CONFORMANCE CRITERIA for

NIST SP 800-63A *ENROLLMENT AND IDENTITY PROOFING*

and

NIST SP 800-63B *AUTHENTICATION AND LIFECYCLE MANAGEMENT*

June 2020

Comments on this publication may be submitted to: dig-comments@nist.gov.

National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-63A Conformance Criteria

Synopsis

All normative requirements for NIST Special Publication (SP) 800-63A *Enrollment and Identity Proofing* and SP 800-63B *Authentication and Lifecycle Management* are presented in those volumes. Pursuant to Office of Management and Budget Policy Memorandum M-19-17, these Conformance Criteria present non-normative informational guidance on all normative requirements contained in those volumes for the assurance levels IAL2 and IAL3 and AAL2 and AAL3. The normative text from those volumes is restated in the Conformance Criteria for clarity of presentation. The complete set of conformance criteria are informative and intended to provide non-normative supplemental guidance to federal agencies and other organizations to facilitate implementation and assessment. The supplemental guidance is intended to provide information to clarify the normative requirement/control and provide non-normative information about how to meet conformance for purposes of implementation and assessment.

Comments or questions on the Conformance Criteria may be sent to dig-comments@nist.gov.

Contents

1 Introduction

This document presents conformance criteria for NIST Special Publication 800-63A *Enrollment and Identity Proofing*. This document presents conformance criteria for all normative requirements and controls for SP 800-63A for assurance levels IAL2/3.

The conformance criteria are enumerated to facilitate referencing and indexing. Similar to the indexing of the inventory of controls for NIST Special Publication 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations*, the enumeration of the conformance criteria is separated into sections for criteria that apply to specific functional areas in SP 800-63A and -63B; this also is intended to facilitate referencing and indexing. An index is also provided for the complete set of conformance criteria to facilitate reference to specific topics and criteria.

All the conformance criteria are presented in the following format:

- **Requirement –** presentation of the normative requirement/control statement from SP 800-63A and SP 800-63B.
- **Supplemental guidance** – presentation of informative guidance to facilitate the understanding, implementation and assessment for each criterion.
- **Assessment objective** – Presentation of the intended objective and outcome from the assessment of conformance for each criterion.
- **Potential assessment methods and objects** – Presentation of suggested methodologies for performing conformance assessment for each criterion.
- **Potential test methods** – Where applicable, presentation of suggested test methodologies for performing conformance testing for applicable criteria.

As described above, each conformance criterion presents the normative requirement/control statement from SP 800-63A. All normative requirements are presented in SP 800-63A and are restated in the conformance criteria for clarity of presentation. The complete set of conformance criteria are informative and intended to provide non-normative supplemental guidance for implementation and assessment. The supplemental guidance is intended to provide information to clarify the normative requirement/control and provide information about how to meet conformance for purposes of implementation and assessment. The assessment objective is intended to present the requirements and controls in terms of outcomes.

SP 800-63-3 applies the NIST Risk Management Framework to identity systems and operations. The risk management framework advances the principle that organizations should have the flexibility to apply and tailor controls and requirements to best meet the risk environment of the organization, its systems and operations, target populations and use cases. Therefore, the conformance criteria are not intended to be prescriptive; rather, the criteria are intended to present the intended outcomes for the requirements and controls and allow flexibility in both the implementation and assessment of the criteria. Potential assessment and test methods are presented as suggested means to achieve/assess conformance to the requirement but should be considered suggestions rather than prescribed methods. Assessors have flexibility and responsibility to determine the most appropriate conformance assessment methods for the specific organization, system and operations, and risk environment.

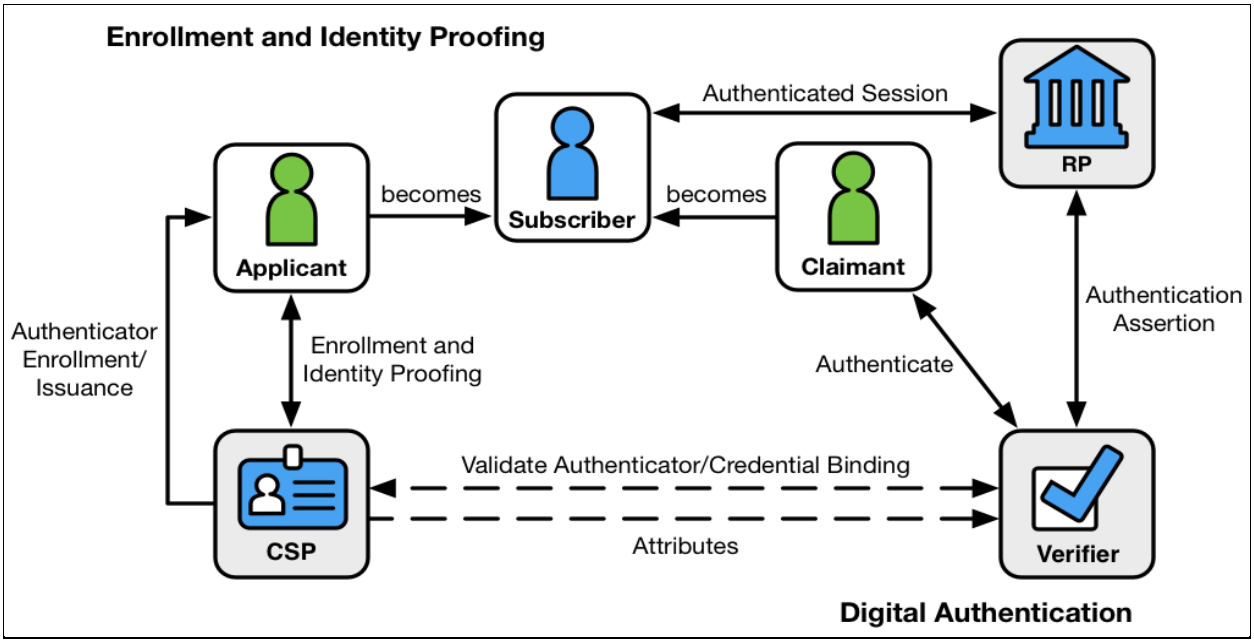
While NIST Special Publications and guidance materials such as these conformance criteria are intended for federal agencies, the potential audiences and uses for the conformance criteria include:

- Federal agencies for the implementation of SP 800-63-3 and assessment of implementation, risks, and controls in meeting FISMA requirements.
- Credential Service providers for the implementation of services and products to meet conformance requirements of SP 800-63-3.
- Organizations and services that perform assessment and, potentially, certification of conformance with SP 800-63-3 requirements.
- Audit organizations that offer and provide audit services for determining federal agency or external non-federal service provider conformance to SP 800-63-3 requirements and controls.
- The General Services Administration to facilitate activities to address the responsibility in Office of Management and Budget Policy Memo M-19-17: "*Determine the feasibility, in coordination with OMB, of establishing or leveraging a public or private sector capability for accrediting ICAM products and services available on GSA acquisition vehicles, and confirm the capability leverages NIST developed criteria for 800-63 assurance levels. This capability should support and not duplicate existing Federal approval processes*."

These conformance criteria are publicly available at the NIST Identity and Access Management Resource Center: https://www.nist.gov/topics/identity-access-management. NIST anticipates that this resource may be periodically updated based on federal agency and industry experience and feedback. Questions and comments on these resources may be sent to dig-comments@nist.gov.

Digital Identity Model Roles

SP 800-63-3 Figure 4-1 presents the *Digital Identity Model* and describes the various entities and interactions that comprise the model as illustrated below.



SP 800-63-3 Figure 4-1 Digital Identity Model

SP 800-63A presents requirements, controls and activities to perform the identity proofing and enrollment activities on the left side of Figure 4-1 *The Digital Identity Model.* After successful identity proofing the applicant is enrolled as a subscriber in the digital identity system. As illustrated the interactions for identity proofing and enrollment are between the applicant and the Credential Service Provider (CSP). The SP 800-63A requirements and controls and, therefore, all the SP 800-63A conformance criteria apply directly to the CSP.

As illustrated on the right side of the model, following successful identity proofing in the CSP's digital identity system, the subscriber registers authenticator(s) to their account to complete enrollment. The subscriber can then prove possession and control of the authenticator(s) for digital authentication transactions. This is a functional model to illustrate the activities involved for enrollment, identity proofing and authentication and presents three entities that may interact with the subscriber for digital authentication transactions – the Relying Party (RP), Verifier, and Credential Service Provider (CSP). In this functional model the RP, CSP, and Verifier roles are depicted separately; however, all the functional roles shown may be provided by a single entity or combinations among the three roles of RP, CSP, and Verifier. The SP 800-63B Conformance Criteria are applicable to all three roles. These roles may be performed by a single entity or may represent separate entities. In most scenarios, federal agencies serve in all three roles of *The Digital Identity Model* -- RP, CSP and Verifier. The exception to this is when a third party, such as the GSA login.gov service, provides federation services on behalf of federal agencies.

Digital identity service providers outside the federal government that voluntarily adopt SP 800-63-3 as a standard will need to examine the roles performed for digital authentication to determine the applicability of the SP 800-63B Conformance Criteria to their specific implementation.

SP 800-63A Optional Identity Proofing Services

In addition to a core set of requirements that are applicable to all CSPs (general and IAL-specific requirements), SP 800-63A includes provisions for several optional services that a CSP may offer as part of its identity service. These optional services include **Supervised Remote Identity Proofing** and the use of **Trusted Referees**.

A CSP is only responsible for meeting the requirements associated with the specific optional services it provides. ***If a CSP opts to provide one or more of these optional services, it is subject to all associated conformance criteria.*** Therefore, the application of the associated conformance criteria is dependent on whether the CSP has opted to offer the service or not. If the CSP has not opted to offer the optional service(s), the associated conformance criteria do not apply.

To facilitate the selection of the applicable conformance criteria, this document groups the requirements and associated criteria for each optional service. Section 2 of this document provides guidance for selecting the conformance criteria to which a CSP is subject.

Conditional Requirements

Some requirements in SP 800-63A and SP 800-63B are conditional based on circumstances. These requirements are characterized as follows; IF (a conditional circumstance occurs), THEN this requirement(s) shall apply. Conditional Conformance Criteria follow the same pattern in the

statement of the normative requirement: IF (this conditional circumstance occurs). THEN this normative requirement and Conformance Criterion shall apply. Conditional conformance criteria are otherwise presented in the same format as all other criteria.

Federal Agency Unique Requirements

Some requirements in SP 800-63A and SP 800-63B apply uniquely to federal agencies and the conformance criteria for these requirements clearly indicate this status. In general, these conformance criteria do not apply to entities external to the federal government that have voluntarily chosen to adopt the SP 800-63A and SP 800-63B standards or are otherwise applying the conformance criteria to the services that they provide.

2 Enrollment and Identity Proofing Conformance Criteria

Selecting Appropriate Requirements

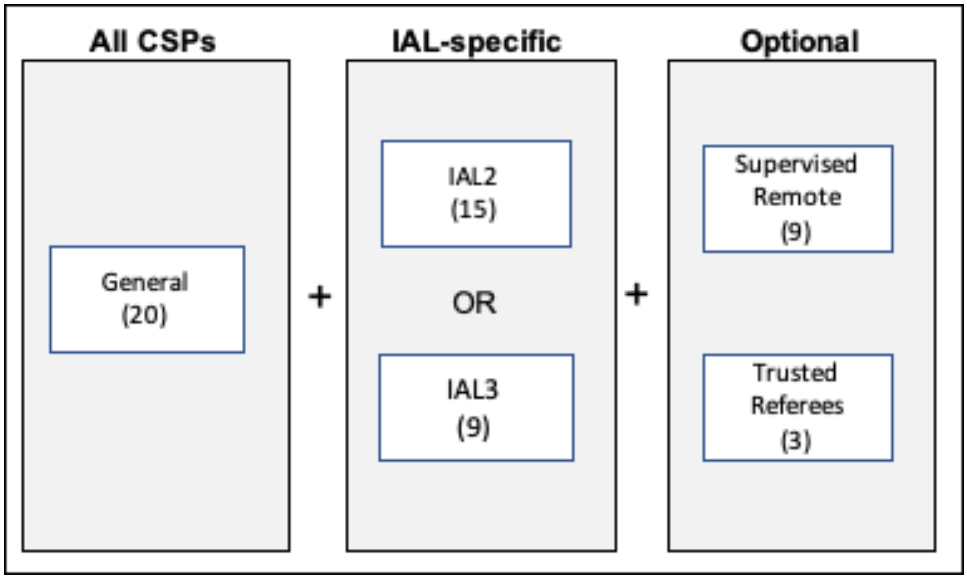
While this document provides guidelines for assessing conformance to all the normative requirements (SHALL and SHALL NOT statements) provided in SP 800-63A, not all requirements are applicable to all service providers. In order to facilitate the selection of requirements applicable to a specific CSP, the conformance criteria in this document are grouped into categories according to functional components of an identity service.

The following steps provide a method for selecting the appropriate requirements, and associated conformance assessment criteria, that are applicable to a particular CSP:

1. Select all of the General (GEN) criteria. Note that, while all General criteria are applicable to all CSPs, some are conditional and may not apply to a specific CSP. In such cases, the assessment results should clearly indicate that a particular criterion is not applicable to that CSP.
2. Determine the identity assurance level at which the CSP is being assessed and select the IAL-specific criteria (IAL2 or IAL3).
3. If the CSP provides Supervised Remote In-person Proofing services, select the Supervised Remote Proofing (SRP) criteria.
4. If the CSP utilizes Trusted Referees, select the Trusted Referees (TRR) criteria.

Index to Conformance Assessment Criteria

The diagram below illustrates how the criteria are grouped according to the identity service component or service. The number of associated criteria is indicated in parentheses.



Index to General Criteria

There are 21 general requirements that apply to all CSPs providing identity proofing services.

ID	63A Section		ID	63A Section
GEN-1	4.2 (1)		GEN-8c	4.2 (7)
GEN-2	4.4.1.1 4.2 (2)		GEN-9	4.2 (8)
GEN-3	4.2 (3)		GEN-10	4.2 (9)
GEN-4a	4.2 (4)		GEN-11	4.2 (10)
GEN-4b	4.2 (4)		GEN-12	4.2 (11)
GEN-5a	4.2 (5)		GEN-13	4.2 (12)
GEN-5b	4.2 (5)		GEN-14	4.6
GEN-6	4.2 (6)		GEN-15	5.2
GEN-7	4.2 (6)		GEN-16	5.3.4.1
GEN-8a	4.2 (7)		GEN-17	5.3.4.1
GEN-8b	4.2 (7)			

Additionally, there are 2 general requirements that apply to biometric collection for in-person identity proofing and enrollment at IAL2 and IAL3.

ID	63A Section		ID	63A Section
GEN-18	5.3.3.1(1)		GEN-19	5.3.3.1(2)

Index to IAL2 Requirements

CSPs that provide identity proofing at IAL2 are responsible for demonstrating conformance to the 15 IAL2 requirements, in addition to all General Requirements.

ID	63A Section		ID	63A Section
IAL2-1	4.4.1.5 4.4		IAL2-7	4.4.1.6 (4)
IAL2-2	4.4.1.2		IAL2-8a	4.4.1.6 (5)
IAL2-3	4.4.1.3		IAL2-8b	4.4.1.6 (5)
IAL2-4a	4.4.1.4		IAL2-8c	4.4.1.6 (5)
IAL-4b	5.3.1		IAL2-8d	4.4.1.6 (5)
IAL2-5	4.4.1.4		IAL2-8e	4.4.1.6 (5)
IAL2-6a	4.4.1.6 (2)		IAL2-9	4.4.1.6 (5) 4.4.1.8
IAL2-6b	4.4.1.6 (1)			

Index to IAL3 Requirements

CSPs that provide identity proofing to IAL3 are responsible for demonstrating conformance with the 10 IAL3 requirements, in addition to all General Requirements.

ID	63A Section		ID	63A Section
IAL3-1	4.5.1		IAL3-6	4.5.6
IAL3-2	4.5.2		IAL3-7	4.5.6
IAL3-3	4.5.3		IAL3-8	4.5.6
IAL3-4	4.5.4		IAL3-9	4.5.6
IAL3-5	4.5.5		IAL3-10	4.5.7

Index to Supervised Remote Proofing Requirements

In addition to the General Requirements, and the IAL-specific requirements, CSPs that perform Supervised Remote In-Person Proofing are responsible for demonstrating conformance with the 8 SRP requirements.

ID	63A Section		ID	63A Section
SRP-1	5.3.3.2		SRP-5	5.3.3.2 (4)
SRP-2	5.3.3.2 (1)		SRP-6	5.3.3.2 (5)
SRP-3	5.3.3.2 (2)		SRP-7	5.3.3.2 (6)
SRP-4	5.3.3.2 (3)		SRP-8	5.3.3.2 (70

Index to Trusted Referee Requirements

CSPs that allow Trusted Referees are responsible for demonstrating conformance with the 3 TRR requirements.

ID	63A Section		ID	63A Section
TRR-1	5.3.4 (2)		TRR-3	5.3.4 (3)
TRR-2	5.3.4 (3)			

3 General Requirements

Component: General – Identity Proofing and/or Enrollment Services

The following requirements apply to all CSPs performing identity proofing at IAL2 or IAL3.

GEN-1	**REQUIREMENT**: Identity proofing SHALL NOT be performed to determine suitability or entitlement to gain access to services or benefits. (4.2) **SUPPLEMENTAL GUIDANCE**: The sole objective of identity proofing is to ensure the applicant is who they claim to be to a stated level of certitude. **ASSESSMENT OBJECTIVE:** determine that the CSP only collects identity information for the purpose of identity proofing. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented policies* for a statement either to the effect that: 1. it does not perform identity proofing to determine suitability or access entitlement; or 2. it performs identity proofing for the sole purpose of ensuring, to some level of certitude, that an applicant is who they claim to be

GEN-2	**REQUIREMENTS**: Collection of PII SHALL be limited to the minimum necessary to resolve to a unique identity in a given context. (4.4.1.1) Collection of PII SHALL be limited to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity with the applicant providing identity evidence for appropriate identity resolution, validation, and verification. (4.2) **SUPPLEMENTAL GUIDANCE**: The goal of identity resolution is to uniquely distinguish an individual within a given population or context. Effective identity resolution uses the smallest set of attributes necessary to resolve to a unique individual. It provides the CSP an important starting point in the overall identity proofing process, to include the initial detection of potential fraud, but in no way represents a complete and successful identity proofing transaction. Collection of PII may include attributes are used to correlate identity evidence to authoritative sources and to provide RPs with attributes used to make authorization decisions. There may be many different sets that suffice as the minimum, so it is recommended that CSPs choose this set to balance privacy and

	the user's usability needs, as well as the likely attributes needed in future uses of the digital identity. Examples of attributes that may be used for minimum identity attribute sets include: • Name (first, last. middle) with combinations and variations, • Address (#, Street, City, County, State, Zip code) with combinations and variations, • Date of birth (DDMMYYYY) with combinations and variations, • Email address, • Phone number. For population sets that are more defined than the general population (e.g., military veterans, Native Americans), these minimum attribute sets may be tailored to that specific community. Additionally, it is recommended that CSPs document which alternative attributes it will accept in cases where an applicant cannot provide the minimum necessary attributes (e.g., applicant does not have a home address or phone number). **ASSESSMENT OBJECTIVES:** 1. confirm the CSP limits the PII it collects to the minimum amount required to resolve to a unique identity in a given context, and 2. confirm it limits the PII it collects to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity with the applicant. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSPs *enrollment* or *system logs* for the attributes it collects for each applicant, and **Examine**: the CSP's *documented policies or practices*: ● regarding the types PII collected for identity proofing; and ● where PII is collected in excess of the minimum required for identity proofing, a list of the additional PII, and the reason or use for which it is being collected.

GEN-3	**REQUIREMENT**: The CSP SHALL provide explicit notice to the applicant at the time of collection regarding the purpose for collecting and maintaining a record of the attributes necessary for identity proofing, including whether such

	attributes are voluntary or mandatory to complete the identity proofing process, and the consequences for not providing the attributes. (4.2) **SUPPLEMENTAL GUIDANCE**: Notice of proofing may contain at a minimum: ● Attribute information that is mandatory ● Attribute information that is voluntary ● What will be done with the information collected ● How the information will be protected ● Consequence of not providing mandatory attribute information (e.g., suspension/termination of the identity proofing process). This notice may be delivered as an online screen (for remote identity proofing), a poster or printed notice at in-person proofing locations, or an oral notice delivered at the time of information collection. **ASSESSMENT OBJECTIVE:** confirm the CSP provides explicit notice to applicants at the time of identity proofing that meets the above requirement **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: at least one of the following: ● *documented policies or practices* to determine the CSP's policy and implementation of providing user notice, or ● the *system's functionality* to view the user notice. ● a *sample* of the notice (poster or printed notice) and determine it includes above required information.

GEN-4a	**REQUIREMENT**: If CSPs process attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively "identity service"), related fraud mitigation, or to comply with law or legal process, then CSPs SHALL implement measures to maintain predictability and manageability commensurate with the privacy risk arising from the additional processing. (4.2 #4) **SUPPLEMENTAL GUIDANCE**: Predictability and manageability measures include providing clear notice, obtaining subscriber consent, or enabling selective use or disclosure of attributes. Predictability is meant to build trust and provide accountability and requires full understanding (and disclosure) of how the attribute information will be used.

	Manageability also builds trust by demonstrating a CSPs ability to control attribute information throughout processing – collection, maintenance, retention. **ASSESSMENT OBJECTIVE:** identify which, if any, measures the CSPs employs to maintain predictability and manageability commensurate with the privacy risk arising from any additional processing of attributes. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented policies or practices* to determine which predictability and manageability measures it employs, (e.g., notice, consent, selective disclosure).

GEN-4b	*If the CSP employs consent as part of its measures to maintain predictability and manageability,* **REQUIREMENT**: …then it SHALL NOT make consent for the additional processing a condition of the identity service. (4.2 #4) **SUPPLEMENTAL GUIDANCE**: Consent involves collecting and recording an affirmative response from the applicant that they agree to the additional processing of their attributes. In order to make this consent meaningful, it is recommended that CSPs first disclose to its applicants which attributes are being collected and processed and why. **ASSESSMENT OBJECTIVE:** determine if the CSP obtains consent from applicants for the additional processing of their attributes and, if it does, confirm that it does not disqualify applicants from using their service for failing to provide this consent. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented policies or practices* to confirm it does not make consent to this additional processing a condition of using its service.

GEN-5a	**REQUIREMENT**: The CSP SHALL provide mechanisms for redress of applicant complaints or problems arising from the identity proofing. (4.2 #5) These [redress] mechanisms SHALL be easy for applicants to find and use. (4.2 #5) **SUPPLEMENTAL GUIDANCE**: Section 4.2 requirement 5 [of 800-63A] requires the CSP to provide effective mechanisms for redressing applicant complaints or problems arising from the identity proofing processes and make the mechanisms easy for applicants to find and access.

	The Privacy Act requires federal CSPs that maintain a system of records to follow procedures to enable applicants to access and, if incorrect, amend their records. Any Privacy Act Statement should include a reference to the applicable SORN(s), which provide the applicant with instructions on how to make a request for access or correction. It is recommended that non-federal CSPs have comparable procedures, including contact information for any third parties if they are the source of the information. It is recommended that CSPs make the availability of any alternative methods for completing the identity proofing and enrollment processes clear to users (e.g., in person at a customer service center, if available) in the event an applicant is unable to properly complete the initial identity proofing and enrollment process requirements online. Note: If the ID proofing process is not successful, it is recommended that CSPs inform the applicant of the procedures to address the issue but avoid informing the applicant of the specifics of why the registration failed. To be effective, the use of a CSP's redress mechanism results in a timely correction of errors, resolution of the dispute or complaint, and the process should not be overly burdensome or complex. It is recommended that the CSP document and publish, in a manner which is easy for Applicants to find and use, its mechanisms for redress of Applicant complaints or problems arising from the identity proofing processes. **ASSESSMENT OBJECTIVES:** 1. confirm the CSP provides redress mechanisms; and 2. confirm these mechanisms are easy for applicants to find and use. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: 1. **Examine**: the CSP's *documented policies or practices* to determine if the CSP provides mechanisms for redress. 2. **Examine**: one or both of the following: o the CSP's *documented policies or practices* to confirm its redress mechanisms are easy for applicants to find and use, or o the *system's functionality* to view how the redress mechanism is made available to applicants.

GEN-5b	**REQUIREMENT**: The CSP SHALL assess the [redress] mechanisms for their efficacy in achieving resolution of complaints or problems. (4.2 #5)

	SUPPLEMENTAL GUIDANCE: "Effective" in this requirement means that use of the redress mechanism will result in a timely correction of errors, resolution of the dispute or complaint, and the process shall not be overly burdensome or complex. It is recommended that CSPs maintain a record or log of all cases – including outcomes - where applicants have sought redress for complaints or problems arising from the identity proofing and provide for the periodic review of these records. **ASSESSMENT OBJECTIVE:** confirm the CSP assesses its redress mechanisms to determine if they are effective in resolving applicant complaints or problems. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the *record of the CSPs assessment* of its redress mechanisms; or **Examine:** the CSP's *records/logs* of previous cases where an applicant sought redress.

GEN-6	**REQUIREMENT**: The identity proofing and enrollment processes SHALL be performed according to an applicable written policy or *practice statement* that specifies the particular steps taken to verify identities. (4.2 #6) **SUPPLEMENTAL GUIDANCE**: Having documented procedures is a prerequisite for transparency, accountability, quality control, auditability, and ease of interoperability among federated communities. The documentation, dissemination, review and update to identity and authentication processes is a core control under NIST 800-53 IA-1 Identification and Authentication Policy and Procedures. **ASSESSMENT OBJECTIVE:** review the CSPs documentation (i.e., policy, standard operating procedures, and/or practices statement) to confirm it accurately represents the CSP's complete identity proofing procedures. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented policies or practices* to determine it accurately represents all aspects of the CSP's identity proofing process.

GEN-7	**REQUIREMENT**: The *practice statement* SHALL include control information detailing how the CSP handles proofing errors that result in an applicant not being successfully enrolled. (4.2 #6)

	SUPPLEMENTAL GUIDANCE: "Proofing errors" in this context refer to circumstances that result in the inability or failure to complete the identity proofing and enrollment processes. Such circumstances may include: ● Applicant abandons the identity proofing and enrollment processes; ● Applicant fails to provide mandatory attribute information; ● Identity evidence of required strength is not provided; ● Identity evidence is rejected following inspection; ● Identity evidence and information do not correlate; ● Information from identity evidence is not validated by issuing or authoritative sources at the required strength; ● Identity evidence verification of binding to the applicant fails; and ● Applicant fails to confirm enrollment code within code validity period. Depending on the circumstances above, it is recommended that the documentation include the number of retries allowed, proofing alternatives (e.g., in-person if remote fails), or fraud countermeasures when anomalies are detected. (4.2) Additional controls for handling identity proofing errors include: ● Advising the applicant of identity proofing failure and recourse options; and, ● Recording the errors in enrollment records/audit logs, along with any mitigating actions. **ASSESSMENT OBJECTIVE:** review the CSP's documentation (i.e., policy, standard operating procedures, or practices statement) to confirm it includes information about how the CSP handles proofing errors. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented policies or practices* to determine how the CSP handles proofing errors that result in an applicant not being successfully enrolled.

GEN-8a	**REQUIREMENT**: The CSP SHALL maintain a record, including audit logs, of all steps taken to verify the identity of the applicant (4.2 #7) **SUPPLEMENTAL GUIDANCE**: Ideally, the CSP's identity system includes the capability to securely record and log key security-related activities associated with the identity proofing process. Examples of key steps that may be recorded in enrollment logs include: ● Identity information collected;

	• Identity evidence provided; • Identity evidence validated; • Identity evidence validation source; • Identity evidence binding verification method; • Identity evidence verification result; • Enrollment code confirmation result; • enrollment result; and • Authenticator enrollment binding. **ASSESSMENT OBJECTIVE:** confirm the CSP's identity system maintains a record, including audit logs, of all steps taken to verify the identity of the applicant. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *audit logs* to view how all steps taken to verify the identities of applicant are recorded by the system.

GEN-8b	**REQUIREMENT**: The CSP SHALL record the types of identity evidence presented in the proofing process. (4.2 #7) **SUPPLEMENTAL GUIDANCE**: Ideally, the CSP's identity system includes the capability to securely record and log specific activities associated with the identity proofing process. For each piece of evidence collected or captured, the record should include: 1. Evidence type; 2. Determined strength; 3. Issuing source; and 4. Method of collection/capture*. * Methods of collection and capture may include camera, flatbed scanner, bar code scanner. **ASSESSMENT OBJECTIVE:** confirm the CSP's identity system maintains a record of the types of identity evidence presented by applicants. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *enrollment records* to confirm the system records the types of identity evidence presented in the proofing process for each applicant.

GEN-8c	**REQUIREMENT**: The CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine: a. Any steps that it will take to verify the identity of the applicant beyond any mandatory requirements specified herein; b. The PII, including any biometrics, images, scans, or other copies of the identity evidence that the CSP will maintain as a record of identity proofing (Note: Specific federal requirements may apply); and c. The schedule of retention for these records (Note: CSPs may be subject to specific retention policies in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply). (4.2 #7) **SUPPLEMENTAL GUIDANCE**: In accordance with its risk management processes, CSPs should conduct – and document the results of - privacy and security risk assessments. It is recommended that the scope of this assessment includes risks associated with: ● Any steps the CSP takes to verify applicant identities beyond what is required by SP 800-63A; ● The CSP's collection, processing, and protection of PII, including any biometrics, images, scans, or other copies of the identity evidence that the CSP will maintain as a record of identity proofing; ● Retention and/or disposal of any records; and ● Adherence to any applicable federal requirements, laws, regulations or policies. **ASSESSMENT OBJECTIVE:** Confirm the CSP has employed a risk assessment process that assessed, at a minimum, the security and privacy risks associated with the above aspects of the identity proofing process. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documentation* to confirm the CSP has employed a risk assessment process and determined its risks associated with: ● any additional steps it takes to verify the identity of an applicant; ● any PII it maintains; and ● the maintenance and retention of identity records.

GEN-9	**REQUIREMENT**: All PII collected as part of the enrollment process SHALL be protected to ensure confidentiality, integrity, and attribution of the information source. (4.2 #8) **SUPPLEMENTAL GUIDANCE**: Unauthorized disclosure of PII can result in tangible and intangible harms to both the CSP as well as the subjects of the PII. After assessing the risks associated with collecting PII as part of its enrollment process, it is recommended that the CSP employ functional and technical mechanisms that adequately protect the confidentiality, integrity, and attribution of the PII under its control. Such mechanisms may include: ● Limiting access to PII data; ● Privacy protecting policies; ● The use of encryption for data at rest and during transmission; and ● Integrity protection mechanisms such as hashes and record access logging. **ASSESSMENT OBJECTIVE:** confirm the CSP protects all PII collected as part of the enrollment process. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's relevant *system documentation* to determine how it protects PII; or **Interview:** appropriate *technical or managerial personnel* to determine how the CSP protects PII.

GEN-10	**REQUIREMENT**: The entire proofing transaction, including transactions that involve a third party, SHALL occur over authenticated protected channels. (4.2 #9) **SUPPLEMENTAL GUIDANCE**: An encrypted communication channel uses approved cryptography where the connection initiator (client) has authenticated the recipient (server). Authenticated protected channels provide confidentiality and man-in-the-middle (MitM) attack protection and are frequently used in the user authentication process. Transport Layer Security* (TLS) is an example of an authenticated protected channel where the certificate presented by the recipient is verified by the initiator. Unless otherwise specified, authenticated protected channels do not require the server to authenticate the client. Authentication of the server is often accomplished through a certificate chain leading to a trusted root rather than individually with each server. (NIST SP 800-

	63-3) *TLS version 1.2 or greater is recommended. **ASSESSMENT OBJECTIVE:** Confirm that the entire proofing transaction – including transactions that involve a third party – occurs over authenticated protected channels. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: one of the both of the following ● the CSP's applicable *system documentation*, or ● *system functionality* to determine that ALL transactions that make up the identity proofing process occur over authenticated protected channels.

GEN-11	**REQUIREMENT**: If the CSP uses fraud mitigation measures, then the CSP SHALL conduct a privacy risk assessment for these mitigation measures. (4.2 #10) Such assessments SHALL include any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography), and be documented per requirement 4.2 (7) above. (4.2 #10) **SUPPLEMENTAL GUIDANCE**: This is a conditional requirement. CSPs may choose to obtain additional confidence in the identity proofing process beyond the requirements for IAL2 and IAL3 through additional fraud mitigation measures. Such measures may include: ● inspecting metadata information, such as by checking geolocation data associated with a mobile device used to send a photo or receive an SMS; ● examining the applicant's device characteristics; ● evaluating behavioral characteristics, such as typing mannerisms, gait, or voice characteristics; and ● checking against authoritative sources, such as the Death Master File. Employing one or more of these fraud mitigation techniques may result in the collection of additional PII about an applicant. Additional PII increases the potential impact of the unauthorized disclosure of this data. As part of the privacy risk assessment on these additional fraud mitigation measures, it is recommended that CSPs consider, at a minimum, the additional data (PII) that is processed, the implications of retaining this additional PII, and ways the

	associated risks can be minimized without negating the effects of the additional measures. These additional fraud mitigation measures are not intended to substitute or replace the mandatory requirements provided in NIST SP 800-63-3. CSPs employing these measures are still responsible for meeting all applicable requirements. **ASSESSMENT OBJECTIVES:** 1. Determine if the CSP uses additional fraud mitigation techniques to gain additional confidence in its identity proofing process. If so, confirm it has conducted a privacy risk assessment with respect to the additional PII associated with employing these mechanisms. 2. Confirm the CSP has documented any privacy risk mitigations it is employing in response the risk assessment conducted on its use of optional fraud mitigation measures. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: *If the CSP employs additional fraud mitigation mechanisms,* **Examine:** the CSP's *risk assessment documentation* to confirm the CSP has conducted a privacy risk assessment on its use of these mechanisms; and **Examine:** the CSP's *risk assessment documentation* to confirm the CSP has captured any privacy risk mitigations.

GEN-12	**REQUIREMENT**: In the event a CSP ceases to conduct identity proofing and enrollment processes, then the CSP SHALL be responsible for fully disposing of or destroying any sensitive data including PII, or its protection from unauthorized access for the duration of retention. (4.2 #11) **SUPPLEMENTAL GUIDANCE**: This is a conditional requirement for CSPs that cease to perform identity proofing and enrollment functions. The CSP is responsible for the proper handling, protection, and retention or disposal of any sensitive data it collects, even after it ceases to provide identity proofing and enrollment services. A CSP may document its policies and procedures for the management of the data is collects in a data handling plan or other document. Additionally, it is recommended that CSPs document any specific retention policies they are subject to, in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply. Specifically, it is recommended that the CSP defines and documents the practices it has in place for fully disposing of or destroying any sensitive data

	including PII, or its continued protection from unauthorized access for the duration of any period of retention. **ASSESSMENT OBJECTIVE:** Confirm the CSP has policies for securely disposing of or destroying and sensitive data it collects, in the event it ceases to provide identity proofing and enrollment services. Additionally, if it is subject to data retention requirements, confirm its plan or for protecting sensitive data from unauthorized access during the required retention period. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *data handling plan* or other *documented practices* to confirm its plan for securely disposing/destroying sensitive data, or protecting it for the duration of retention, in the event is ceases operations.

GEN-13	**REQUIREMENT**: Regardless of whether the CSP is a federal agency or non-federal entity, the following requirements apply to the federal agency *offering or using* the proofing service: a. The agency SHALL consult with their Senior Agency Official for Privacy (SAOP) to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers Privacy Act requirements. b. The agency SHALL publish a System of Records Notice (SORN) to cover such collection, as applicable. c. The agency SHALL consult with their SAOP to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers E-Government Act of 2002 requirements. d. The agency SHALL publish a Privacy Impact Assessment (PIA) to cover such collection, as applicable. (4.2 #12) **SUPPLEMENTAL GUIDANCE**: This requirement applies to Federal agencies whether providing authentication services directly or through a commercial provider. This requirement directs Agencies to consult with their Senior Agency Official for Privacy (SAOP) and conduct an analysis to determine whether the collection of PII to issue or maintain authenticators triggers the requirements of the *Privacy Act of 1974* or the requirements of the *E-Government Act of 2002.* Based on this consultation and analysis, the agency may need to publish a System of Records Notice (SORN) and/or a Privacy Impact Assessment (PIA) to cover such collections, as applicable. While this requirement specifically applies only to federal agencies, CSPs that provide services to federal agencies may be expected to provide information about their identity services in support of an Agency's privacy analysis and PIA.

	ASSESSMENT OBJECTIVE: confirm that the agency offering or using the identity proofing service has: ● consulted with its SAOP to determine if the service is subject to the Privacy Act of 1974 and/or the E-Government Act of 2002 and, if applicable; ● published a SORN and/or PIA. ***POTENTIAL ASSESSMENT METHODS AND OBJECTS****:* ***For Federal Agencies Only****:* *If an agency's SAOP determines that the identity proofing services is subject to Privacy Act and/or E-Government Act of 2002 requirements:* **Examine**: the agency's *System of Records Notice (SORN)* and/or *Privacy Impact Assessment (PIA)*, as applicable.

GEN-14	**REQUIREMENT**: An enrollment code SHALL be comprised of one of the following: 1. Minimally, a random six character alphanumeric or equivalent entropy. For example, a code generated using an approved random number generator or a serial number for a physical hardware authenticator; OR 2. A machine-readable optical label, such as a QR Code, that contains data of similar or higher entropy as a random six character alphanumeric. (4.6) **SUPPLEMENTAL GUIDANCE**: The use of an enrollment code for address confirmation is a requirement for IAL2 remote identity proofing and enrollment. CSPs that perform in-person identity at IAL2 and IAL3 may voluntarily choose to use enrollment codes for such binding, but this is not required. Enrollment codes may also be used for in-person proofing and enrollment processes if an authenticator(s) is not registered to the subscribers' account at the time of in-person identity proofing and, therefore, the authenticator binding would need to occur at a later time. Enrollment codes may be used for authenticator binding to subscribers' accounts in such circumstances. Enrollment code use for IAL2 remote identity proofing allows the CSP to confirms that the applicant controls a validated address of record. Authenticator binding may not be completed in the same session for in-person identity proofing. Enrollment codes may be used for binding an authenticator to subscribers' accounts at a later time in such circumstances. The requirements presented in this criterion apply to all enrollment codes that may be used by the CSP for any purpose.

	Enrollment code use has the additional requirement for code validity periods. The validity period is determined by the type of address where the enrollment code is sent, as follows: ● 10 days, when sent to a postal address of record within the contiguous United States; ● 30 days, when sent to a postal address of record outside the contiguous United States; ● 10 minutes, when sent to a telephone of record (SMS or voice); ● 24 hours, when sent to an email address of record; ● 7 days if provided directly to the applicant during an in-person proofing session for authenticator binding at IAL2 or IAL3. These validity periods are presented again in conformance criterion IAL2-8c which presents the mandatory requirement for enrollment code confirmation for IAL2 remote identity proofing. **ASSESSMENT OBJECTIVE:** determine if a CSP uses enrollment codes in its identity proofing process and, if so, confirm the enrollment codes are comprised of *one* of the following: 1. Minimally, a random six character alphanumeric or equivalent entropy. For example, a code generated using an approved random number generator or a serial number for a physical hardware authenticator; or 2. A machine-readable optical label, such as a QR Code, that contains data of similar or higher entropy as a random six character alphanumeric. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: one or both of the following: ● the CSP's *systems documentation* that provides the technical specifications for creating enrollment codes, and/or; ● an actual *example of an enrollment code* that would be sent to an applicant.

GEN-15	**REQUIREMENT**: Training requirements for personnel validating evidence SHALL be based on the policies, guidelines, or requirements of the CSP or RP. (5.2) **SUPPLEMENTAL GUIDANCE**: The training requirement presented in section 5.2 pertains to personnel performing the validation of identity evidence but does not specify training content. The CSP policies, guidelines, or

	requirements for validating identity evidence for identity proofing would be appropriate for the type of training intended by this requirement. Such content may include: ● the CSP's policy for types of evidence it collects and validates in order to meet the requirements of designated IALs; ● validation of security features for the types of identity evidence collected; ● detection of evidence alteration, falsification, or forgery for the types of identity evidence collected. Procedures for the validation of identity evidence information with issuing and authoritative sources. This training may be accomplished through written training material, oral instruction, on-the-job training and mentoring, or other means. CSPs may perform some of the requirements for identity evidence validation through automated services and equipment. Therefore, personnel training would be based on the CSPs policies and procedures for the manual performance of evidence validation. **ASSESSMENT OBJECTIVE:** Determination that the CSP provides training to personnel performing identity evidence validation, consistent with its policies, procedures, or requirements. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSPs *documented policies and procedures* to determine its requirements for training personnel who validate evidence; or **Interview**: CSP management personnel to determine that it trains personnel who validate evidence according to the CSP's policies, guidelines, or requirements.

GEN-16	*This criterion applies to CSPs that provide identity proofing and enrollment services to minors (under the age of 18):* **REQUIREMENT**: If the *CSP provides identity proofing and enrollment services to minors (under the age of 18), then…*the CSP SHALL give special consideration to the legal restrictions of interacting with minors unable to meet the evidence requirements of identity proofing [to ensure compliance with the Children's Online Privacy Protection Act of 1998 (COPPA), and other laws, as applicable]. (5.3.4.1 #1) **SUPPLEMENTAL GUIDANCE**: In general, minors will not possess the types of evidence required to meet the CSP's minimum requirements for a given IAL. ICSPs that provide identity services to minors will need to determine and document the special considerations it applies to minors. Such special

	considerations may include the use of trusted referees and an expanded list of acceptable evidence types to include evidence a minor would likely possess, such as school IDs. **ASSESSMENT OBJECTIVE:** If the CSP interacts with minors, confirm it gives special considerations to minors who are unable to meet the evidence requirements. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: *If the CSP provides identity proofing and enrollment services to minors:* **Examine**: the CSP's *documented policies or procedures* to determine which special considerations it gives to minors who are unable to meet the evidence requirements for identity proofing.

GEN-17	*This criterion applies to CSPs that provide identity proofing and enrollment services to minors under the age of 13:* **REQUIREMENT**: If the *CSP provides identity proofing and enrollment services to minors under the age of 13, then…*minors under age 13 require additional special considerations under COPPA, and other laws, to which the CSP SHALL ensure compliance, as applicable. (5.3.4.1 #2) **SUPPLEMENTAL GUIDANCE**: COPPA [Children's Online Privacy Protection Rule] imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age. (Title 15 – U.S.C. §6501 – §6506) CSPs that provide identity services to minors under age 13 will need to determine and document the special considerations it applies to identity proofing and enrollment of minors under age 13. **ASSESSMENT OBJECTIVE:** If the CSP interacts with minors under the age of 13, confirm it complies with COPPA and other applicable laws. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: *If the CSP interacts with minors under the age of 13,* **Examine**: the CSP's *documented policies or procedures* to determine it complies with COPPA and other applicable laws.

Biometric Collection and Comparison

GEN-18 and GEN-19 address requirements associated with biometric collection for in-person identity proofing and enrollment at IAL2 and IAL3.

Biometric Collection:

For IAL3, biometric collection is mandatory for in-person and supervised remote identity proofing. During enrollment, biometrics may be collected for the purposes of biometric comparison used to verify the binding of identity evidence to the applicant. Additionally, biometrics may be collected and associated with the subscriber's identity account as an authentication factor for purposes of account recovery, re-proofing and non-repudiation.

SP 800-63A also allows for the optional collection of biometric characteristics s at IAL2 for the purpose of binding an authenticator to the subscribers' account as an authentication factor for account recovery, re-proofing and non-repudiation. Biometrics collection may also be performed at IAL2 if biometric comparison is used for verifying the binding of identity evidence to the applicant.

Biometrics collected as part of the identity proofing and enrollment processes may be stored (retained) as part of the subscriber's identity account and used for biometric comparison for re-proofing and account recovery at a later date.

GEN-18 and GEN-19 provide conformance assessment guidance for requirements associated with biometric collection and are applicable at both IALs 2 and 3.

GEN-18	***GEN-18 and GEN-19 apply to the collection of biometric characteristics for in-person (physical or supervised remote) identity proofing and are mandatory at IAL3. These criteria also apply to CSPs that optionally choose to collect biometric characteristics through in-person identity-proofing identity proofing and enrollment at IAL2.*** **REQUIREMENT**: The CSP SHALL have the operator view the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process. (5.3.3.1 #1) **SUPPLEMENTAL GUIDANCE**: Applicants may try to defraud the identity proofing process by using fake fingers or by applying non-natural materials - such as latex, silicon, or glue – to their fingers, faces, or other sources of biometrics. It is recommended that identity proofing operators be trained to recognize such practices and to examine all biometric sources used in the identity proofing for the presence of foreign materials. It is recommended that the CSP documents and applies technologies and procedures which ensure that the proofing operator reviews the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process.

	ASSESSMENT OBJECTIVE: Determine if the CSP provides in-person proofing (physical or supervised remote) and, if so, confirm proofing operators examine all biometric sources used in the identity proofing process for the presence of non-natural materials. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented processes* regarding the procedures remote proofing operators use to evaluate biometric sources for the presence of non-natural materials. **Interview:** *trained operators* to determine their procedures for examining biometric sources.

GEN-19	***GEN-18 and GEN-19 apply to the collection of biometric characteristics for in-person (physical or supervised remote) identity proofing and are mandatory at IAL3. These criteria also apply to CSPs that collect biometric characteristics through in-person identity-proofing identity proofing and enrollment at IAL2.*** **REQUIREMENT**: The CSP SHALL collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject. All biometric performance requirements in SP 800-63B, Section 5.2.3 apply. (5.3.3.1 #2) **SUPPLEMENTAL GUIDANCE**: Applicants may try to defraud the identity proofing process by having another person present themselves for biometric collection. The risk of this happening is increased if the identity proofing process is not completed in a single session and during supervised remote identity proofing processes. Documenting the technologies and procedures the CSP employs to ensure that biometric samples are taken from the applicant him/herself and not another person facilitates the assessment against this requirement. **ASSESSMENT OBJECTIVE:** Confirm the CSP has a procedure for ensuring biometric samples are taken from the applicant themselves and not from another person. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented processes* regarding the procedures the CSP employs to ensure biometric samples are taken from the intended applicant of the identity proofing process; or

	Interview: *trained operators* to determine their procedures for ensuring biometric samples are taken from the applicants themselves and not from another person.

4 IAL2

Component: IAL2 – Identity Proofing and/or Enrollment Services

In addition to those requirements presented in the General section of this document, the following requirements apply to all CSPs performing identity proofing and enrollment at IAL2.

IAL2-1	**REQUIREMENT**: The CSP SHALL support in-person or remote identity proofing, or both. (4.4.1.5) **SUPPLEMENTAL GUIDANCE**: IAL2 allows for remote or in-person identity proofing. IAL2 supports a wide range of acceptable identity proofing techniques in order to increase user adoption, decrease false negatives (legitimate applicants that cannot successfully complete identity proofing), and detect to the best extent possible the presentation of fraudulent identities by a malicious applicant. (SP 800-63A) Remote proofing presents challenges to achieving the desired outcomes described above that can be overcome through the use specific processes and technologies. Potential processes and controls that CSPs may employ to mitigate risks associated with remote identity proofing at IAL2 include: 1. A remote operator is present during at least part of the identity proofing session and can provide positive confirmation that the requirements for IAL2 identity proofing are met. Employing real-time remote operators provides the capability for the identity proofing process to be completed in a single session and allows the remote operator to direct the applicant for proper presentation and examination of identity evidence and biometrics collection. 2. The CSP employs automated technologies and services (e.g., liveness detection, identity evidence verification and validation, and presentation attack detection, if applicable) which can ensure the requirements for IAL2 identity proofing are met and protect against spoofing attacks. This process also provides the capability for the identity proofing process to be completed in a single session. 3. The CSP employs an off-line operator to evaluate the evidence and images collected during a previous identity proofing process. In this scenario, the identity proofing process requires more than one session with the applicant and is not completed until the operator provides a positive confirmation that all requirements for IAL2 identity proofing are met. **ASSESSMENT OBJECTIVE:** determine which options, from the list below, the CSPs employs and confirm it has documented its policies and practices relating to each of the supported options:

	● in-person identity proofing; ● remote identity proofing; ● supervised remote identity proofing; and/or, ● trusted referees. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: 1. **Examine**: the CSP's *documented polices* or *practices* to determine which type(s) of processes it employs to identity proof applicants to IAL2. 2. **Examine:** the CSP's *documented policies or practices* to confirm that the CSP identity proofs in accordance to the requirements for each type of identity proofing option it supports.

IAL2-2	**REQUIREMENT**: The CSP SHALL collect the following from the applicant: 1. One piece of SUPERIOR or STRONG evidence if the evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence and the CSP validates the evidence directly with the issuing source; OR 2. Two pieces of STRONG evidence; OR 3. One piece of STRONG evidence plus two pieces of FAIR evidence (4.4.1.2) **SUPPLEMENTAL GUIDANCE**: The goal of identity validation is to collect the most appropriate identity evidence (e.g., a passport or driver's license) from the applicant and determine its authenticity, validity, and accuracy. Identity validation is made up of three process steps: 1) collecting the appropriate identity evidence, 2) confirming the evidence is genuine and authentic, and 3) confirming the data contained on the identity evidence is valid, current, and related to a real-life subject. (5.2) Appendix B of this document presents notional strengths for types of evidence that may be presented for identity proofing purposes. Documenting the types and strengths of evidence the CSP collects for each proofing encounter demonstrates conformance for this requirement. (Also see GEN-8b.) Examples of methods and how they can be used to capture identity evidence images or extract data for validation include: ● Cameras to capture an images of identity evidence for the purposes of evidence validation;

	• Document scanner to capture images of identity evidence for the purpose of evidence validation; and • Bar-code scanner to capture and extract information from standardized barcodes embedded on identity evidence. High resolution images of at least 300 ppi are necessary for proper evidence examination and validation. **ASSESSMENT OBJECTIVE:** confirm the CSP's policy for identity evidence collection meets the identity evidence quality requirements (see NIST 800-63A, Section 5.2.1) for IAL2. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented policies or practices* to determine how the CSP meets the identity evidence quality requirements provided in NIST SP 800-63A, Section 5.2.1.

IAL2-3	**REQUIREMENT**: The CSP SHALL validate each piece of evidence with a process that can achieve the same strength as the evidence presented (see IAL2-3 above). For example, if two forms of STRONG identity evidence are presented, each piece of evidence will be validated at a strength of STRONG. (4.4.1.3) **SUPPLEMENTAL GUIDANCE**: The goal of identity validation is to collect the most appropriate identity evidence (e.g., a passport, driver's license) from the applicant and determine its authenticity, validity, and accuracy. Identity validation is made up of three process steps: 1) collect the appropriate identity evidence, 2) confirm the evidence is genuine and authentic, and 3) confirm the data contained on the identity evidence is valid, current, and related to a real-life subject. (5.2) Evidence validation for authenticity involves examining the evidence for: • Confirmation of required information completeness and format for the identity evidence type. • Detection of evidence tampering or the creation of counterfeit or fraudulent evidence. • Confirmation of security features. See Appendix C to this document for types of commonly used security features for identity evidence. Most of the capabilities to confirm security features on identity evidence are dependent upon physically viewing the evidence directly, tactile feel of the evidence, and viewing the evidence under specialized lighting or through the use

	of specialized equipment (see Appendix C). Therefore, the validation of evidence that may be submitted remotely for remote identity proofing methods is particularly challenging. For this reason, CSPs opting to provide remote identity proofing may find it most effective to use automated evidence validation products and services. If automated evidence validation solutions are not used, CSPs may choose to apply similar procedures for IAL2 remote proofing as are required for IAL3 supervised remote proofing. These procedures provide that a trained operator can remotely supervise the evidence collection process, require the applicant to turn or tilt evidence or apply lighting to be able to confirm security features on evidence that is presented for the identity proofing encounter in a recorded video or webcast. Alternatively, a CSP may use an automated interface for the capture of identity evidence images that similarly can direct the applicant to turn, tilt or provide lighting on evidence presented for identity proofing purposes. The next step in identity evidence validation for authenticity and integrity is to verify the correctness of information from the identity evidence against the issuing source for the evidence or an authoritative source that has linkage to the issuing source. Results of these checks for authenticity and integrity should be recorded. Table 5-2 in NIST SP 800-63A lists strengths, ranging from unacceptable to superior, of identity validation performed by the CSP to validate the evidence presented for the current proofing session and the information contained therein. **ASSESSMENT OBJECTIVE:** confirm the CSP's policy for identity evidence validation meets the identity evidence validation requirements (see SP 800-63A, Section 5.2.2) for IAL2. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented policies or practices* to determine how the CSP meets the identity evidence quality requirements provided in NIST SP 800-63A, Section 5.2.2; or **Examine**: the CSP's *enrollment records* or *system logs* to confirm the steps taken to validate identity evidence meet the identity evidence validation requirements.

IAL2-4a	**REQUIREMENT**: The CSP SHALL verify identity evidence as follows: 1. At a minimum, the applicant's binding to identity evidence must be verified by a process that is able to achieve a strength of STRONG. (4.4.1.4)

SUPPLEMENTAL GUIDANCE: The goal of identity verification is to confirm and establish a linkage between the validated evidence for the claimed identity and the real-life applicant presenting the evidence

The table below shows IAL2 verification methods.

Table: IAL2 Verification Methods and Strengths

Verification Strength	Verification Method	Description
Superior	Biometric Verification	Biometric comparison against biometric characteristics on the strongest piece(s) of evidence against live biometric capture for remote or in-person identity proofing. May be used for identity verification for FAIR, STRONG, and SUPERIOR strength.
Strong	In-Person Physical Verification	Physical comparison of applicant to facial-image photograph on strongest piece(s) of validated evidence. May be used for identity verification for FAIR and STRONG strength.
Strong	Remote Physical Verification	Physical comparison of applicant to facial-image photograph on strongest piece(s) of validated evidence. May be used for identity verification for FAIR and STRONG strength.

For IAL2 this linkage is achieved through a physical or biometric comparison of the facial image (i.e., photograph) on the strongest piece of evidence to the applicant or by a biometric comparison between information on the evidence and a biometric characteristic obtained from the applicant, most likely facial image.

Physical comparison is a comparison by a person (i.e., CSP-trained personnel) of the applicant to the photograph (i.e., facial image) on any of the strongest piece(s) of validated identity evidence collected. This comparison can be an in-person comparison for in-person identity proofing processes or may be conducted remotely for remote identity proofing. In both cases, the operator must perform a physical comparison of the applicant to the facial image photograph on the evidence. That is, the in-person proofing personnel will physically compare the facial image of the live applicant to the facial image photograph on the strongest piece of validated evidence. For remote physical comparison, the applicants' facial image may be captured by high resolution

	video or camera for physical comparison to the facial image photograph on the identity evidence. For identity proofing verification, biometric comparison is an automated comparison of a biometric characteristic recorded on the strongest piece of identity evidence compared to the corresponding biometric characteristic of the applicant captured live during the identity proofing session Remote identity proofing requires the collection of both an image of the identity evidence and a live capture of the facial image of the applicant for physical or biometric comparison. The CSP must employ liveness and presentation attack detection capabilities to ensure that the applicant's facial image or other biometric characteristic used for comparison is "live" and not a spoofing or presentation attack. Potential methods for remote identity proofing processes to mitigate such spoofing and presentation attacks are presented below. ● A remote operator is present during the identity proofing session (similar to supervised remote in-person proofing) and can conduct a real-time physical comparison between an image of the identity evidence and a live video of the applicant. In order to confirm the video stream is live and not pre-recorded, the Operator could direct the applicant to move their head in specific ways, or even ask the applicant a question. Once a positive confirmation is recorded from the operator, and all other requirements are met, the identity proofing can be completed in a single session. ● The CSP employs automated capabilities which are specifically designed to compare the image of the identity evidence with the applicant, and which also employ liveness detection technologies. Pending a positive confirmation from the automated comparison, and the satisfaction of all other requirements, the identity proofing can be completed in a single session. ● The CSP employs liveness detection technology during the capture of the facial image, and an off-line operator performs the physical comparison of images captured during the identity proofing session. The identity proofing process requires more than one session with the applicant and is not completed until the operator provides a positive confirmation of the comparison and the other requirements are met. **ASSESSMENT OBJECTIVE:** confirm the CSP's identity system records an operator's determination as to the verification of the applicant's binding to the identity evidence. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: a sample *enrollment record* or *audit log* to confirm the CSP's identity system records the results of evidence verification process for each applicant.

IAL2-4b	*For IAL2 remote proofing:* **REQUIREMENT**: The collection of biometric characteristics for physical or biometric comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity] performed remotely SHALL adhere to all requirements as specified in SP 800-63B, Section 5.2.3. (5.3.1) **SUPPLEMENTAL GUIDANCE**: See SP 800-63B conformance criteria BIO 1 – 12 for conformance criteria for the implementation and conformance assessment of requirements of SP 800-63B section 5.2.3. **ASSESSMENT OBJECTIVE:** For the collection and comparison of biometric characteristics, including facial image, for identity verification at IAL2, confirm that the CSP conducts a physical or biometric comparison of the applicant to identity evidence in accordance with applicable requirements in SP 900-63B, Section 5.2.3. See SP 800-63B conformance criteria BIO- 1 – 12 for supplemental guidance. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSPs *documented policies* or *system documentation* to determine its procedures for the collection of biometric characteristics for physical and biometric comparison of the applicant to identity evidence.

IAL2-5	**REQUIREMENT**: 2. Knowledge-based verification (KBV) SHALL NOT be used for in-person (physical or supervised remote) identity verification. (4.4.1.4) **SUPPLEMENTAL GUIDANCE**: identity verification is performed against the strongest piece of identity evidence submitted and validated. For IAL2 the strongest piece of evidence will always be either STRONG or SUPERIOR evidence. KBV (sometimes referred to as knowledge-based authentication) is only permitted as a verification method for evidence at the FAIR strength level; therefore, verification of FAIR evidence binding will never be required for IAL2. (SP 800-63A, Section 5.1 #2) **ASSESSMENT OBJECTIVE:** Confirm that the CSP does not use KBV as an identity verification method for in-person identity verification. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented policies or practices* to determine it does not use KBV for in-person (physical or supervised remote) identity verification.

IAL2-6a	**REQUIREMENT**: The CSP SHALL confirm address of record. (4.4.1.6 #2) **SUPPLEMENTAL GUIDANCE**: Valid records to confirm address are issuing source(s) or authoritative source(s). Ideally, the CSP will confirm an address of record through validation of the address contained on any supplied, valid piece of identity evidence. However, the CSP may confirm address of record by validating information supplied by the applicant that is not contained on any supplied piece of identity evidence. Postal addresses are preferred, however these guidelines support any type of address that can be validated against an issuing or authoritative source, whether physical or digital. Acceptable addresses of record include postal addresses, email addresses, and telephone numbers. The types of addresses of record a CSP accepts will determine, in part, the method it employs to validate them. For instance, postal addresses can be validated by confirming it against a piece of supplied, valid identity evidence. Email addresses may be confirmed by sending an email to the provided address. **ASSESSMENT OBJECTIVE:** determine the following: 1. the type(s) of addresses the CSP confirms as part of its identity proofing and enrollment process; and 2. the specific method(s) the CSP uses to confirm these addresses of record. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented processes* regarding: 1. the types of addresses of record it confirms; and 2. its method for confirming addresses of record. **Interview:** *trained personnel* regarding: 1. the types of addresses of record it confirms; and 2. its method for confirming addresses of record.

IAL2-6b	**REQUIREMENTS**: Valid records to confirm address SHALL be issuing source(s) or authoritative source(s). (4.4.1.6 #1) Self-asserted address data that has not been confirmed in records SHALL NOT be used for confirmation. (4.4.1.6 #3)

	SUPPLEMENTAL GUIDANCE: An address of record is a "validated and verified location (physical or digital) where an individual can receive communications using approved mechanisms." (Definitions, 800-63-3) IAL2 requires confirming an applicant's address of record. SP 800-63A allows this to be accomplished in two ways: 1) validation of the address contained on a valid piece of identity evidence, or 2) by employing a mechanism such as enrollment codes to validate an address not contained on a supplied piece of identity evidence. Addresses that are supplied by an applicant, either verbally or on a non-valid piece of identity evidence, are not valid for confirming an applicant's address of record. **ASSESSMENT OBJECTIVES:** 1. when confirming address of record using supplied identity evidence, verify the CSP only considers valid records, and 2. confirm the CSP does not accept self-asserted addresses. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented polices* or *practices* to determine processes used to confirm address, and **Examine**: *enrollment records* or *system logs* to determine that only validated and confirmed addresses are accepted.

IAL2-7	***Note that IAL2-7 applies only to in-person proofing at IAL2.*** **REQUIREMENT**: *If the CSP performs in-person proofing for IAL2 and provides an enrollment code directly to the subscriber for binding to an authenticator at a later time, then the enrollment code*…SHALL be valid for a maximum of 7 days. (4.4.1.6 #4.c) **SUPPLEMENTAL GUIDANCE**: Upon successful completion of the identity proofing process the CSP will typically register one or more authenticators to the subscribers' account or may optionally choose to bind an authenticator(s) at a later time. If the CSP chooses to use an enrollment code provided directly to the applicant to authenticate for such later binding, the validity period for the enrollment code is a maximum of seven days (see SP 800-63A conformance criterion GEN -14). **ASSESSMENT OBJECTIVE:** If the CSP offers in-person identity proofing at IAL2, determine if the CSP provides an enrollment code directly to the

	subscriber for subsequent authenticator binding and, if so, confirm the enrollment code is valid for a maximum of seven (7) days. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: CSP's *documentation* for authenticator binding for in-person at enrollment processes to determine whether t enrollment codes provided directly to subscribers for subsequent authenticator binding are valid for a maximum of seven (7) days.

IAL2-8a	***Note that conformance criteria IAL2-8a through IAL2-8e apply to remote identity proofing processes at IAL2.*** *For remote identity proofing at IAL2:* **REQUIREMENT**: The CSP SHALL send an enrollment code to a confirmed address of record for the applicant. (4.4.1.6 #5.a) **SUPPLEMENTAL GUIDANCE**: Enrollment codes used for IAL2 remote identity proofing may be sent to any confirmed address of record – postal, mobile phone number for SMS, or email addresses. **ASSESSMENT OBJECTIVES:** when conducting remote identity proofing for IAL2, confirm the CSP: 1. sends enrollment codes; and 2. only sends enrollment codes to confirmed addresses, as determined by IAL2-6a and IAL2-6b above. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: *enrollment records* or *system logs* to determine that enrollment codes are only sent to confirmed addresses of record.

IAL2-8b	*For remote identity proofing at IAL2:* **REQUIREMENT**: The applicant SHALL present a valid enrollment code to complete the identity proofing process. (4.4.1.6 #5.b) **SUPPLEMENTAL GUIDANCE**: Per IAL2-8a above, sending an enrollment code to a confirmed address of record, as captured during the identity proofing process, is required to complete the remote identity proofing process and provides additional confidence in the binding of that address to the applicant.

	Valid enrollment codes mean that the correct enrollment code is submitted by the applicant within prescribed validity periods. Enrollment code validity periods depend on the type of address where the code is sent as shown in IAL2-8c below. Information captured in the CSP's enrollment records or system logs facilitate assessment against this requirement. Ideally, this information would include details about the validity of the enrollment code (date and time applicant entered code; confirmation it was the correct code; and confirmation it was not expired). **ASSESSMENT OBJECTIVE:** confirm the remote identity proofing process at IAL2 cannot be completed until the applicant presents a valid enrollment code. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: *enrollment records* or *system logs* to confirm applicants cannot complete the identity proofing process without presenting a valid enrollment code.

IAL2-8c	***Note that the following enrollment code validity periods apply to enrollment codes sent to confirmed addresses of record for IAL2 remote in-person proofing only.*** **REQUIREMENT**: Enrollment codes shall have the following maximum validities: (4.4.1.6 #5.e): i. 10 days, when sent to a postal address of record within the contiguous United States; ii. 30 days, when sent to a postal address of record outside the contiguous United States; iii. 10 minutes, when sent to a telephone of record (SMS or voice); iv. 24 hours, when sent to an email address of record. (4.4.1.6 #5) **SUPPLEMENTAL GUIDANCE**: Enrollment codes sent to addresses of record are only valid for a limited amount of time, depending on the type of address of record to which they are sent. Applicants that present enrollment codes that are no longer valid (aka, expired) cannot use this code to complete their identity proofing process. **ASSESSMENT OBJECTIVE:** confirm that the CSP: ● limits the amount of time an enrollment code is valid, based on the type of address of record to which it was sent; and ● does not accept an invalid enrollment code to complete the identity proofing process.

	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: one of the following: ● the CSP's *documented policy* for enrollment code maximum validity times; and, ● the *system's functionality* to confirm that invalid enrollment codes cannot be used to complete the identity proofing process. ● enrollment records to determine proper enrollment code confirmation. **Interview:** *trained personnel* to confirm that: ● enrollment codes have a maximum validity, based on the type of address of record to which they are sent; and, ● invalid enrollment codes cannot be used to complete the identity proofing process.

IAL2-8d	*If the enrollment code sent to the confirmed address of record as part of the remote identity proofing at IAL2 is also intended to be an authentication factor,* a. **REQUIREMENT**: (*If the enrollment code sent to the confirmed address of record as part of the remote identity proofing process at IAL2 is also intended to be an authentication factor,* then…it SHALL be reset upon first use. (4.4.1.6 #5.d) **SUPPLEMENTAL GUIDANCE**: Enrollment codes sent as an authentication factor for address confirmation may only be used once. **ASSESSMENT OBJECTIVE:** determine if the CSP intends for an enrollment code to be used as an authentication factor and, if so, confirm that is only used once. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: one or both of the following: ● the CSP's *documented processes* for use of enrollment codes used as an authentication factor that an enrollment code can only be used once; or ● the *system's functionality* to confirm that an enrollment code may only be used once to confirm address for enrollment.

IAL2-8e	*If the CSP performs remote proofing at IAL2, and optionally sends* ***notification of proofing in addition to sending the required enrollment code***

	a. **REQUIREMENT**: *If the CSP performs remote proofing at IAL2 and optionally sends* ***notification of proofing in addition to sending the required enrollment code, then…***The CSP SHALL ensure the enrollment code and notification of proofing are sent to different addresses of record. (4.4.1.6 #5.f) **SUPPLEMENTAL GUIDANCE**: For example, if the CSP sends an enrollment code to a phone number validated in records, a proofing notification may be sent to the postal address validated in records or obtained from validated and verified evidence, such as a driver's license. **ASSESSMENT OBJECTIVE:** if the CSP optionally sends a notification of proofing to applicants in addition to the required enrollment code for IAL@ remote identity proofing, confirm that the CSP uses a different address than the one used for enrollment codes. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSPs *enrollment records or system logs* for confirmation it sends enrollment codes and, if used, notifications of proofing to different addresses of record for IAL2 remote identity proofing.

IAL2-9	**REQUIREMENTS**: The CSP SHALL employ appropriately tailored security controls, to include control enhancements, from the moderate or high baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standard. The CSP SHALL ensure that the minimum assurance-related controls for moderate-impact systems or equivalent are satisfied. (4.4.1.8) **SUPPLEMENTAL GUIDANCE**: NIST SP 800-53 provides a comprehensive catalog of controls, three security control baselines (low, moderate, and high impact), and guidance for tailoring the appropriate baseline to specific needs and risk environments for federal information systems. These controls are the operational, technical, and management safeguards to maintain the integrity, confidentiality, and security of federal information systems and are intended to be used in conjunction with the NIST risk management framework outlined in SP 800-37 and SP 800-63-3 section 5, Digital Identity Risk Management. NIST SP 800-53 presents security control baselines determined by the security categorization of the information system (low, moderate or high) from NIST FIPS 199 Standards for Security Categorization of Federal Information and Information Systems. For IAL2, the moderate baseline controls (see https://nvd.nist.gov/800-53/Rev4/impact/moderate) may be considered the starting point for the selection, enhancement, and tailoring of the security controls presented. Guidance on tailoring the control baselines to best meet the

	organization's risk environment, systems and operations is presented in SP 800-53 section 3.2. Tailoring Baseline Security Controls. While SP 800-53 and other NIST Special Publications in the SP-800-XXX series apply to federal agencies for the implementation of the Federal information Security Modernization (Management) Act (FISMA), non-federal entities providing services for federal information systems may also need to demonstrate appropriate controls and should similarly use SP 800-53 and associated publications as resources. Non-federal entities may be subject to and conformant with other applicable controls systems and processes for information system security (e.g., FEDRAMP, ISO/IEC 27001). SP800-63A allows the application of equivalent controls from such standards and processes to meet conformance with this criterion. **ASSESSMENT OBJECTIVES:** 1. confirm the CSP employs appropriately tailored security controls to include control enhancements, from the moderate or high baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standard. 2. confirm the CSP has satisfied the minimum assurance-related controls for moderate-impact systems or equivalent. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: 1. **Examine**: the CSPs *documentation* to determine it employs appropriately tailored security controls to include control enhancements, from the moderate or high baseline of security controls defined in SP 800-53 or equivalent federal process (such as FEDRAMP) or industry standard; and; 2. **Examine:** the CSPs documentation to determine it has satisfied the minimum assurance-related controls for moderate-impact systems or equivalent. Such documentation may include: ● Determination of Authorization to Operate (ATO) for the IAL2 identity system and operations; ● Digital Identity Acceptance Statement for IAL2 in accordance with SP 800-63-3 section 5.5 Digital Identity Acceptance Statement; ● Documentation of organizational risk management policies and procedures consistent with NIST SP 800-37 and SP 800-53 moderate and high impact controls or appropriate equivalent.

5 IAL3

Component: IAL3 – Identity Proofing and/or Enrollment Services

In addition to those requirements presented in the General section of this document, CSPs that provide identity proofing and/or enrollment services at IAL3 must demonstrate conformance to the following requirements.

IAL3-1	**REQUIREMENT**: Collection of PII SHALL be limited to the minimum necessary to resolve to a unique identity record. (4.5.1) *Note: This is the same conformance criterion and requirement as presented in GEN – 2. It is included here for completeness and does not represent a separate or different criterion.* **SUPPLEMENTAL GUIDANCE**: The goal of identity resolution is to uniquely distinguish an individual within a given population or context. Effective identity resolution uses the smallest set of attributes necessary to resolve to a unique individual. It provides the CSP an important starting point in the overall identity proofing process, to include the initial detection of potential fraud, but in no way represents a complete and successful identity proofing transaction. This may include attributes that correlate identity evidence to authoritative sources and to provide RPs with attributes used to make authorization decisions. There may be many different sets that suffice as the minimum, so it is recommended that CSPs choose this set to balance privacy and the user's usability needs, as well as the likely attributes needed in future uses of the digital identity. Examples of attributes that may be used for minimum identity attribute sets include: • Name (first, last. middle) with combinations and variations, • Address (#, Street, City, County, State, Zip code) with combinations and variations, • Date of birth (DDMMYYYY) with combinations and variations, • Email address, • Phone number. For population sets that are more defined than the general U.S. population (e.g., military veterans, Native Americans), these minimum attribute sets may be tailored to that specific community.

	Additionally, it is recommended that CSPs document which alternative attributes it will accept in cases where an applicant cannot provide the minimum necessary attributes (e.g., applicant does not have a home address or phone number). **ASSESSMENT OBJECTIVE:** Confirm the CSP limits the amount of PII it collects to the minimum amount required to resolve to a unique identity in a given context. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine:** the CSP's *documented policies or practices* to determine the minimum set of PII required by the CSP to achieve identity resolution.

IAL3-2	**REQUIREMENT**: The CSP SHALL collect the following from the applicant: 1. Two pieces of SUPERIOR evidence; OR 2. One piece of SUPERIOR evidence and one piece of STRONG evidence if the issuing source of the STRONG evidence, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence and the CSP validates the evidence directly with the issuing source; OR 3. Two pieces of STRONG evidence plus one piece of FAIR evidence. (4.5.2) **SUPPLEMENTAL GUIDANCE**: The goal of identity validation is to collect the most appropriate identity evidence (e.g., a passport or driver's license) from the applicant and determine its authenticity, validity, and accuracy. Identity validation is made up of three process steps: 1) collecting the appropriate identity evidence, 2) confirming the evidence is genuine and authentic, and 3) confirming the data contained on the identity evidence is valid, current, and related to a real-life subject. (5.2) Appendix B of this document provides a list of notional strength of evidence types that may be submitted for IAL3 identity proofing. Documenting the types of evidence the CSP collects facilitates the conformance assessment against this requirement. Methods of evidence collection/capture will depend on the type of evidence the CSPs require and the types of devices to which the CSP can reasonably consider its applicants will have access. Examples of methods and how they can be used to capture identity evidences include: ● Cameras to capture the applicant's photo or an image of the identity evidence;

	• Scanners to capture documents, which can then be compared against a known template by automated software to extract information (OCR); and • Commercial off-the-shelf bar code scanners that can capture and extract information from standardized barcodes embedded on identity evidence. **ASSESSMENT OBJECTIVE:** confirm the CSP's policy for identity evidence collection meets the identity evidence quality requirements (see NIST 800-63A, Section 5.2.1) for IAL3. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented policies or practices* to determine how the CSP meets the identity evidence quality requirements provided in NIST SP 800-63A, Section 5.2.1.

IAL3-3	**REQUIREMENT**: The CSP SHALL validate identity evidence as follows: Each piece of evidence must be validated with a process that is able to achieve the same strength as the evidence presented. For example, if two forms of STRONG identity evidence are presented, each piece of evidence will be validated at a strength of STRONG. (4.5.3) **SUPPLEMENTAL GUIDANCE**: The goal of identity validation is to collect the most appropriate identity evidence (e.g., a passport, driver's license) from the applicant and determine its authenticity, validity, and accuracy. Identity validation is made up of three process steps: 1) collecting the appropriate identity evidence, 2) confirming the evidence is genuine and authentic, and 3) confirming the data contained on the identity evidence is valid, current, and related to a real-life subject. (5.2) Evidence validation for authenticity involves examining the evidence for: • Confirmation of required information completeness and format for the identity evidence type. • Detection of evidence tampering or the creation of counterfeit or fraudulent evidence. • Confirmation of security features. See Appendix C to this document for types of commonly used security features for identity evidence. The capabilities to confirm security features on identity evidence are dependent upon physically viewing the evidence directly, tactile feel of the evidence, and viewing the evidence under specialized lighting or through the use of specialized equipment (see Appendix C). These checks for authenticity can also be performed by automated identity evidence validation equipment and services.

	The next step in identity evidence validation for authenticity and integrity is to verify the correctness of information from the identity evidence against the issuing source for the evidence or an authoritative source that has linkage to the issuing source. Results of these checks for authenticity and integrity should be recorded. Table 5-2 in NIST SP 800-63A lists strengths, ranging from unacceptable to superior, of identity validation performed by the CSP to validate the evidence presented for the current proofing session and the information contained therein. **ASSESSMENT OBJECTIVE:** confirm the CSP's policy for identity evidence validation meets the identity evidence validation requirements (see SP 800-63A, Section 5.2.2) for IAL3. **Examine**: the CSP's *documented policies or practices* to determine how the CSP meets the identity evidence quality requirements provided in NIST SP 800-63A, Section 5.2.2; or **Examine**: the CSP's *enrollment records* or *system logs* to confirm the steps taken to validate identity evidence meet the identity evidence validation requirements.

IAL3-4	**REQUIREMENT**: The CSP SHALL verify identity evidence as follows: 1. At a minimum, the applicant's binding to identity evidence must be verified by a process that is able to achieve a strength of SUPERIOR. 2. KBV SHALL NOT be used for in-person (physical or supervised remote) identity verification. (4.5.4) **SUPPLEMENTAL GUIDANCE**: The goal of identity verification is to confirm and establish a linkage between the claimed identity and the real-life applicant presenting the evidence. (SP 800-63A, Section 5.3) The applicant's ownership of the claimed identity has been confirmed by matching the applicant to the strongest piece of identity evidence collected to support the claimed identity (e.g., driver's license, passport). The strongest piece of evidence for IAL3 must be at the SUPERIOR level. Therefore, the linkage of the applicant to the evidence must be verified at the SUPERIOR level. For IAL3, this linkage is achieved through a biometric comparison of the facial image (i.e., photograph) or other biometric modality on the strongest piece of evidence to a corresponding biometric characteristic captured live from the applicant during the in-person proofing session. IAL3 identity verification methods are shown in the table below.

	A physical comparison is a comparison by a person (i.e., CSP trained operator) of the applicant to a photograph (i.e., facial image) from the strongest identity evidence collected. The operator performs a physical comparison of the in-person applicant to the photograph on the evidence. A biometric comparison is an automated comparison of biometric modalities present on the strongest piece of identity evidence to corresponding biometric modalities of the applicant captured during the identity proofing session. Identity verification is performed against the strongest piece of identity evidence submitted and validated. For IAL3 the strongest piece of evidence will always be either STRONG or SUPERIOR evidence. KBV (sometimes referred to as knowledge-based authentication) is only permitted as a verification method for evidence at the FAIR strength level; therefore, verification of FAIR evidence binding will never be required for IAL3 **ASSESSMENT OBJECTIVES:** 1. confirm the CSP's identity system records the method and determination of the verification of the applicant's binding to the identity evidence; and 2. confirm the CSP does not use KBV for in-person identity verification. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: a sample *enrollment record* or *audit log* to confirm the CSP's identity management system records the results of evidence verification process for each applicant; and **Examine**: system documentation to confirm the CSP does not use KBV for identity verification.

IAL3-5	**REQUIREMENT**: The CSP SHALL perform all identity proofing steps with the applicant in-person. (4.5.5) **SUPPLEMENTAL GUIDANCE**: IAL3 adds additional rigor to the steps required at IAL2, to include providing further evidence of superior strength, and is subject to additional and specific processes (including the use of biometrics) to further protect the identity and RP from impersonation, fraud, or other significantly harmful damages. Biometrics are used to detect fraudulent enrollments, duplicate enrollments, and as a mechanism to re-establish binding to a credential. In addition, identity proofing at IAL3 is performed in-person (to include supervised remote). See Section 5.3.3 for more details. (4.5) NIST SP 800-63A identifies two types of acceptable proofing options:

	• in-person identity proofing, where the applicant and the system operator are physically present at the same location at the same time, and • supervised remote identity proofing, where the applicant interacts with the system operator via a remote connection at the same time. CSPs may employ one or both of these methods to identity proof applicants to IAL3. **ASSESSMENT OBJECTIVE:** determine which options, from the list below, the CSPs employs and confirm it has documented its policies and practices relating to each of the supported options: • in-person identity proofing; and/or, • supervised remote identity proofing. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented polices* or *practices* to determine which type(s) of processes it employs to identity proof applicants to IAL2. **Examine:** the CSP's *documented policies or practices* to confirm that the CSP identity proofs in accordance to the requirements for each type of identity proofing option it supports.

IAL3-6	**REQUIREMENT**: 1. The CSP SHALL confirm address of record. (4.5.6) 2. Self-asserted address data SHALL NOT be used for confirmation. (4.5.6) **SUPPLEMENTAL GUIDANCE**: Valid records to confirm address are issuing source(s) or authoritative source(s). Acceptable addresses of record include postal addresses, email addresses, and telephone numbers. The types of addresses of record a CSP accepts will determine, in part, the method it employs to validate them. For instance, postal addresses can be validated by confirming it against a piece of supplied, valid identity evidence. Email addresses may be confirmed by sending an email to the provided address. Addresses that are supplied by an applicant, either verbally or on a non-validated piece of identity evidence, are not valid for confirming an applicant's address of record. **ASSESSMENT OBJECTIVE:** determine the following: 1. the type(s) of addresses the CSP confirms as part of its identity proofing and enrollment process; and

	2. the specific method(s) the CSP uses to confirm these addresses of record. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented polices* or *practices* to determine what it considers valid records to confirm addresses; and **Examine**: *enrollment records* or *system logs* to determine that only validated and confirmed addresses are accepted.

IAL3-7	**REQUIREMENT**: A notification of proofing SHALL be sent to the confirmed address of record. (4.5.6.3) **SUPPLEMENTAL GUIDANCE**: In order to reduce the risk of a person fraudulently being enrolled into the CSP's identity service, CSPs are required to notify applicants, using the confirmed address of record, that an in-person IAL3 identity proofing event has been completed in their name. The method of notification will be appropriate to the confirmed address(es) of record permitted by the CSP. **ASSESSMENT OBJECTIVE:** Confirm that the CSP sends a notification of proofing to the applicant's address of record. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine:** one or both of the following: ● *enrollment records* or *system logs* to determine that notification of proofing is sent to applicants' confirmed addresses of record; or ● the CSP's *documented polices* or *practices* to determine that it sends notification or proofing to applicants' confirmed address of record.

IAL3-8	*If the CSP provides an enrollment code directly to the subscriber (for binding to an authenticator at a later time):* **REQUIREMENT**: *If the CSP provides an enrollment code directly to the subscriber (for binding to an authenticator at a later time) …*The enrollment code SHALL be valid for a maximum of 7 days. (4.5.6.4) **SUPPLEMENTAL GUIDANCE**: Upon successful completion of the identity proofing process – and during the same, in-person session - the CSP may optionally provide an enrollment code directly to the applicant for binding an authenticator(s) to the subscribers' account at a later time. For as long as it is

	valid, the enrollment code allows the subscriber to bind one or more authenticators to the identity record created during the in-person identity proofing session. **ASSESSMENT OBJECTIVE:** determine if the CSP provides an enrollment code directly to the subscriber and, if so, confirm the enrollment code is valid for a maximum of seven (7) days. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: ● **Examine**: CSP's *documentation* for the specification that enrollment codes provided directly to subscribers are valid for a maximum of seven (7) days on its enrollment codes.

IAL3-9	**REQUIREMENTS**: The CSP SHALL employ appropriately tailored security controls, to include control enhancements, from the high baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standard. (4.5.8) The CSP SHALL ensure that the minimum assurance-related controls for high-impact systems or equivalent are satisfied. (4.5.8) **SUPPLEMENTAL GUIDANCE**: NIST SP 800-53 provides a comprehensive catalog of controls, three security control baselines (low, moderate, and high impact), and guidance for tailoring the appropriate baseline to specific needs and risk environments for federal information systems. These controls are the operational, technical, and management safeguards to maintain the integrity, confidentiality, and security of federal information systems and are intended to be used in conjunction with the NIST risk management framework outlined in SP 800-37 and SP 800-63-3 section 5 Digital Identity Risk Management. NIST SP 800-53 presents security control baselines determined by the security categorization of the information system (low, moderate or high) from NIST FIPS 199 Standards for Security Categorization of Federal Information and Information Systems. For IAL3 the high baseline controls (see https://nvd.nist.gov/800-53/Rev4/impact/high) may be considered the starting point for the selection, enhancement, and tailoring of the security controls presented. Guidance on tailoring the control baselines to best meet the organization's risk environment, systems and operations is presented in SP 800-53 section 3.2. Tailoring Baseline Security Controls. While SP 800-53 and other NIST Special Publications in the SP-800-XXX series apply to federal agencies for the implementation of the Federal Information Security Modernization Act (FISMA), non-federal entities providing services for federal information services also are subject to FISMA and should similarly use SP 800-53 and associated publications for appropriate controls. Non-federal entities may be subject to and conformant with other

	applicable controls systems and processes for information system security (e.g., FEDRAMP, ISO/IEC 27001). SP 800-63A allows the application of equivalent controls from such standards and processes to meet conformance with this criterion. **ASSESSMENT OBJECTIVES:** 1. confirm the CSP employs appropriately tailored security controls to include control enhancements, from the high baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standard. 2. confirm the CSP has satisfied the minimum assurance-related controls for high-impact systems or equivalent. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: 1. **Examine**: the CSPs *documentation* to determine it employs appropriately tailored security controls to include control enhancements, from the high baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standard; and 2. **Examine:** the CSPs documentation to determine it has satisfied the minimum assurance-related controls for high-impact systems or equivalent. Such documentation may include: ● Determination of Authorization to Operate (ATO) for the IAL3 identity system and operations; ● Digital Identity Acceptance Statement for IAL3 in accordance with SP 800-63-3 section 5.5 Digital Identity Acceptance Statement; ● Documentation of organizational risk management policies and procedures consistent with NIST SP 800-37 and SP 800-53 high impact controls or appropriate equivalent.

IAL3-10	*For IAL3 in-person (physical or supervised remote) enrollment:* **REQUIREMENT**: The CSP SHALL collect and record a biometric sample at the time of proofing (e.g., facial image, fingerprints) for the purposes of non-repudiation and re-proofing. (4.5.7) **SUPPLEMENTAL GUIDANCE**: A biometric sample collected from the applicant at the time of identity proofing, and subsequently associated with their identity account, serves several purposes, including non-repudiation, re-proofing, account recovery and allowing for the later binding of an authenticator to the identity account. The collection and recording of a biometric characteristic for these purposes during identity proofing and enrollment is optional at IAL2.

	SP 800-63B provides requirements and recommendations for biometric collection, including: ● the use of an authenticated protected channel between the biometric sensor/scanner and the endpoint/workstation; ● the use of PAD technologies for automated biometric collection; and ● performing physical comparison for manual biometric collection. **ASSESSMENT OBJECTIVE:** for IAL3, confirm that the CSP collects a biometric sample (such as a facial image or fingerprints) and that all biometrics are collected in accordance with requirements in SP 800-63B section 5.2.3. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: *If the CSP provides identity proofing at IAL3:* **Examine:** the CSP's *documented policies* or *practices* for its policy about collecting a biometric sample at the time of identity proofing; or **Interview:** *trained operators* to determine their procedures for collecting biometric samples; or **Test**: *system functionality* for biometric collection.

6 Supervised Remote Identity Proofing

Component: Supervised Remote Identity Proofing

Supervised remote identity proofing is intended to provide controls for comparable levels of confidence and security to in-person IAL3 identity proofing for identity proofing processes that are performed remotely. Supervised remote identity proofing is optional for CSPs; that is, if a CSP chooses to use supervised remote identity proofing, then the requirements of section 5.3.3.2 would apply. It should be noted that the term "supervised remote identity proofing" has specialized meaning in SP 800-63A and is used only to refer to the specialized equipment and controls required in section 5.3.3.2.

In addition to those requirements presented in the General section of this document, as well as the applicable IAL3 identity validation and verification requirements, CSPs that provide supervised remote identity proofing services must demonstrate conformance with the requirements contained in this section.

The following requirements for supervised remote proofing apply specifically to IAL3. If the equipment/facilities used for supervised remote proofing are used for IAL2 identity proofing, the requirements in section 5.3.3.2 of SP 800-63A for supervised remote proofing do not apply. In this case, the requirements for conventional remote identity proofing are applicable.

SRP-1	**REQUIREMENT**: Supervised remote identity proofing and enrollment transactions SHALL meet the following requirements, in addition to the IAL3 validation and verification requirements specified in Section 4.6. (5.3.3.2) **SUPPLEMENTAL GUIDANCE**: Supervised remote identity proofing involves the use of a CSP-controlled station at a remote location that is connected to a trained operator at a central location. The goal of this arrangement is to permit identity proofing of individuals in remote locations where it is not practical for them to travel to the CSP for in-person identity proofing. The purpose of supervised remote identity proofing is to take advantage of improvements in sensor technology (cameras and biometric sensors) and communications bandwidth to closely duplicate the security of in-person identity proofing, which has been the requirement for high-assurance identity proofing in the past. This can be done through the use of a remote identity proofing station (or kiosk) which is under the control of the CSP or a third party that is trusted by the CSP to maintain its integrity. Supervised remote identity proofing may also be used for achieving comparability with in-person requirements when face-to-face (i.e., in-person) encounters may present health risks to the applicant, CSP personnel or both. This circumstance may occur due to circumstances such as the covid-19 pandemic where face-to-face encounters may present health risks. In such

	circumstance supervised remote identity proofing may be used in a common facility where the applicant and CSP are in different locations in the facility but not actually interacting face-to-face. In such circumstances supervised remote identity proofing processing may be used. It is intended that CSPs employing supervised remote identity proofing will document the procedures, equipment, and controls for supervised remote proofing in an applicable written policy or *practice statement* as described in SP 800-63A conformance criterion GEN-6. **ASSESSMENT OBJECTIVE:** If supervised remote identity proofing is employed by the CSP, ensure that the procedures, equipment, and controls meet all applicable requirements, including the IAL3 validation and verification requirements specified in Section 4.6 of SP 800-63A and applicable conformance criteria for IAL3 provided in this document. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documentation* regarding its use of supervised remote proofing at IAL3.

SRP-2	**REQUIREMENT**: The CSP SHALL monitor the entire identity proofing session, from which the applicant SHALL NOT depart — for example, by a continuous high-resolution video transmission of the applicant. (5.3.3.2 #1) **SUPPLEMENTAL GUIDANCE**: The integrity of supervised remote identity proofing depends upon the applicant being continuously present during the entire session. An applicant who steps away from an in-process session may do so to alter their biometric source or substitute a different person to complete the identity proofing process. **ASSESSMENT OBJECTIVE:** Confirm that the CSP employs a suitable method for ensuring an applicant is continuously present during the entire identity proofing session. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: one or both the of the following: ● the CSP's *documentation* to determine how it monitors remote identity proofing sessions; or ● a demonstration of the *system functionality* that monitors remote identity proofing sessions.

SRP-3	**REQUIREMENT**: The CSP SHALL have a live operator participate remotely with the applicant for the entirety of the identity proofing session. (5.3.3.2 #2)

	SUPPLEMENTAL GUIDANCE: Having a trained operator supervise and participate in a remote identity proofing session reduces the opportunity for an applicant to defraud the process. As described in SP 800-63A, the **operator** is a person who has received specific training on enrollment and identity proofing procedures and the detection of potential fraud by an applicant. **ASSESSMENT OBJECTIVE:** Confirm that the CSP's supervised remote proofing process involves a live operator participating with the applicant during the entire identity proofing session. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: one or both the of the following: ● the CSP's *documentation* to determine the process by which live operators participate in remote identity proofing sessions; or ● a demonstration of the *system functionality* that involves the live operator's participation with an applicant.

SRP-4	**REQUIREMENT**: The CSP SHALL require all actions taken by the applicant during the identity proofing session to be clearly visible to the remote operator. (5.3.3.2 #3) **SUPPLEMENTAL GUIDANCE**: The camera(s) a CSP employs to monitor the actions taken by a remote applicant during the identity proofing session should be positioned in such a way that the upper body, hands, and face of the applicant are always visible. Additionally, the components of the remote identity proofing station (including such things as keyboard, fingerprint capture device, signature pad, and scanner, as applicable) should be arranged such that all interactions with these devices is within the field of view. **ASSESSMENT OBJECTIVE:** Confirm the cameras on the CSP's remote identity proofing stations are situated in such a way that all identity proofing actions taken by an applicant are clearly visible to the remote operator. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: a demonstration of the *system functionality* that confirms all actions are visible to a remote operator.

SRP-5	**REQUIREMENT**: The CSP SHALL require that all digital ~~verification~~ [validation] of evidence (e.g., via chip or wireless technologies) be performed by integrated scanners and sensors. (5.3.3.2 #4) **SUPPLEMENTAL GUIDANCE**: Technologies exist that allow for the digital validation of identity evidence via electronic means (such as RFID to read the

	data off e-passports and chip readers for smartcards). The scanners and sensors employed to access these features should be integrated into the remote identity proofing stations in order to reduce the likelihood of being tampered with, removed, or replaced. To be integrated means the devices themselves are a component of the workstation (i.e., smartcard readers or fingerprint sensors built into a laptop) or the devices, and their connections, are secured in a protective case or locked box. **ASSESSMENT OBJECTIVE:** Confirm that any scanners or sensors used to validate evidence are integrated into the remote identity proofing stations (aka, kiosks). **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: one or both the of the following: ● *system documentation*, such as remote identity proofing station specifications; or ● an actual *remote identity proofing station* employed by the CSP.

SRP-6	**REQUIREMENT**: The CSP SHALL require operators to have undergone a training program to detect potential fraud and to properly perform a supervised remote proofing session. (5.3.3.2 #5) **SUPPLEMENTAL GUIDANCE**: A comprehensive training program for supervised remote identity proofing operators may include some or all the following: ● Purpose and objectives of the identity proofing and enrollment process, as employed by the CSP; ● Supervised remote identity proofing process workflow; ● Identity evidence validation processes; ● Threats associated with the identity proofing process and how to detect potential fraud; and ● System and process troubleshooting and problem resolution. **ASSESSMENT OBJECTIVE:** Confirm the CSP requires all its supervised remote identity proofing operators to have completed appropriate training. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: 1. the CSP's *documented policies or practices* to determine how it trains its supervised remote identity proofing operators; and 2. its *training records*.

SRP-7	**REQUIREMENT**: The CSP SHALL employ physical tamper detection and resistance features appropriate for the environment in which it is located. (5.3.3.2 #6) **SUPPLEMENTAL GUIDANCE**: For example, a kiosk located in a restricted area or one where it is monitored by a trusted individual requires less tamper detection than one that is located in a semi-public area such as a shopping mall concourse. (SP 800-63A) Requirements for protection of the kiosk depend on the specific kiosk capabilities (e.g., anti-tamper features). In most (perhaps all) cases, the kiosk will be overseen by a human attendant that can supplement the security features and protect the integrity of the kiosk. Between the attendant and the kiosk, the forms of protection provided may include (but are not limited to): ● Ensuring that a single individual (applicant) interacts with the kiosk during any identity proofing session; ● Ensuring that the physical integrity of the kiosk and its sensors is maintained at all times; ● Verifying that the applicant is not using any devices to spoof biometric sensors (finger covers, for example); and ● Reporting any problems with the kiosk to the CSP. **ASSESSMENT OBJECTIVE:** Confirm the CSP's remote identity proofing stations or kiosks include appropriate tamper resistance and detection features. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: one or both the of the following: ● *system documentation*, such as remote identity proofing station specifications; or ● an actual *supervised remote identity proofing station (kiosk)* employed by the CSP.

SRP-8	**REQUIREMENT**: The CSP SHALL ensure that all communications occur over a mutually authenticated protected channel. (5.3.3.2 #7) **SUPPLEMENTAL GUIDANCE**: Mutually authenticated protected channels employ approved cryptography to encrypt communications between Supervised remote identity proofing stations/kiosks are required to employ mutual authentication where both the station/kiosk and server authenticate to each other. This is most often accomplished through the use of mutual TLS. Upon successful mutual authentication, an encrypted communication channel is

	established between the workstation/kiosk and the server which protects the data exchanged between them. **ASSESSMENT OBJECTIVE:** Confirm the CSP's supervised remote identity proofing stations or kiosks communicate with the identity service via mutually authenticated protected channels. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: one or both the of the following: ● *system documentation*, such as remote identity proofing station specifications; or ● an actual *supervised remote identity proofing station (kiosk)* employed by the CSP.

7 Trusted Referees

Component: Trusted Referees

The use of trusted referees is optional for CSPs; that is, if a CSP chooses to use trusted referees for identity proofing and enrollment, then the requirements of SP 800-63A section 5.3.4 would apply. The use of trusted referees is intended to assist in the identity proofing and enrollment for populations that are unable to meet IAL2 and IAL3 identity proofing requirements, or otherwise would be challenged to perform identity proofing and enrollment process requirements. Such populations may include, but are not limited to:

- disabled individuals;
- elderly individuals;
- homeless individuals,
- individuals with little or no access to online services or computing devices;
- unbanked and individuals with little or no credit history;
- victims of identity theft;
- children under 18; and
- immigrants.

In addition to those requirements presented in the General section of this document, as well as the applicable IAL requirements, CSPs that use trusted referees in their identity proofing services must demonstrate conformance with the requirements contained in this section.

TRR-1	**REQUIREMENT**: If the CSP uses trusted referees, then…The CSP SHALL establish written policy and procedures as to how a trusted referee is determined and the lifecycle by which the trusted referee retains their status as a valid referee, to include any restrictions, as well as any revocation and suspension requirements. (5.3.4 #2) **SUPPLEMENTAL GUIDANCE**: In instances where an individual cannot meet the identity evidence requirements specified in Section 4.4.1, the agency may use a trusted referee to assist in identity proofing the applicant. It is intended that CSPs using trusted referees for identity proofing and enrollment will document the procedures and controls in an applicable written policy or *practice statement* as described in SP 800-63A conformance criterion GEN-6. The CSP may use trusted referees — such as notaries, legal guardians, medical professionals, conservators, persons with power of attorney, or some other form of trained and approved or certified individuals — that can vouch for or act on behalf of the applicant in accordance with applicable laws, regulations, or agency policy. The CSP may use a trusted referee for both remote and in-person processes. (5.3.4 #1)

	SP 800-63A section 5.3.4 intentionally avoids presenting overly prescriptive requirements in order to allow CSPs flexibility in establishing processes for trusted referees that can best meet their operating environment and target populations. Therefore, the CSP documentation for the use of trusted referees may include: • types of trusted referees permitted, • use(s) of referees, • trusted referee enrollment procedures, • identity proofing processes for trusted referees and the applicants they represent, • trusted referee relationship to applicants, • procures for recording trusted referees in enrollment records and logs, • contact and communication procedures for trusted referees and the applicants they represent. **ASSESSMENT OBJECTIVE:** If the CSP allows the use of Trusted Referees, confirm it has written policy and procedures governing its use of trusted referees. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documentation* to determine its policies and procedures on its use of trusted referees.

TRR-2	**REQUIREMENT**: If the CSP uses trusted referees, then…The CSP SHALL proof the trusted referee at the same IAL as the applicant proofing. (5.3.4 #3) **SUPPLEMENTAL GUIDANCE**: Trusted referees, who participate in the identity proofing process on behalf of an applicant need to be identity proofed themselves to the same level as that of the applicant. If CSPs allows the use of Trusted Referees, its documented policies should state this requirement. **ASSESSMENT OBJECTIVE:** If the CSP allows the use of Trusted Referees, confirm its written policy states that they must be proofed to the same IAL (or stronger) as that of the applicant. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented policies* to determine to which IAL Trusted Referees must be proofed.

TRR-3	**REQUIREMENT**: If the CSP uses trusted referees, then…The CSP SHALL determine the minimum evidence required to bind the relationship between the trusted referee and the applicant. (5.3.4 #3) **SUPPLEMENTAL GUIDANCE**: In addition to proofing a Trusted Referee to the same (or greater) IAL as that of the applicant, CSPs will need to determine its process for proving a legitimate relationship to the applicant. The CSP should consider and document the types of evidence (i.e., power of attorney) it will accept to "bind" the relationship between Trusted Referee and an applicant. This minimum evidence may vary based on IAL. Additionally, for the purposes of auditability, the CSPs identity service should record all evidence collected and the binding/linkage between the Trusted Referee and applicant. **ASSESSMENT OBJECTIVE:** if the CSPs allows the use of Trusted Referees, confirm it has determined the minimum evidence required to bind the relationship between the trusted referee and the applicant. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: the CSP's *documented policies or procedures* to determine which types of evidence it accepts to bind the relationship between a trusted referee and an applicant at a given IAL.

Appendix A -- Knowledge Based Verification

Knowledge-based Verification Conformance Criteria

The conformance criteria for Knowledge-based Verification have been removed from the full set of SP 800-63A conformance criteria and the KBV requirements are presented in Appendix A for information purposes. NIST SP 800-63A section 5.3 specifies that KBV can only be used for the purposes of identity resolution and for identity verification of a single piece of identity evidence at the "fair" level (on the scale of unacceptable, weak, fair, strong, and superior). Due to the wide availability of KBV information and, therefore, KBV answers to potential impostors, KBV presents very limited strength to the verification process. The objective of the verification phase in identity proofing is to bind the validated identity evidence from the validation phase of identity proofing to the real-world identity of the applicant. SP 800-63A section 5.3 and Table 5-3 present a graduated scale for methods that may be used to verify the binding of validated identity evidence to the identity proofing applicant and specify that KBV may be used only to bind a single piece of identity evidence at the "fair" level. Since IAL2 requires identity evidence of at least the "strong" level and, therefore, verification of binding at least at the "strong" level, KBV could never be used exclusively for verification of such binding. Additional verification of such binding is always required for identity evidence beyond KBV in order to meet IAL2 for SP 800-63A. For this reason, the conformance criteria are moved to Appendix A for information as it is not intended that conformance assessment for these criteria would be applicable.

KBV-1	**REQUIREMENT**: The CSP SHALL adhere to the requirements in Section 5.3.2 if KBV is used to verify an identity. (5.3.1)

KBV-2	**REQUIREMENT**: The CSP SHALL NOT use KBV to verify an applicant's identity against more than one piece of validated identity evidence. (5.3.2 #1)

KBV-3	**REQUIREMENT**: The CSP SHALL only use information that is expected to be known only to the applicant and the authoritative source, to include any information needed to begin the KBV process. (5.3.2 #2)

KBV-4	**REQUIREMENT**: Information accessible freely, for a fee in the public domain, or via the black market SHALL NOT be used. (5.3.2 #2)

KBV-5	**REQUIREMENT**: The CSP SHALL allow a resolved and validated identity to opt out of KBV and leverage another process for verification. (5.3.2 #3)

KVB-6	**REQUIREMENT**: The CSP SHALL ensure that transaction information has at least 20 bits of entropy. For example, to reach minimum entropy requirements, the CSP could ask the applicant for verification of the amount(s) and transaction numbers(s) of a micro-deposit(s) to a valid bank account, so long as the total number of digits is seven or greater. (5.3.2 #4)

KBV-7	**REQUIREMENT**: The CSP MAY perform KBV by asking the applicant questions to demonstrate they are the owner of the claimed information. However, the following requirements apply: b. The CSP SHALL require a minimum of four KBV questions with each requiring a correct answer to successfully complete the KBV step. (5.3.2 #5)

KBV-8	**REQUIREMENT**: e. The CSP SHALL time out KBV sessions after two minutes of inactivity per question. In cases of session timeout, the CSP SHALL restart the entire KBV process and consider this a failed attempt. (5.3.2 #5)

KBV-9	**REQUIREMENT**: f. The CSP SHALL NOT present a majority of diversionary KBV questions (i.e., those where "none of the above" is the correct answer). (5.3.2 #5)

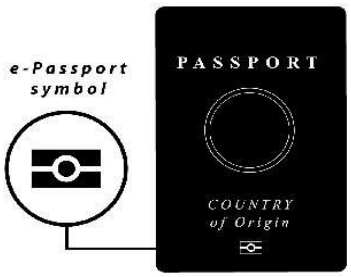
KBV-10	**REQUIREMENT**: h. The CSP SHALL NOT ask a KBV question that provides information that could assist in answering any future KBV question in a single session or a subsequent session after a failed attempt. (5.3.2 #5)

KBV-11	**REQUIREMENT**: i. The CSP SHALL NOT use KBV questions for which the answers do not change (e.g., "What was your first car?"). (5.3.2 #5)

KBV-12	**REQUIREMENT**: j. The CSP SHALL ensure that any KBV question does not reveal PII that the applicant has not already provided, nor personal information that, when combined with other information in a KBV session, could result in unique identification. (5.3.2 #5)

Appendix B -- Notional Strength of Evidence Types Table

Table B-1 Notional Strength of Evidence Types

Type of Evidence	Strength	Notes
US Passport	Superior	Includes US Passport cards
Foreign e-Passport	Superior	
Personal Identity Verification (PIV) card	Superior	
Common Access card (CAC)	Superior	
Personal Identity Verification Interoperable (PIV-I) card	Superior	
Transportation Worker Identification Credential (TWIC)	Superior	
Permanent Resident Card	Superior	Issued on or after May 11, 2010
Native American Enhanced Tribal Card	Superior	

Type of Evidence	Strength	Notes
REAL ID cards	Strong+	Includes REAL ID driver's licenses and ID cards. REAL ID cards have a star printed in the upper right-hand corner. Card and personal information must be validated with appropriate DMV or AAMVA.
Enhanced ID cards	Strong+	Includes Enhanced ID driver's licenses and ID cards. Must be validated with appropriate DMV or AAMVA.
U.S. Uniformed Services Privilege and Identification Card (U.S. Military ID)	Strong+	Includes Uniformed Services Dependent ID Cards. Must be validated with appropriate military issuing source.
Permanent Resident Card	Strong	Issued Prior to May 11, 2010
Native American Tribal Photo Identification Card	Strong	
Driver's License or ID card (REAL ID non-compliant)	Strong	

Type of Evidence	Strength	Notes
School ID card	Fair	Includes facial image photograph
Utility account statement	Fair	
Credit/debit card and account statement	Fair	
Financial institution account statement	Fair	
US Social Security Card	Weak	
Original or certified copy of a birth certificate issued by a state, county, municipal authority or outlying possession of the United States bearing an official seal	Weak	

Note: the classification Strong+ denotes evidence that may be considered to meet the evidence strength requirement for the IAL2 requirement for one piece of STRONG evidence and the IAL3 evidence strength requirement for one piece of SUPERIOR evidence and one piece of STRONG+ evidence given the strength of the original identity proofing for these evidence types, provided that the STRONG+ evidence must be validated with the issuing sources listed in order to meet this evidence strength classification.

Appendix C – Types of Identity Evidence Security Features

Identity evidence may contain multiple forms of security features. Some forms of security features may be confirmed through visible inspection, tactile examination, specialized lighting, manipulation (e.g., tilting or turning to allow light refraction), or specialized equipment. Following are descriptions for common types of security features, including the capabilities necessary for confirmation of the security feature.

Security Feature (examination capability)	**Description**
Fine-line or Guilloche Pattern (visual)	Background pattern of continuous fine lines printed in wavy, overlapping pattern.
Ghost image (visual)	Half-tone reproduction of original image (e.g., facial image), may be printed behind printed data.
Overlapped data (visual)	Variable data (e.g., signature, seal, text) printed over another field such as facial image or seal.
Transparent image (visual)	See-through, window-like image feature (e.g., facial image) visible for both sides of the evidence.
Rainbow printing (visual)	Controlled color shifts of printed text in a continuous, linear fashion.
Holographic Images (visual, tilting)	Light field record of objects that will appear and change as view of evidence is tilted and turned. Most state-issued driver's licenses and IDs contain at least one holographic image.
Variable laser engraved images (visual, tilting)	Laser-engraved images at different angles so that image view changes with tilting angle of viewing evidence.
Iridescent Inks and Custom Foil Stamping (visual, tilting)	Custom designs and printing that will change color properties depending on the angle at which evidence is viewed.
Laser perforation (visual, light, tactile)	Perforated holes made by laser beam to form images. The images can be viewed under light source; image holes have tactile feel.
UV printing (visual, UV lighting)	A UV image or text that can only be viewed with special lighting. UV images may appear on the front or back of the evidence.
Microprinting (visual, magnifier)	Microtext of static or variable data that can be confirmed when viewed under a magnifier. Requires magnification of at least 10X to view.

Laser embossing (tactile)	Use of laser to emboss image or text for tactile feel on only one side of the evidence.
Barcode (visual, barcode reader)	Machine readable, encoded data (typically personalized printed data) for 2-D barcode, readable with barcode reader.
UV printing (visual, UV lighting)	A UV image or text that can only be viewed with specialized lighting. UV images may appear on the front or back of a card.