <mailto:dig-comments@nist.gov>

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

## 103 **Reports on Computer Systems Technology**

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

## 115 **Abstract**

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

## 125 **Keywords**

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

## 128 **Note to Reviewers**

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

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

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

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

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

### 173 **Identity Proofing and Enrollment**

- 174 • NIST sees a need for inclusion of an unattended, fully remote Identity Assurance  
175 Level (IAL) 2 identity proofing workflow that provides security and convenience,  
176 but does not require face recognition. Accordingly, NIST seeks input on the  
177 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?

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

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

225 **Call for Patent Claims**

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

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

- 235 a) assurance in the form of a general disclaimer to the effect that such party does not  
236 hold and does not currently intend holding any essential patent claim(s); or
- 237 b) assurance that a license to such essential patent claim(s) will be made available  
238 to applicants desiring to utilize the license for the purpose of complying with the  
239 guidance or requirements in this ITL draft publication either:
  - 240 i. under reasonable terms and conditions that are demonstrably free of any unfair  
241 discrimination; or
  - 242 ii. without compensation and under reasonable terms and conditions that are  
243 demonstrably free of any unfair discrimination.

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

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

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

253	<b>Table of Contents</b>	
254	<b>1. Purpose</b>	2
255	<b>2. Introduction</b>	3
256	2.1. Expected Outcomes of Identity Proofing	4
257	2.2. Identity Assurance Levels	4
258	<b>3. Definitions and Abbreviations</b>	5
259	<b>4. Identity Resolution, Validation, and Verification</b>	6
260	4.1. Identity Proofing and Enrollment	6
261	4.1.1. Process Flow	8
262	4.2. Identity Resolution	9
263	4.3. Identity Validation and Identity Evidence Collection	9
264	4.3.1. Characteristics of Acceptable Physical Evidence	9
265	4.3.2. Characteristics of Acceptable Digital Evidence	10
266	4.3.3. Evidence Strength Requirements	10
267	4.3.4. Identity Evidence and Attribute Validation	12
268	4.4. Identity Verification	14
269	4.4.1. Identity Verification Methods	14
270	<b>5. Identity Assurance Level Requirements</b>	16
271	5.1. General Requirements	16
272	5.1.1. Identity Service Documentation and Records	16
273	5.1.2. General Privacy Requirements	17
274	5.1.3. General Equity Requirements	19
275	5.1.4. General Security Requirements	20
276	5.1.5. Additional Requirements for Federal Agencies	20
277	5.1.6. Requirements for Enrollment Codes	21
278	5.1.7. Requirements for Notifications of Identity Proofing	22
279	5.1.8. Requirements for Use of Biometrics	22
280	5.1.9. Trusted Referees and Applicant References	24
281	5.1.10. Requirements for Interacting with Minors	25
282	5.2. Identity Proofing Process	25

283	5.3. Identity Assurance Level 1 . . . . .	26
284	5.3.1. Automated Attack Prevention . . . . .	26
285	5.3.2. Evidence and Core Attributes Collection Requirements . . . . .	26
286	5.3.3. Evidence and Core Attributes Validation Requirements . . . . .	27
287	5.3.4. Identity Verification Requirements . . . . .	27
288	5.3.5. Notification of Proofing Requirement . . . . .	27
289	5.4. Identity Assurance Level 2 . . . . .	28
290	5.4.1. Automated Attack Prevention . . . . .	28
291	5.4.2. Evidence and Core Attribute Collection Requirements . . . . .	28
292	5.4.3. Evidence and Core Attributes Validation Requirements . . . . .	28
293	5.4.4. Identity Verification Requirements . . . . .	29
294	5.4.5. Notification of Proofing Requirement . . . . .	29
295	5.5. Identity Assurance Level 3 . . . . .	29
296	5.5.1. Automated Attack Prevention . . . . .	29
297	5.5.2. Evidence and Core Attributes Collection Requirements . . . . .	30
298	5.5.3. Validation Requirements . . . . .	30
299	5.5.4. Identity Verification Requirements . . . . .	31
300	5.5.5. Notification of Proofing Requirement . . . . .	31
301	5.5.6. Biometric Collection . . . . .	31
302	5.5.7. In-person Proofing Requirements . . . . .	31
303	5.5.8. Requirements for IAL3 Supervised Remote Identity Proofing . . . . .	31
304	5.6. Summary of Requirements . . . . .	32
305	<b>6. Subscriber Accounts . . . . .</b>	<b>34</b>
306	6.1. Subscriber Accounts . . . . .	34
307	6.2. Subscriber Account Access . . . . .	35
308	6.3. Subscriber Account Lifecycle . . . . .	35
309	6.3.1. Subscriber Account Activity . . . . .	35
310	6.3.2. Subscriber Account Termination . . . . .	35
311	<b>7. Threats and Security Considerations . . . . .</b>	<b>36</b>
312	7.1. Threat Mitigation Strategies . . . . .	37

313	7.2. Collaboration with Adjacent Programs . . . . .	39
314	<b>8. Privacy Considerations . . . . .</b>	<b>40</b>
315	8.1. Collection and Data Minimization . . . . .	40
316	8.1.1. Social Security Numbers . . . . .	40
317	8.2. Notice and Consent . . . . .	40
318	8.3. Use Limitation . . . . .	41
319	8.4. Redress . . . . .	41
320	8.5. Privacy Risk Assessment . . . . .	42
321	8.6. Agency-Specific Privacy Compliance . . . . .	42
322	<b>9. Usability Considerations . . . . .</b>	<b>44</b>
323	9.1. General User Considerations During Enrollment and Identity Proofing . . .	45
324	9.2. Pre-Enrollment Preparation . . . . .	45
325	9.3. Enrollment and Proofing Session . . . . .	47
326	9.4. Post-Enrollment . . . . .	50
327	<b>10. Equity Considerations . . . . .</b>	<b>51</b>
328	10.1. Equity and Identity Resolution . . . . .	51
329	10.2. Equity and Identity Validation . . . . .	52
330	10.3. Equity and Identity Verification . . . . .	53
331	10.4. Equity and User Experience . . . . .	54
332	<b>References . . . . .</b>	<b>56</b>
333	General References . . . . .	56
334	Standards . . . . .	57
335	NIST Special Publications . . . . .	57
336	<b>Appendix A. Change Log . . . . .</b>	<b>59</b>
337	<b>List of Tables</b>	
338	1. IAL Requirements Summary . . . . .	33
339	2. Enrollment and Identity Proofing Threats . . . . .	37
340	3. Enrollment and Issuance Threat Mitigation Strategies . . . . .	38

341 **List of Figures**

342 1. Identity Proofing Process . . . . . 8

343 **Acknowledgments**

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

352 **1. Purpose**

353 *This section is informative.*

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

357 This document provides requirements for the identity proofing of individuals at each  
358 Identity Assurance Level (IAL) for the purposes of enrolling them into an identity  
359 service or providing them access to online resources. It applies to the identity proofing of  
360 individuals over a network or in person. Verifying the identities of people calling into a  
361 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*

## 393 2.1. Expected Outcomes of Identity Proofing

394 The expected outcomes of identity proofing include:

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

## 404 2.2. Identity Assurance Levels

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

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

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

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

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

422 **3. Definitions and Abbreviations**

423 *This section is informative*

424 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 an 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:

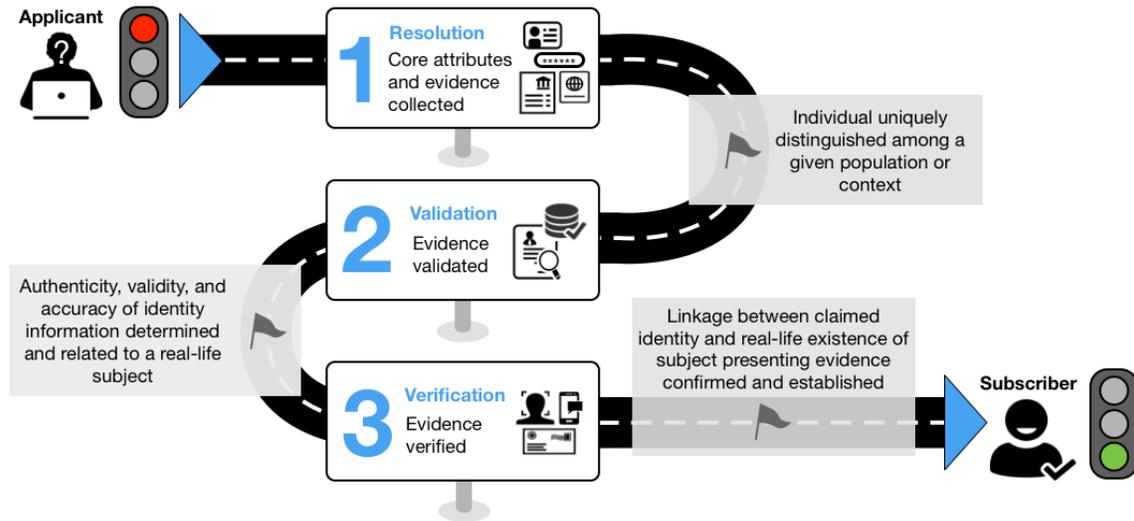
1. Full name
2. Date of birth
3. Home address

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

464 **4.1.1. Process Flow**

465 *This section is informative.*

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



**Figure 1.** Identity Proofing Process

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

469 **1. Resolution**

- 470 a) The CSP collects attributes from the applicant, such as name, address, date of  
471 birth, email, and phone number.
- 472 b) The CSP also collects one or more pieces of identity evidence, such as a  
473 driver's license or a passport.

474 **2. Validation**

- 475 a) The CSP validates the attributes obtained in steps 1a by checking them against  
476 authoritative or credible sources.
- 477 b) The CSP validates the authenticity, accuracy, and currency of the presented  
478 evidence.

479 **3. Verification**

- 480 a) The CSP asks the applicant to take a photo of themselves, with **liveness checks**.
- 481 b) The CSP compares the pictures on the license and the passport to the photo of  
482 the live applicant's photo from the previous step and determines they match.

- 483 c) The CSP sends an enrollment code to the validated phone number of the  
484 applicant, the applicant provides the enrollment code to the CSP, and the CSP  
485 confirms they match, verifying they the applicant is in possession and control  
486 of the validated phone number.
- 487 d) The applicant has been successfully identity proofed and can be enrolled into  
488 a subscriber account.

## 489 4.2. Identity Resolution

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

## 495 4.3. Identity Validation and Identity Evidence Collection

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

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

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

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

### 515 4.3.1. Characteristics of Acceptable Physical Evidence

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

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

#### 526 4.3.2. Characteristics of Acceptable Digital Evidence

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

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

#### 542 4.3.3. Evidence Strength Requirements

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

548 **4.3.3.1. Fair Evidence Requirements**

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

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

560 **4.3.3.2. Strong Evidence Requirements**

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

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

#### 579 **4.3.3.3. Superior Evidence Requirements**

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

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

#### 598 **4.3.4. Identity Evidence and Attribute Validation**

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

##### 601 **4.3.4.1. Evidence Validation**

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

- 604 • Confirming the evidence is in the correct format and includes complete information  
605 for the identity evidence type.
- 606 • Confirming the evidence is not counterfeit and that it has not been tampered with.
- 607 • Confirming any security features.

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

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

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

#### 616 **4.3.4.2. Attribute Validation**

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

#### 620 **4.3.4.3. Evidence and Attribute Validation Methods**

621 Acceptable methods for validating presented evidence include:

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

#### 629 **4.3.4.4. Validation Sources**

630 Core attributes that are contained on identity evidence that has been validated according  
631 to [Sec. 4.3.4.1](#) can be considered validated, in which case no further validation is  
632 required.

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

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

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

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

#### 655 **4.4. Identity Verification**

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

##### 659 **4.4.1. Identity Verification Methods**

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

- 663 • **Enrollment code verification** as specified in [Sec. 5.1.6](#).
- 664 • **In-person physical comparison.** The CSP operator and applicant interact in person  
665 for the identity proofing event. The CSP operator performs a physical comparison  
666 of the facial portrait presented on identity evidence to the face of the applicant  
667 engaged in the identity proofing event.
- 668 • **Remote (attended and unattended) physical facial image comparison.** The CSP  
669 operator performs a physical comparison of the facial portrait presented on identity  
670 evidence to the facial image of the applicant engaged in the identity proofing event.  
671 The CSP operator may interact directly with the applicant during some or all of the  
672 identity proofing event (attended) or may conduct the comparison at a later time  
673 (unattended) using a captured video or photograph and the uploaded copy of the  
674 evidence. If the comparison is performed at a later time, steps are taken to ensure  
675 the captured video or photograph was taken from the live applicant present during  
676 the identity proofing event.
- 677 • **Automated biometric comparison.** Biometric system comparison may be  
678 performed for in-person or remote identity proofing events. The facial portrait,  
679 or other biometric characteristic, contained on identity evidence is compared by  
680 an automated biometric comparison system to the facial image photograph of the  
681 live applicant or other biometric live sample submitted by the applicant during  
682 the identity proofing event. The automated biometric comparison system uses a  
683 mathematical algorithm for the comparison.

- 684 • **Control of a digital account.** An individual is able to demonstrate control of  
685 a digital account (e.g., online bank account) or signed digital assertion (e.g.,  
686 verifiable credentials) through the use of authentication or federation protocols.  
687 This may be done in person through presentation of the credential to a device or  
688 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<sup>1</sup>;
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);

---

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

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

#### 724 5.1.1.1. Ceasing Operations

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

#### 732 5.1.1.2. Fraud Mitigation Measures

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

#### 743 5.1.2. General Privacy Requirements

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

#### 746 5.1.2.1. Privacy Risk Assessment

- 747 1. The CSP **SHALL** conduct and document a privacy risk assessment for the  
748 processes used for identity proofing and enrollment.<sup>2</sup> At a minimum, the privacy  
749 risk assessment **SHALL** assess the risks associated with:
- 750 a) Any processing of PII for the purpose of identity proofing and enrollment,  
751 including identity attributes, biometrics, images, video, scans, or copies of  
752 identity evidence;

---

<sup>2</sup>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 diligence.

#### 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.

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

### 793 **5.1.3. General Equity Requirements**

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

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

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

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

#### 822 **5.1.4. General Security Requirements**

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

#### 831 **5.1.5. Additional Requirements for Federal Agencies**

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

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

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

#### 863 5.1.6. Requirements for Enrollment Codes

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

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

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

### 888 **5.1.7. Requirements for Notifications of Identity Proofing**

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

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

894 Notifications of proofing:

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

### 905 **5.1.8. Requirements for Use of Biometrics**

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

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

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

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

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

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

### 959 **5.1.9. Trusted Referees and Applicant References**

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

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

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

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

#### 993 **5.1.9.1. Requirements for Trusted Referees**

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

996 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;

- 1029 • An in-person, physical interaction with the applicant process; and
- 1030 • An IAL3 Supervised Remote Identity Proofing process.

1031 Identity proofing at IAL1 and IAL2 allow for any of the these processes to be used, while  
1032 IAL3 requires in-person, physical interaction with the applicant or IAL3 Supervised  
1033 Remote Identity Proofing.

1034 The following sections provide requirements for identity proofing at each IAL.

### 1035 **5.3. Identity Assurance Level 1**

1036 IAL1 permits both remote and in-person identity proofing. Identity proofing processes  
1037 at IAL1 allow for a range of acceptable techniques in order to detect the presentation of  
1038 fraudulent identities by a malicious actor while facilitating user adoption and minimizing  
1039 false negatives and application departures (legitimate applicants who do not successfully  
1040 complete identity proofing). Notably, the use of biometric matching, such as the  
1041 automated comparison of a facial portrait to supplied evidence, at IAL1 is optional,  
1042 providing pathways to proofing and enrollment where such collection may not be viable  
1043 or where privacy and equity risks outweigh security considerations.

1044 The following requirements apply to all CSPs providing identity proofing and enrollment  
1045 services at IAL1.

#### 1046 **5.3.1. Automated Attack Prevention**

1047 The CSP **SHALL** implement a means to prevent automated attacks on the identity  
1048 proofing process. Acceptable means include, but are not limited to: bot detection,  
1049 mitigation, and management solutions; behavioral analytics; web application firewall  
1050 settings; and traffic analysis.

#### 1051 **5.3.2. Evidence and Core Attributes Collection Requirements**

##### 1052 **5.3.2.1. Evidence Collection**

1053 For remote or in-person identity proofing, the CSP **SHALL** collect *one* of the following  
1054 from the applicant:

- 1055 1. One piece of SUPERIOR evidence, or
- 1056 2. One piece of STRONG evidence and one piece of FAIR evidence

##### 1057 **5.3.2.2. Collection of Additional Attributes**

1058 Validated evidence is the preferred source of identity attributes. If the presented identity  
1059 evidence does not provide all the attributes the CSP considers core attributes, **it MAY**  
1060 collect attributes that are self-asserted by the applicant.

1061 **5.3.3. Evidence and Core Attributes Validation Requirements**

1062 The CSP **SHALL** validate the genuineness of each piece of SUPERIOR and STRONG  
1063 evidence by *one* of the following:

- 1064 1. Visual inspection by trained personnel
- 1065 2. The use of technologies that can confirm the integrity of physical security features  
1066 or detect if the evidence is fraudulent or has been inappropriately modified
- 1067 3. If present, confirming the integrity of digital security features

1068 The CSP **SHALL** validate the genuineness of each piece of FAIR evidence by visual  
1069 inspection by trained personnel.

1070 The CSP **SHALL** validate all core attributes by *both*:

- 1071 1. Validating the accuracy of attributes (such as account or reference number,  
1072 name, and date of birth) obtained from pieces of evidence by comparison with  
1073 authoritative or credible sources, and
- 1074 2. Validating the accuracy of self-asserted attributes by comparison with authoritative  
1075 or credible sources.

1076 For added assurance, the CSP **SHALL** evaluate the core attributes, as validated by various  
1077 sources, for overall consistency.

1078 **5.3.4. Identity Verification Requirements**

1079 The CSP **SHALL** verify the binding of the applicant to the claimed identity by *one* of the  
1080 following:

- 1081 1. Physical comparison of the applicant's face or biometric comparison of the facial  
1082 image of the applicant to the facial portrait included on a piece of SUPERIOR or  
1083 STRONG evidence, or
- 1084 2. Demonstrated association with a digital account through an AAL1 authentication or  
1085 an AAL1 and FAL1 federation protocol, or
- 1086 3. Verification of the applicant's return of a valid enrollment code [Sec. 5.1.6](#)

1087 **5.3.5. Notification of Proofing Requirement**

1088 Upon the successful completion of identity proofing at IAL1, the CSP **SHOULD** send a  
1089 notification of proofing to a validated address for the applicant, as specified in [Sec. 5.1.7](#).

1090 **5.4. Identity Assurance Level 2**

1091 Like IAL1, IAL2 identity proofing allows for both remote and in-person identity proofing  
1092 processes in order to maximize accessibility while still mitigating against impersonation  
1093 attacks and other identity proofing errors. Remote IAL2 identity proofing can be  
1094 accomplished by the CSP via a fully automated process, a CSP operator attended process,  
1095 or a combination of the two.

1096 **5.4.1. Automated Attack Prevention**

1097 The CSP **SHALL** implement a means to prevent automated attacks on the identity  
1098 proofing process. Acceptable means include, but are not limited to: bot detection,  
1099 mitigation, and management solutions; behavioral analytics; web application firewall  
1100 settings; and traffic analysis.

1101 **5.4.2. Evidence and Core Attribute Collection Requirements**

1102 **5.4.2.1. Evidence Collection**

1103 For remote or in-person identity proofing, the CSP **SHALL** collect *one* of the following  
1104 from the applicant:

- 1105 1. One piece of SUPERIOR evidence
- 1106 2. One piece of STRONG evidence and one piece of FAIR evidence

1107 **5.4.2.2. Collection of Attributes**

1108 Validated evidence is the preferred source of identity attributes. If the presented identity  
1109 evidence does not provide all the attributes, the CSP considers core attributes, it **MAY**  
1110 collect attributes that are self-asserted by the applicant.

1111 **5.4.3. Evidence and Core Attributes Validation Requirements**

1112 The CSP **SHALL** validate the genuineness of each piece of SUPERIOR and STRONG  
1113 evidence by one of the following:

- 1114 1. Visual inspection by trained personnel
- 1115 2. The use of technologies that can confirm the integrity of physical security features  
1116 or detect if the evidence is fraudulent or has been inappropriately modified
- 1117 3. If present, confirming the integrity of digital security features

1118 The CSP **SHALL** validate all core attributes by:

- 1119 1. Validating the accuracy of attributes (such as account or reference number,  
1120 name, and date of birth) obtained from pieces of evidence by comparison with  
1121 authoritative or credible sources, and

- 1122 2. validating the accuracy of self-asserted attributes by comparison with authoritative  
1123 or credible sources

1124 For added assurance, the CSP **SHALL** evaluate the core attributes, as validated by various  
1125 sources, for overall consistency.

#### 1126 **5.4.4. Identity Verification Requirements**

##### 1127 **5.4.4.1. Remote Identity Proofing**

1128 The CSP **SHALL** verify the binding of the applicant to the claimed identity by *one* of the  
1129 following:

- 1130 1. Comparison of a collected biometric characteristic, such as a facial image, to the  
1131 associated reference biometric contained on a piece of presented SUPERIOR or  
1132 STRONG evidence
- 1133 2. Demonstrated association with a digital account through an AAL2 authentication or  
1134 an AAL2 and FAL2 federation protocol

##### 1135 **5.4.4.2. In-person Identity Proofing**

1136 The CSP **SHALL** verify the binding of the applicant to the claimed identity by physical or  
1137 biometric comparison of the facial image of the applicant to the facial portrait contained  
1138 on a piece of presented SUPERIOR or STRONG evidence.

##### 1139 **5.4.5. Notification of Proofing Requirement**

1140 Upon the successful completion of identity proofing at IAL2, the CSP **SHALL** send a  
1141 notification of proofing to a validated address for the applicant, as specified in [Sec. 5.1.7](#).

#### 1142 **5.5. Identity Assurance Level 3**

1143 IAL3 adds additional rigor to the steps required at IAL2 and is subject to additional and  
1144 specific processes (including the use of biometric information comparison, collection,  
1145 and retention) to further protect the identity and RP from impersonation, fraud, or other  
1146 significantly harmful damages. In addition, identity proofing at IAL3 is performed in  
1147 person (to include supervised remote identity proofing defined in [Sec. 5.5.8](#)).

##### 1148 **5.5.1. Automated Attack Prevention**

1149 The CSP **SHALL** implement a means to prevent automated attacks on the identity  
1150 proofing process. Acceptable means include, but are not limited to: bot detection,  
1151 mitigation, and management solutions; behavioral analytics; web application firewall  
1152 settings; and traffic analysis.

1153 **5.5.2. Evidence and Core Attributes Collection Requirements**

1154 **5.5.2.1. Evidence Collection**

1155 The CSP **SHALL** collect evidence from the applicant according to *one* of the following  
1156 options:

- 1157 1. Two pieces of SUPERIOR evidence, or
- 1158 2. One piece of SUPERIOR evidence and one piece of STRONG evidence, or
- 1159 3. Two pieces of STRONG evidence and one piece of FAIR evidence

1160 **5.5.2.2. Collection of Attributes**

1161 Validated evidence is the preferred source of identity attributes. If the presented identity  
1162 evidence does not provide all the attributes the CSP considers core attributes, it **MAY**  
1163 collect attributes that are self-asserted by the applicant.

1164 **5.5.3. Validation Requirements**

1165 **5.5.3.1. Evidence Validation Requirements**

1166 The CSP **SHALL** validate the genuineness of each piece of SUPERIOR evidence by  
1167 confirming the integrity of its cryptographic security features and validating any digital  
1168 signatures.

1169 The CSP **SHALL** validate the genuineness of each piece of STRONG evidence by *one* of  
1170 the following:

- 1171 1. Visual inspection by trained personnel
- 1172 2. The use of technologies that can confirm the integrity of physical security features  
1173 and detect if the evidence is fraudulent or has been inappropriately modified
- 1174 3. If present, confirming the integrity of digital security features, including the validity  
1175 of the issuer's digital signature

1176 **5.5.3.2. Core Attribute Validation Requirements**

1177 The CSP **SHALL** validate all core attributes by *both*:

- 1178 1. Validating the accuracy of attributes obtained from pieces of evidence or applicant  
1179 self-assertion by comparison with authoritative or credible sources
- 1180 2. Validating the cryptographic features of any presented digital evidence, as described  
1181 above

1182 For added assurance, the CSP **SHALL** evaluate the core attributes, as validated by various  
1183 sources, for overall consistency.

1184 **5.5.4. Identity Verification Requirements**

1185 The CSP **SHALL** verify the binding of the applicant to the claimed identity by *one* of the  
1186 following:

- 1187 1. Comparison of a collected biometric characteristic, such as a facial image, to the  
1188 associated reference biometric characteristic contained on a piece of presented  
1189 SUPERIOR or STRONG evidence
- 1190 2. Demonstrated association with a digital account through, at a minimum, an AAL2  
1191 authentication or an AAL2 and FAL2 federation protocol

1192 **5.5.5. Notification of Proofing Requirement**

1193 Upon the successful completion of identity proofing at IAL3, the CSP **SHALL** send a  
1194 notification of proofing to a validated address for the applicant, as specified in [Sec. 5.1.7](#).

1195 **5.5.6. Biometric Collection**

1196 The CSP **SHALL** collect and record a biometric sample at the time of proofing (e.g.,  
1197 facial image, fingerprints) for the purposes of non-repudiation and re-proofing.

1198 **5.5.7. In-person Proofing Requirements**

1199 In-person proofing at IAL3 **SHALL** be conducted in *one* of two ways:

- 1200 • An in-person interaction between the applicant and a CSP operator, or
- 1201 • A remote interaction with the applicant, supervised by an **operator**, based on the  
1202 requirements in [Sec. 5.5.8, IAL3 Supervised Remote Identity Proofing](#).

1203 Regardless of which of the two methods the CSP employs, the following requirements  
1204 apply to identity proofing at IAL3:

- 1205 1. The CSP **SHALL** have the operator view the biometric source (e.g., fingers, face)  
1206 for the presence of any non-natural materials.
- 1207 2. The CSP **SHALL** collect biometrics in such a way that ensures that the biometric is  
1208 collected from the applicant, and not another subject.

1209 **5.5.8. Requirements for IAL3 Supervised Remote Identity Proofing**

1210 IAL3 Supervised Remote Identity Proofing is intended to achieve comparable levels of  
1211 confidence and security to an in-person interaction with the applicant.

1212 The following requirements apply to all IAL3 Supervised Remote Identity Proofing  
1213 sessions:

- 1214 1. The CSP **SHALL** monitor the entire identity proofing session, and **SHALL** ensure  
1215 the applicant is continuously present during the entire identity proofing session —  
1216 for example, by a continuous high-resolution video transmission of the applicant.

- 1217 2. The CSP **SHALL** have a live operator participate remotely with the applicant for  
1218 the entirety of the identity proofing session.
- 1219 3. The CSP **SHALL** require all actions taken by the applicant during the identity  
1220 proofing session to be clearly visible to the remote operator.
- 1221 4. The CSP **SHALL** require that all digital verification of evidence (e.g., via chip  
1222 or wireless technologies) be performed by integrated scanners and sensors (e.g.,  
1223 embedded fingerprint reader).
- 1224 5. The CSP **SHALL** require operators to have undergone a training program to detect  
1225 potential fraud and to properly perform a supervised remote proofing session.
- 1226 6. The CSP **SHALL** employ physical tamper detection and resistance features  
1227 appropriate for the environment in which it is located. For example, a kiosk located  
1228 in a restricted area or one where it is monitored by a trusted individual requires less  
1229 tamper detection than one that is located in a semi-public area such as a shopping  
1230 mall concourse.
- 1231 7. The CSP **SHALL** ensure that all communications occur over a mutually  
1232 authenticated protected channel.

## 1233 **5.6. Summary of Requirements**

1234 **Table 1** summarizes the requirements for each of the identity assurance levels:

**Table 1.** IAL Requirements Summary

<b>Requirement</b>	<b>IAL1</b>	<b>IAL2</b>	<b>IAL3</b>
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

1235 **6. Subscriber Accounts**

1236 *This section is normative.*

1237 **6.1. Subscriber Accounts**

1238 With the exception of identity proofing for the purposes of providing one-time access  
1239 to an online service, or when an applicant declines enrollment into an account, the CSP  
1240 **SHALL** enroll the applicant as a subscriber into its identity service and establish a unique  
1241 *subscriber account* for that subscriber following the successful identity proofing of an  
1242 applicant.

1243 The CSP **SHALL** assign a unique identifier to each subscriber account.

1244 At a minimum the CSP **SHALL** include the following information in each subscriber  
1245 account:

- 1246 • Unique identifier established for the subscriber
- 1247 • A record of the identity proofing steps completed for the subscriber in accordance  
1248 with [Sec. 5.1.1](#)
- 1249 • Maximum IAL successfully achieved for the identity proofing of the subscriber
- 1250 • Subscriber consent provided for the processing, retention, or disclosure of any  
1251 personal or sensitive information maintained in the subscriber account
- 1252 • All authenticators currently bound to the subscriber account, whether registered at  
1253 enrollment or subsequent to enrollment
- 1254 • All attributes that were validated during the identity proofing process or in  
1255 subsequent transactions to support RP access

1256 The CSP **SHALL** record information in the subscriber account that was collected during  
1257 the identity proofing process or subsequently updated for each subscriber, including:

- 1258 • Validated identity evidence
- 1259 • Validated attribute information
- 1260 • Attribute information that was collected for enrollment in the CSP identity service  
1261 that was not validated for identity proofing purposes

1262 The CSP **SHALL** perform a privacy risk assessment for the processing, retention, or  
1263 disclosure of any personal information maintained in the subscriber account in accordance  
1264 with [Sec. 5.1.2](#).

1265 **6.2. Subscriber Account Access**

1266 In order to meet the requirement that accounts containing PII be protected by multi-  
1267 factor authentication (MFA), the CSP **SHALL** provide a way for subscribers to access the  
1268 information in their subscriber account through AAL2 or AAL3 authentication processes  
1269 using authenticators registered to the subscriber account.

1270 The CSP **SHALL** provide the capability for subscribers to change or update the personal  
1271 information contained in their subscriber account.

1272 **6.3. Subscriber Account Lifecycle**

1273 **6.3.1. Subscriber Account Activity**

1274 The CSP **SHALL** establish and maintain a unique subscriber account for each active  
1275 subscriber in the CSP identity system from the time of enrollment to the time of account  
1276 closure, as described below. **Until the account is closed, the CSP SHALL provide for**  
1277 **the use of the subscriber account, information contained in the account, and registered**  
1278 **authenticators.**

1279 **6.3.2. Subscriber Account Termination**

1280 The CSP **SHALL** terminate the subscriber account and discontinue its use when one of  
1281 the following occur:

- 1282 • The subscriber elects to terminate their subscriber account with the CSP.
- 1283 • The CSP determines, following any due notice period and requirements established  
1284 by the CSP, that the subscriber account has been compromised.
- 1285 • The CSP determines, following any due notice period and requirements established  
1286 by the CSP, that the subscriber has violated the policies or rules for participation in  
1287 the CSP identity service.
- 1288 • The CSP determines, following any due notice period and requirements established  
1289 by the CSP, that the subscriber account is inactive in accordance with the policies or  
1290 rules established by the CSP.
- 1291 • The CSP ceases identity system and services operations.

1292 The CSP **SHALL** delete any personal or sensitive information from the subscriber  
1293 account records following account termination in accordance with **the record retention**  
1294 **and disposal requirements.**

1295 **7. Threats and Security Considerations**

1296 *This section is informative.*

1297 Effective protection of identity proofing processes requires the layering of security  
1298 controls and processes throughout a transaction with a given applicant. To achieve this, it  
1299 is necessary to understand where and how threats can arise and compromise enrollments.  
1300 There are three general categories of threats to the identity proofing process:

- 1301 • **Impersonation:** where an attacker attempts to pose as another, legitimate,  
1302 individual (e.g., identity theft)
- 1303 • **False or Fraudulent Representation:** where an attacker may create a false identity  
1304 or false claims about an identity (e.g., synthetic identity fraud)
- 1305 • **Infrastructure:** where attackers may seek to compromise confidentiality,  
1306 availability, and integrity of the infrastructure, data, software, or people supporting  
1307 the CSPs identity proofing process (e.g., distributed denial of service, insider  
1308 threats)

1309 This section focuses on impersonation and false or fraudulent representation threats,  
1310 as infrastructure threats are addressed by traditional computer security controls (e.g.,  
1311 intrusion protection, record keeping, independent audits) and are outside the scope of this  
1312 document. For more information on security controls, see [SP800-53], *Recommended*  
1313 *Security and Privacy Controls for Federal Information Systems and Organizations.*

**Table 2.** Enrollment and Identity Proofing Threats

<b>Attack/Threat</b>	<b>Description</b>	<b>Example</b>
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.

1314 **7.1. Threat Mitigation Strategies**

1315 Threats to the enrollment and identity proofing process are summarized in [Table 2](#).  
 1316 Related mechanisms that assist in mitigating the threats identified above are summarized  
 1317 in [Table 3](#). These mitigations should not be considered comprehensive but a summary of  
 1318 mitigations detailed more thoroughly at each Identity Assurance Level and applied based  
 1319 on the risk assessment processes detailed in [\[SP800-63\] Sec. 5](#).

**Table 3.** Enrollment and Issuance Threat Mitigation Strategies

<b>Threat/Attack</b>	<b>Mitigation Strategies</b>	<b>Normative Reference(s)</b>
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

1320 **7.2. Collaboration with Adjacent Programs**

1321 Identity proofing services typically serve as the front door for critical business or  
1322 service functions. Accordingly, these services should not operate in a vacuum. Close  
1323 coordination of identity proofing and CSP functions with cybersecurity teams, threat  
1324 intelligence teams, and program integrity teams can enable a more complete protection  
1325 of business capabilities while constantly improving identity proofing capabilities.  
1326 For example, payment fraud data collected by program integrity teams could provide  
1327 indicators of compromised subscriber accounts and potential weaknesses in identity  
1328 proofing implementations. Similarly, threat intelligence teams may receive indications of  
1329 new tactics, techniques, and procedures that may impact identity proofing processes.  
1330 CSPs and RPs should seek to establish consistent mechanisms for the exchange of  
1331 information between critical security and fraud stakeholders. Where the CSP is external,  
1332 this may be complicated, but should be considered in contractual and legal mechanisms.  
1333 All data collected, transmitted, or shared should be minimized and subject to a detailed  
1334 privacy and legal assessment.

## 1335 **8. Privacy Considerations**

1336 *This section is informative.*

1337 These privacy considerations provide additional information in implementing the  
1338 requirements set forth in [Sec. 5.1.2](#).

### 1339 **8.1. Collection and Data Minimization**

1340 The guidelines permit the collection of only the PII necessary to validate the existence  
1341 of the claimed identity and associate the claimed identity to the applicant, based on  
1342 best available practices for appropriate identity resolution, validation, and verification.  
1343 Collecting unnecessary PII can create confusion regarding why information not being  
1344 used for the identity proofing service is being collected. This leads to invasiveness or  
1345 overreach concerns, which can lead to loss of applicant trust. Further, PII retention can  
1346 become vulnerable to unauthorized access or use. Data minimization reduces the amount  
1347 of PII vulnerable to unauthorized access or use, and encourages trust in the identity  
1348 proofing process.

#### 1349 **8.1.1. Social Security Numbers**

1350 These guidelines permit the CSP collection of the SSN as an attribute for use in identity  
1351 resolution. However, over-reliance on the SSN can contribute to misuse and place the  
1352 applicant at risk of harm, such as through identity theft. Nonetheless, the SSN may  
1353 facilitate identity resolution for CSPs, in particular federal agencies that use the SSN  
1354 to correlate an applicant to agency records. This document recognizes the role of the SSN  
1355 as an attribute and makes appropriate allowance for its use. Knowledge of the SSN is not  
1356 sufficient to serve as identity evidence.

1357 Where possible, CSPs and agencies should consider mechanisms to limit the proliferation  
1358 and exposure of SSNs during the identity proofing process. This is particularly pertinent  
1359 where the SSN is communicated to third party providers during attribute validation  
1360 processes. To the extent possible, privacy protective techniques and technologies should  
1361 be applied to reduce the risk of an individual's SSN being exposed, stored, or maintained  
1362 by third party systems. Examples of this could be the use of attribute claims (e.g., yes/no  
1363 responses from a validator) to confirm the validity of a SSN without requiring it to be  
1364 unnecessarily transmitted and stored by the third party. As with all attributes in the  
1365 identity proofing process, the value and risk of each attribute being processed is subject  
1366 to a privacy risk assessment and for federal agencies the PIA and SORN. The SSN  
1367 should only be collected where it is necessary to support resolution associated with the  
1368 applications assurance and risk levels.

### 1369 **8.2. Notice and Consent**

1370 The guidelines require the CSP to provide explicit notice to the applicant at the time of  
1371 collection regarding the purpose for collecting and maintaining a record of the attributes

1372 necessary for identity proofing, including whether such attributes are voluntary or  
1373 mandatory in order to complete the identity proofing transactions, and the consequences  
1374 for not providing the attributes.

1375 An effective notice will take into account user experience design standards and research,  
1376 and an assessment of privacy risks that may arise from the collection. Various factors  
1377 should be considered, including incorrectly inferring that applicants understand why  
1378 attributes are collected, that collected information may be combined with other data  
1379 sources, etc. An effective notice is never only a pointer leading to a complex, legalistic  
1380 privacy policy or general terms and conditions that applicants are unlikely to read or  
1381 understand.

### 1382 **8.3. Use Limitation**

1383 The guidelines require CSPs to use measures to maintain the objectives of predictability  
1384 (enabling reliable assumptions by individuals, owners, and operators about PII and  
1385 its processing by an information system) and manageability (providing the capability  
1386 for granular administration of PII, including alteration, deletion, and selective  
1387 disclosure) commensurate with privacy risks that can arise from the processing of  
1388 attributes for purposes other than identity proofing, authentication, authorization, or  
1389 attribute assertion, related fraud mitigation, or to comply with law or legal process  
1390 [NISTIR8062].

1391 CSPs may have various business purposes for processing attributes, including providing  
1392 non-identity services to subscribers. However, processing attributes for other purposes  
1393 than those disclosed to a subject can create additional privacy risks. CSPs can determine  
1394 appropriate measures commensurate with the privacy risk arising from the additional  
1395 processing. For example, absent applicable law, regulation or policy, it may not be  
1396 necessary to get consent when processing attributes to provide non-identity services  
1397 requested by subscribers, although notices may help subscribers maintain reliable  
1398 assumptions about the processing (predictability). Other processing of attributes may  
1399 carry different privacy risks that call for obtaining consent or allowing subscribers more  
1400 control over the use or disclosure of specific attributes (manageability). Subscriber  
1401 consent needs to be meaningful; therefore, when CSPs do use consent measures, they  
1402 cannot make acceptance by the subscriber of additional uses a condition of providing the  
1403 identity service.

1404 Consult your SAOP if there are questions about whether the proposed processing falls  
1405 outside the scope of the permitted processing or the appropriate privacy risk mitigation  
1406 measures.

### 1407 **8.4. Redress**

1408 The guidelines require the CSP to provide effective mechanisms for redressing applicant  
1409 complaints or problems arising from the identity proofing, and make the mechanisms easy

1410 for applicants to find and access.

1411 The Privacy Act requires federal CSPs that maintain a system of records to follow  
1412 procedures to enable applicants to access and, if incorrect, amend their records. Any  
1413 Privacy Act Statement should include a reference to the applicable SORN(s) (see  
1414 [Sec. 5.1.2](#)), which provide the applicant with instructions on how to make a request for  
1415 access or correction. Non-federal CSPs should have comparable procedures, including  
1416 contact information for any third parties if they are the source of the information.

1417 CSPs should make the availability of alternative methods for completing the process clear  
1418 to applicants (e.g., in person at a customer service center) in the event an applicant is  
1419 unable to establish their identity and complete the registration process online.

1420 Note: If the identity proofing process is not successful, CSPs should inform  
1421 the applicant of the procedures to address the issue but should not inform the  
1422 applicant of the specifics of why the registration failed (e.g., do not inform  
1423 the applicant, “Your SSN did not match the one that we have on record for  
1424 you”), as doing so could allow fraudulent applicants to gain more knowledge  
1425 about the accuracy of the PII.

## 1426 **8.5. Privacy Risk Assessment**

1427 The guidelines require the CSP to conduct a privacy risk assessment. In conducting a  
1428 privacy risk assessment, CSPs should consider:

- 1429 1. The likelihood that the action it takes (e.g., additional verification steps or records  
1430 retention) could create a problem for the applicant, such as invasiveness or  
1431 unauthorized access to the information; and
- 1432 2. The impact if a problem ~~did occur~~, CSPs should be able to justify any response it  
1433 takes to identified privacy risks, including accepting the risk, mitigating the risk,  
1434 and sharing the risk. The use of applicant consent should be considered a form  
1435 of sharing the risk, and therefore should only be used when an applicant could  
1436 reasonably be expected to have the capacity to assess and accept the shared risk.

## 1437 **8.6. Agency-Specific Privacy Compliance**

1438 The guidelines cover specific compliance obligations for federal CSPs. It is critical  
1439 to involve your agency’s SAOP in the earliest stages of digital authentication system  
1440 development to assess and mitigate privacy risks and advise the agency on compliance  
1441 requirements, such as whether or not the PII collection to conduct identity proofing  
1442 triggers the Privacy Act of 1974 [[PrivacyAct](#)] or the E-Government Act of 2002 [[E-Gov](#)]  
1443 requirement to conduct a Privacy Impact Assessment. For example, with respect to  
1444 identity proofing, it is likely that the Privacy Act requirements will be triggered and  
1445 require coverage by either a new or existing Privacy Act system of records due to the

1446 collection and maintenance of PII or other attributes necessary to conduct identity  
1447 proofing.

1448 The SAOP can similarly assist the agency in determining whether a PIA is required.  
1449 These considerations should not be read as a requirement to develop a Privacy Act SORN  
1450 or PIA for identity proofing alone; in many cases it will make the most sense to draft  
1451 a PIA and SORN that encompasses the entire digital identity lifecycle or includes the  
1452 identity proofing process as part of a larger, programmatic PIA that discusses the program  
1453 or benefit to which the the agency is establishing online access.

1454 Due to the many components of the digital identity lifecycle, it is important for the  
1455 SAOP to have an awareness and understanding of each individual component. For  
1456 example, other privacy artifacts may be applicable to an agency offering or using proofing  
1457 services such as Data Use Agreements, Computer Matching Agreements, etc. The SAOP  
1458 can assist the agency in determining what additional requirements apply. Moreover, a  
1459 thorough understanding of the individual components of digital authentication will enable  
1460 the SAOP to thoroughly assess and mitigate privacy risks either through compliance  
1461 processes or by other means.

## 1462 **9. Usability Considerations**

1463 *This section is informative.*

1464 Note: In this section, the term “users” means “applicants” or “subscribers.”

1465 This section is intended to raise implementers’ awareness of the usability considerations  
1466 associated with enrollment and identity proofing (for usability considerations for typical  
1467 authenticator usage and intermittent events, see [SP800-63B] Sec. 10.

1468 [ISO/IEC9241-11] defines usability as the “extent to which a system, product, or service  
1469 can be used by specified users to achieve specified goals with effectiveness, efficiency  
1470 and satisfaction in a specified context of use.” This definition focuses on users, goals,  
1471 and context of use as the necessary elements for achieving effectiveness, efficiency, and  
1472 satisfaction. A holistic approach considering these key elements is necessary to achieve  
1473 usability.

1474 The overarching goal of usability for enrollment and identity proofing is to promote a  
1475 smooth, positive enrollment process for users by minimizing user burden (e.g., time and  
1476 frustration) and enrollment friction (e.g., the number of steps to complete and amount  
1477 of information to track). To achieve this goal, organizations have to first familiarize  
1478 themselves with their users.

1479 The enrollment and identity proofing process sets the stage for a user’s interactions with a  
1480 given CSP and the online services that the user will access; as negative first impressions  
1481 can influence user perception of subsequent interactions, organizations need to promote a  
1482 positive user experience throughout the process.

1483 Usability cannot be achieved in a piecemeal manner. Performing a usability evaluation on  
1484 the enrollment and identity proofing process is critical. It is important to conduct usability  
1485 evaluation with representative users, realistic goals and tasks, and appropriate contexts of  
1486 use. The enrollment and identity proofing process should be designed and implemented  
1487 so it is easy for users to do the right thing, hard to do the wrong thing, and easy to recover  
1488 when the wrong thing happens.

1489 From the user’s perspective, the three main steps of enrollment and identity proofing are  
1490 pre-enrollment preparation, the enrollment and proofing session, and post-enrollment  
1491 actions. These steps may occur in a single session or there could be significant time  
1492 elapsed between each one (e.g., days or weeks).

1493 General and step-specific usability considerations are described in sub-sections below.

1494 Guidelines and considerations are described from the users’ perspective.

1495 Accessibility differs from usability and is out of scope for this document. [Section 508]  
1496 was enacted to eliminate barriers in information technology and require federal agencies  
1497 to make their electronic and information technology public content accessible to people  
1498 with disabilities. Refer to Section 508 law and standards for accessibility guidance.

## 1499 **9.1. General User Considerations During Enrollment and Identity Proofing**

1500 This sub-section provides usability considerations that are applicable across all steps of  
1501 the enrollment process. Usability considerations specific to each step are detailed in Secs.  
1502 9.2 to 9.4.

- 1503 • To avoid user frustration, streamline the process required for enrollment to make  
1504 each step as clear and easy as possible.
- 1505 • Clearly communicate how and where to acquire technical assistance. For example,  
1506 provide helpful information such as a link to online self-service feature, chat  
1507 sessions, and a phone number for help desk support. Ideally, sufficient information  
1508 should be provided to enable users to answer their own enrollment preparation  
1509 questions without outside intervention.
- 1510 • Clearly explain who is collecting their data and why. Also indicate the path their  
1511 data will take, in particular where the data is being stored.
- 1512 • Ensure all information presented is usable.
  - 1513 – Follow good information design practice for all user-facing materials (e.g.,  
1514 data collection notices and fillable forms).
  - 1515 – Write materials in plain language and avoid technical jargon. If appropriate,  
1516 tailor language to the literacy level of the intended population. Use active  
1517 voice and conversational style, logically sequence main points, use the same  
1518 word consistently rather than synonyms to avoid confusion, and use bullets,  
1519 numbers, and formatting where appropriate to aid readability.
  - 1520 – Consider text legibility, such as font style, size, color, and contrast with  
1521 surrounding background. The highest contrast is black on white. Text  
1522 legibility is important because users have different levels of visual acuity.  
1523 Illegible text will contribute to user comprehension errors or user entry errors  
1524 (e.g., when completing fillable forms). Use sans serif font styles for electronic  
1525 materials and serif fonts for paper materials. When possible, avoid fonts that  
1526 do not clearly distinguish between easily confusable characters (such as the  
1527 letter “O” and the number “0”). This is especially important for enrollment  
1528 codes. Use a minimum font size of 12 points, as long as the text fits the  
1529 display.
- 1530 • Perform a usability evaluation for each step with representative users. Establish  
1531 realistic goals and tasks, and appropriate contexts of use for the usability evaluation.

## 1532 **9.2. Pre-Enrollment Preparation**

1533 This section describes an effective approach to facilitate sufficient pre-enrollment  
1534 preparation so users can avoid challenging, frustrating enrollment sessions. Ensuring

1535 users are as prepared as possible for their enrollment sessions is critical to the overall  
1536 success and usability of the enrollment and identity proofing process.

1537 Such preparation is only possible if users receive the necessary information (e.g., required  
1538 documentation) in a usable format in an appropriate timeframe. This includes making  
1539 users aware of exactly what identity evidence will be required. Users do not need to know  
1540 anything about IALs or whether the identity evidence required is scored as “fair,” “strong,”  
1541 or “superior,” whereas organizations need to know what IAL is required for access to a  
1542 particular system.

1543 To ensure users are equipped to make informed decisions about whether to proceed with  
1544 the enrollment process, and what will be needed for their session, provide users:

- 1545 • Information about the entire process, such as what to expect in each step.
  - 1546 – Clear explanations of the expected timeframes to allow users to plan  
1547 accordingly.
- 1548 • Explanation of the need for — and benefits of — identity proofing to allow users to  
1549 understand the value proposition.
- 1550 • Information on the monetary amount and acceptable forms of payment, and if  
1551 there is an enrollment fee. Offering a larger variety of acceptable forms of payment  
1552 allows users to choose their preferred payment operation.
- 1553 • Information on whether the user’s enrollment session will be in-person or in-person  
1554 over remote channels, and whether a user can choose. Only provide information  
1555 relevant to the allowable session option(s).
  - 1556 – Information on the location(s), whether a user can choose their preferred  
1557 location, and necessary logistical information for in-person or in-person over  
1558 remote channels session. Note that users may be reluctant to bring identity  
1559 evidence to certain public places (bank versus supermarket), as it increases  
1560 exposure to loss or theft.
  - 1561 – Information on the technical requirements (e.g., requirements for internet  
1562 access) for remote sessions.
  - 1563 – An option to set an appointment for in-person or in-person over remote  
1564 channels identity proofing sessions to minimize wait times. If walk-ins are  
1565 allowed, make it clear to users that their wait times may be greater without an  
1566 appointment.
- 1567 \* Provide clear instructions for setting up an enrollment session  
1568 appointment, reminders, and how to reschedule existing appointments.
- 1569 \* Offer appointment reminders and allow users to specify their preferred  
1570 appointment reminder format(s) (e.g., postal mail, voicemail, email, text  
1571 message). Users need information such as date, time, location, and a  
1572 description of required identity evidence.

- 1573 • Information on the allowed and required identity evidence and attributes, whether  
1574 each piece is voluntary or mandatory, and the consequences for not providing the  
1575 complete set of identity evidence. Users need to know the specific combinations of  
1576 identity evidence, including requirements specific to a piece of identity evidence  
1577 (e.g., a raised seal on a birth certificate). This is especially important due to  
1578 potential difficulties procuring the necessary identity evidence.
  - 1579 – Where possible, implement tools to make it easier to obtain the necessary  
1580 identity evidence.
  - 1581 – Inform users of any special requirements for minors and people with unique  
1582 needs. For example, provide users with the information on whether applicant  
1583 reference and/or trusted referee processes are available and information  
1584 necessary to use those processes (see [Sec. 5.1.9](#)).
  - 1585 – If forms are required:
    - 1586 \* Provide fillable forms before and at the enrollment session. Do not  
1587 require users to have access to a printer.
    - 1588 \* Minimize the amount of information users must enter on a form, as users  
1589 are easily frustrated and more error-prone with longer forms. Where  
1590 possible, pre-populate forms.

### 1591 **9.3. Enrollment and Proofing Session**

1592 Usability considerations specific to the enrollment session include:

- 1593 • At the start of the identity proofing session, remind users of the procedure. Do  
1594 not expect them to remember the procedures described during the pre-enrollment  
1595 preparation step. If the enrollment session does not immediately follow pre-  
1596 enrollment preparation, it is especially important to clearly remind users of the  
1597 typical timeframe to complete the proofing and enrollment phase.
- 1598 • Provide rescheduling options for in-person or in-person over remote channels.
- 1599 • Provide a checklist with the allowed and required identity evidence to ensure  
1600 users have the requisite identity evidence to proceed with the enrollment session,  
1601 including enrollment codes, if applicable. If users do not have the complete set of  
1602 identity evidence, they must be informed regarding whether they can complete a  
1603 partial identity proofing session.
- 1604 • Notify users regarding what information will be destroyed, what, if any, information  
1605 will be retained for future follow-up sessions, and what identity evidence they will  
1606 need to bring to complete a future session. Ideally, users can choose whether they  
1607 would like to complete a partial identity proofing session.

- 1608 • Set user expectations regarding the outcome of the enrollment session as prior  
1609 identity verification experiences may drive their expectations (e.g., receiving a  
1610 driver's license in person, receiving a passport in the mail).
- 1611 • Clearly indicate whether users will receive an authenticator immediately at the end  
1612 of a successful enrollment session, if users have to schedule an appointment to pick  
1613 it up in person, or if users will receive it in the mail and when they can expect to  
1614 receive it.
- 1615 • During the enrollment session, there are several requirements to provide users with  
1616 explicit notice at the time of identity proofing, such as what data will be retained on  
1617 record by the CSP (see [Sec. 5.1](#) and [Sec. 8](#) for detailed requirements on notices). If  
1618 CSPs seek consent from a user for additional attributes or uses of their attributes for  
1619 any purpose other than identity proofing, authentication, authorization or attribute  
1620 assertions, per 4.2 requirement (5), make CSPs aware that requesting additional  
1621 attributes or uses may be unexpected or may make users uncomfortable. If users  
1622 do not perceive benefit(s) to the additional collection or uses, but perceive extra  
1623 risk, they may be unwilling or hesitant to provide consent or continue the process.  
1624 Provide users with explicit notice of the additional requirements.
- 1625 • If an enrollment code is issued:
  - 1626 – Notify users in advance that they will receive an enrollment code, when to  
1627 expect it, the length of time for which the code is valid, and how it will arrive  
1628 (e.g., physical mail, SMS, landline telephone, email, or physical mailing  
1629 address).
  - 1630 – When an enrollment code is delivered to a user, include instructions on how  
1631 to use the code, and the length of time for which the code is valid. This  
1632 is especially important given the short validity timeframes specified in  
1633 [Sec. 5.1.6](#).
  - 1634 – If issuing a machine-readable optical label, such as a QR Code (see  
1635 [Sec. 5.1.6](#)), provide users with information on how to obtain QR code  
1636 scanning capabilities (e.g., acceptable QR code applications).
  - 1637 – Inform users that they will be required to repeat the enrollment process if  
1638 enrollment codes expire or are lost before use.
  - 1639 – Provide users with alternative options as not all users are able to access and  
1640 use technology equitably. For example, users may not have the technology  
1641 needed for this approach to be feasible.
- 1642 • At the end of the enrollment session,
  - 1643 – If enrollment is successful, send users confirmation regarding the successful  
1644 enrollment and information on next steps (e.g., when and where to pick up  
1645 their authenticator, when it will arrive in the mail).

- 1646 – If enrollment is partially complete (due to users not having the complete set  
1647 of identity evidence, users choosing to stop the process, or session timeouts),  
1648 communicate to users:
- 1649 \* what information will be destroyed;
  - 1650 \* what, if any, information will be retained for future follow-up sessions;
  - 1651 \* how long the information will be retained; and
  - 1652 \* what identity evidence they will need to bring to a future session.
- 1653 – If enrollment is unsuccessful, provide users with clear instructions for  
1654 alternative enrollment session types, for example, offering in-person proofing  
1655 for users that ~~can not~~ complete remote proofing.
- 1656 • If users receive the authenticator during the enrollment session, provide users  
1657 information on the use and maintenance of the authenticator. For example,  
1658 information could include instructions for use (especially if there are different  
1659 requirements for first-time use or initialization), information on authenticator  
1660 expiration, how to protect the authenticator, and what to do if the authenticator  
1661 is lost or stolen.
  - 1662 • For both in-person and remote identity proofing, additional usability considerations  
1663 apply:
    - 1664 – At the start of the enrollment session, operators or attendants need to explain  
1665 their role to users (e.g., whether operators or attendants will walk users  
1666 through the enrollment session or observe silently and only interact as  
1667 needed).
    - 1668 – At the start of the enrollment session, inform users that they must not depart  
1669 during the session, and that their actions must be visible throughout the  
1670 session.
    - 1671 – When biometrics are collected during the enrollment session, provide users  
1672 clear instructions on how to complete the collection process. The instructions  
1673 are best given just prior to the process. Verbal instructions with corrective  
1674 feedback from a live operator are the most effective (e.g., instruct users where  
1675 the biometric sensor is, when to start, how to interact with the sensor, and  
1676 when the biometric collection is completed).
  - 1677 • Since remote identity proofing is conducted online, follow general web usability  
1678 principles. For example:
    - 1679 – Design the user interface to walk users through the enrollment process.
    - 1680 – Reduce users' memory load.
    - 1681 – 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.

## 1703 **10. Equity Considerations**

1704 *This section is informative.*

1705 This section is intended to provide guidance to CSPs for assessing the risks associated  
1706 with inequitable access, treatment, or outcomes for individuals using its identity services,  
1707 as required in [Sec. 5.1.3](#). It provides a non-exhaustive list of potential areas in the identity  
1708 proofing process that may be subject to inequities, as well as possible mitigations that can  
1709 be applied. CSPs can use this section as a starting point for considering where the risks  
1710 for inequitable access, treatment, or outcomes exist within its identity service. It is not  
1711 intended that the ~~below guidance~~ be considered a definitive, all-inclusive list of associated  
1712 equity risks to identity services.

1713 In assessing equity risks, a CSP starts by considering the overall user population served  
1714 by its identity proofing and enrollment service. Additionally, the CSP further identifies  
1715 groups of users within the population whose shared characteristic(s) can cause them to  
1716 be subject to inequitable access, treatment, or outcomes when using that service. CSPs  
1717 are encouraged to assess the effectiveness of any mitigations by evaluating their impacts  
1718 on the affected user group(s). The usability considerations provided in [Sec. 9](#) should also  
1719 be considered when applying equity risk mitigations to help improve the overall usability  
1720 and equity for all persons using an identity service.

### 1721 **10.1. Equity and Identity Resolution**

1722 Identity resolution involves collecting the minimum set of attributes to be able to  
1723 distinguish the claimed identity as a single, unique individual within the population  
1724 served by the identity service. Attributes are obtained from ~~presented~~ identity evidence,  
1725 applicant self-assertion, and/or back-end attribute providers.

1726 This section provides a set of possible problems and mitigations with the inequitable  
1727 access, treatment, or outcomes associated with the identity resolution process:

1728 **Description: The identity service design requires an applicant to enter their name**  
1729 **using a Western name format (e.g., first name, last name, optional middle name).**

1730 Possible mitigations include:

- 1731 1. Analyzing possible name configurations and determine how all names can be  
1732 accurately accommodated using the name fields
- 1733 2. Providing easy-to-find and use guidance to users on how to enter all names using  
1734 the name fields

1735 **Description: The identity service cannot accommodate applicants whose name,**  
1736 **gender, or other attributes have changed and are not consistently reflected on the**  
1737 **presented identity evidence or match what is in the attribute verifier's records.**

1738 Possible mitigations include:

- 1739 1. Providing Trusted Referees (Sec. 5.1.9.1) who can make risk-based decisions based  
1740 on the specific applicant circumstances
- 1741 2. Allowing for the use of Applicant References (Sec. 5.1.9.2) who can vouch for the  
1742 difference in attributes

## 1743 10.2. Equity and Identity Validation

1744 Identity evidence and core attribute validation involves confirming the genuineness,  
1745 currency, and accuracy of presented identity evidence and the accuracy of any additional  
1746 attributes. These outcomes are accomplished by comparison of the evidence and attributes  
1747 against data held by authoritative or credible sources. When considered together with the  
1748 identity resolution phase, the result of successful validation phase is the confirmation, to  
1749 some level of confidence, that the claimed identity exists in the real world.

1750 This section provides a set of possible problems and mitigations with the inequitable  
1751 access, treatment, or outcomes associated with the evidence and attribute validation  
1752 process:

1753 **Description: Certain user groups do not possess the necessary minimum evidence to**  
1754 **meet the requirements of a given IAL.**

1755 Possible mitigations include:

- 1756 1. Providing Trusted Referees (Sec. 5.1.9.1) who can make risk-based decisions based  
1757 on the specific applicant circumstances
- 1758 2. Allowing for the use of Applicant References (Sec. 5.1.9.2) who can vouch for the  
1759 applicant

1760 **Description: Records held by authoritative and credible sources (e.g., mobile**  
1761 **network operators and phone number verifiers) are insufficient to support the**  
1762 **validation of core attributes or presented evidence for applicants belonging to**  
1763 **certain user groups.**

1764 Possible mitigations include:

- 1765 1. Providing Trusted Referees (Sec. 5.1.9.1) who can make risk-based decisions based  
1766 on the specific applicant circumstances
- 1767 2. Employing alternative authoritative or credible sources

1768 **Description: Records held by authoritative and credible sources may include**  
1769 **inaccurate or false information about persons who are the victims of identity fraud.**

1770 Possible mitigations include:

- 1771 1. Providing Trusted Referees (Sec. 5.1.9.1) who can make risk-based decisions based  
1772 on the specific applicant circumstances
- 1773 2. Allowing ~~for~~ the use of Applicant References (Sec. 5.1.9.2) who can vouch for the  
1774 difference in attributes

1775 **10.3. Equity and Identity Verification**

1776 Identity verification involves proving the binding between the applicant undergoing the  
1777 identity proofing process and the validated, real-world identity established through the  
1778 identity resolution and validation steps. It most often involves collecting a picture (facial  
1779 image capture) of the applicant taken during the identity proofing event and comparing it  
1780 a photograph contained on a presented and validated piece of identity evidence.

1781 This section provides a set of possible problems and mitigations with the inequitable  
1782 treatment or outcomes associated with the identity verification phase:

1783 **Description: Image capture technologies lack the ability to capture certain skin**  
1784 **tones or facial features of sufficient quality to perform a comparison.**

1785 Possible mitigations include:

- 1786 1. Employing robust image capture technologies that are able to accommodate  
1787 different skin tones, facial features, and lighting situations
- 1788 2. Conducting operational testing to determine if the image capture technologies have  
1789 introduced unintentional biases
- 1790 3. Providing risk-based alternative processes that compensate for residual bias and  
1791 technological limitations

1792 **Description: Facial coverings worn for religious purposes impede the ability to**  
1793 **capture a facial image of an applicant.**

1794 Possible mitigations include:

- 1795 1. Providing Trusted Referees (Sec. 5.1.9.1) who can make risk-based decisions based  
1796 on the specific applicant circumstances.
- 1797 2. Providing alternative ways to accomplish identity verification, such as an in-person  
1798 proofing.

1799 **Description: When using 1:1 facial image comparison technologies, biased facial**  
1800 **comparison algorithms may result in false non-matches.**

1801 Possible mitigations include:

- 1802 1. Using algorithms that are independently tested for consistent performance across  
1803 demographic groups and image types
- 1804 2. Supporting alternative processes to compensate for residual bias and technological  
1805 limitations
- 1806 3. Conducting ongoing quality monitoring and operational testing to identify  
1807 performance variances ~~are identified~~ across demographic groups and implementing  
1808 corrective actions as needed (e.g., updated algorithms, machine learning, etc.)

1809 **Description: When employing physical facial image comparison performed by CSP**  
1810 **operators, human biases and inconsistencies in making facial comparisons may**  
1811 **result in false non-matches.**

1812 Possible mitigations include:

- 1813 1. Defining policy and procedures aimed at reducing/eliminating the inequitable  
1814 treatment of applicants by CSP operators/agents
- 1815 2. Rigorously training and certifying ~~of~~ operators
- 1816 3. Conducting ongoing quality monitoring and taking corrective actions when biases,  
1817 ~~or inequitable treatments~~ or outcomes, are identified

#### 1818 **10.4. Equity and User Experience**

1819 The Usability Considerations section of this document (Sec. 9) provides CSPs with  
1820 guidance on how to provide applicants with a smooth, positive identity proofing  
1821 experience. In addition to the specific considerations provided in Sec. 9, this section  
1822 provides CSPs with additional considerations when considering the equity of their user  
1823 experience.

1824 **Description: Lack of access to needed technology (e.g. connected mobile device or**  
1825 **computer), or difficulties in using required technologies, unduly burdens some user**  
1826 **groups.**

1827 Possible mitigations include:

- 1828 1. Allowing the use of helpers who assist applicants, who are otherwise able to meet  
1829 the identity proofing requirements, in the use of the required technologies and  
1830 activities
- 1831 2. Allowing the use of publicly-available devices (e.g., computers or tablets) and  
1832 providing online help resources for completing the identity proofing process on a  
1833 non-applicant-owned computer or device
- 1834 3. Providing in-person proofing options

1835 **Description: The remote or in-person identity proofing process presents challenges**  
1836 **for persons with disabilities.**

1837 Possible mitigations for remote identity proofing include:

- 1838 1. Providing Trusted Referees (Sec. 5.1.9.1) who are trained to communicate and  
1839 assist people with a variety of needs or disabilities (e.g., fluent in sign language)
- 1840 2. Allowing for the use of Applicant References (Sec. 5.1.9.2)
- 1841 3. Supporting the use of accessibility and other technologies, such as audible  
1842 instructions, screen readers and voice recognition technologies

1843 Possible mitigations for in-person identity proofing include:

- 1844 1. Providing trained operators who are trained to communicate and assist people with  
1845 a variety of needs or disabilities (e.g., fluent in sign language)
- 1846 2. Choosing equipment and workstations that can be adjusted to different heights and  
1847 angles
- 1848 3. Selecting locations that are convenient and comply with ADA accessibility  
1849 guidelines

1850 **References**

1851 *This section is informative.*

1852 **General References**

1853 **[A-130]** OMB Circular A-130, *Managing Federal Information as a Strategic Resource*,  
1854 July 28, 2016, available at: [https://obamawhitehouse.archives.gov/sites/default/files/omb/  
1855 assets/OMB/circulars/a130/a130revised.pdf](https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf).

1856 **[COPPA]** *Children’s Online Privacy Protection Act of 1998 (“COPPA”)*, 15 U.S.C. 6501-  
1857 6505, 16 CFR Part 312, available at: [https://www.law.cornell.edu/uscode/text/15/chapter-  
1858 91](https://www.law.cornell.edu/uscode/text/15/chapter-91).

1859 **[EO13985]** Executive Order 13985, *Executive Order On Advancing Racial Equity and*  
1860 *Support for Underserved Communities Through the Federal Government*, January 20,  
1861 2021, available at: [https://www.whitehouse.gov/briefing-room/presidential-actions/  
1862 2021/01/20/executive-order-advancing-racial-equity-and-support-for-underserved-  
1863 communities-through-the-federal-government/](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/).

1864 **[DMF]** National Technical Information Service, *Social Security Death Master File*,  
1865 available at: <https://www.ssdmf.com/Library/InfoManage/Guide.asp?FolderID=1>.

1866 **[E-Gov]** *E-Government Act of 2002* (includes FISMA) (P.L. 107-347), December  
1867 2002, available at: [https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-  
1868 107publ347.pdf](https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf).

1869 **[FBCACP]** *X.509 Certificate Policy For The Federal Bridge Certification Authority*  
1870 *(FBCA)*, Version 2.30, October 5, 2016, available at: [https://www.idmanagement.gov/wp-  
1871 content/uploads/sites/1171/uploads/FBCA\\_CP.pdf](https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FBCA_CP.pdf).

1872 **[FBCASUP]** *FBCA Supplementary Antecedent, In-Person Definition*, July 16, 2009.

1873 **[FEDRAMP]** General Services Administration, *Federal Risk and Authorization*  
1874 *Management Program*, available at: <https://www.fedramp.gov/>.

1875 **[GPG45]** UK Cabinet Office, Good Practice Guide 45, *Identity proofing and verification*  
1876 *of an individual*, December 3, 2014, available at: [https://www.gov.uk/government/  
1877 publications/identity-proofing-and-verification-of-an-individual](https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual).

1878 **[M-03-22]** OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy*  
1879 *Provisions of the E-Government Act of 2002*, September 26, 2003, available at: [https:  
1880 //georgewbush-whitehouse.archives.gov/omb/memoranda/m03-22.html](https://georgewbush-whitehouse.archives.gov/omb/memoranda/m03-22.html).

1881 **[M-04-04]** OMB Memorandum M-04-04, *E-Authentication Guidance for Federal*  
1882 *Agencies*, December 16, 2003, available at: [https://georgewbush-whitehouse.archives.  
1883 gov/omb/memoranda/fy04/m04-04.pdf](https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy04/m04-04.pdf).

1884 **[NISTIR8062]** NIST Internal Report 8062, *An Introduction to Privacy Engineering and*

1885 *Risk Management in Federal Systems*, January 2017, available at: <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf>.

1887 **[NIST-Privacy]** *NIST Privacy Framework*, available at: <https://www.nist.gov/privacy-framework>.

1889 **[NIST-RMF]** *NIST Risk Management Framework*, available at: <https://csrc.nist.gov/Projects/risk-management/about-rmf>.

1891 **[PatriotAct]** *Patriot Act of 2001*, available at: [https://www.justice.gov/archive/ll/what\\_is\\_the\\_patriot\\_act.pdf](https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf).

1893 **[PrivacyAct]** *Privacy Act of 1974* (P.L. 93-579), December 1974, available at: <https://www.justice.gov/opcl/privacy-act-1974>.

1895 **[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](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).

1900 **[Section508]** Section 508 Law and Related Laws and Policies (January 30, 2017), available at: <https://www.section508.gov/manage/laws-and-policies/>.

## 1902 **Standards**

1903 **[Canada]** Government of Canada, *Guideline on Identity Assurance*, available at: <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678&section=HTML>.

1905 **[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>.

1908 **[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](https://openid.net/specs/openid-connect-core-1_0.html).

## 1911 **NIST Special Publications**

1912 NIST 800 Series Special Publications are available at: < <https://csrc.nist.gov/publications/sp800> >.  
1913 The following publications may be of particular interest to those implementing these  
1914 guidelines.

1915 **[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.  
1916

1917 10, 2020), <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>.

1918 **[SP800-63]** NIST Special Publication 800-63-4, *Digital Identity Guidelines*, November  
1919 2022, <https://doi.org/10.6028/NIST.SP.800-63-4.ipd>.

1920 **[SP800-63B]** NIST Special Publication 800-63B-4, *Digital Identity Guidelines:*  
1921 *Authentication and Lifecycle Management*, November 2022, [https://doi.org/10.6028/](https://doi.org/10.6028/NIST.SP.800-63b-4.ipd)  
1922 [NIST.SP.800-63b-4.ipd](https://doi.org/10.6028/NIST.SP.800-63b-4.ipd).

1923 **[SP800-63C]** NIST Special Publication 800-63C-4, *Digital Identity Guidelines:*  
1924 *Assertions and Federation*, November 2022, [https://doi.org/10.6028/NIST.SP.800-63c-](https://doi.org/10.6028/NIST.SP.800-63c-4.ipd)  
1925 [4.ipd](https://doi.org/10.6028/NIST.SP.800-63c-4.ipd).

1926 **[SP800-157]** NIST Special Publication 800-157, *Guidelines for Derived Personal Identity*  
1927 *Verification (PIV) Credentials*, December 2014, [https://dx.doi.org/10.6028/NIST.SP.800-](https://dx.doi.org/10.6028/NIST.SP.800-157)  
1928 [157](https://dx.doi.org/10.6028/NIST.SP.800-157).

1929 **Appendix A. Change Log**

1930 *This appendix is informative.*

1931 This appendix provides a high-level overview of the changes to SP 800-63A since its  
1932 initial release.

- 1933 • Adds requirements for a new IAL1 for lower-risk applications
- 1934 • Swaps the content in sections 4 and 5 to facilitate the introduction of identity  
1935 proofing concepts before providing related requirements
- 1936 • Provides guidance and requirements for characteristics of acceptable identity  
1937 evidence, including physical documents and digital evidence
- 1938 • Decouples the collection of identity attributes from the collection of identity  
1939 evidence
- 1940 • Introduces the concept of core attributes
- 1941 • Expands acceptable evidence and attribute validation sources to include credible  
1942 sources
- 1943 • Adds requirements for CSP-specific privacy risk assessments and considerations for  
1944 integrating the results into agency PIAs
- 1945 • Adds new guidance and requirements for the consideration of equity risks  
1946 associated with identity proofing processes
- 1947 • Provides guidance and requirements for the use of Trusted Referees and Applicant  
1948 References