MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

ENROLLMENT AND IDENTITY PROOFING PRACTICES STATEMENT TEMPLATES

Supporting Remote Proofing in Accordance with NIST SP 800-63A Identity Assurance Levels 2 & 3

Russ Reopell and Andy Seymour

MAY 2020

ACKNOWLEDGEMENTS

The authors would like to thank and acknowledge the many colleagues who helped with the development and review of this paper. In particular, the support from Lorrayne Auld and Mary Yang with the MITRE Corporation, was instrumental to this paper's publication and release.

EXECUTIVE SUMMARY

This document is as a guide for Credential Service Providers (CSPs) to use in developing an Enrollment and Identity Proofing Practice Statement (EIPPS), and for documenting CSP identity proofing practices. An EIPPS describes the basic processes a CSP should use based on current published guidance from the National Institute of Standards and Technology (NIST).

Federal agencies and commercial service providers offering credentialing services should follow the general process flows described in NIST Special Publication (SP) 800-63-3, Digital Identity Guidelines, and its accompanying volume, for enrolling and proofing the identity of applicants. Although other documents describe the processes related to identity proofing, this document uses NIST SP 800-63A, *Digital Identity Guidelines: Enrollment and Identity Proofing,* as the basis for the identity proofing process. Some sections of the document have been influenced by other publications and information available on enrollment and identity proofing best practices. This document first refines the foundational, basic three-step process flow described in NIST SP 800-63A, to describe a six-step process with an optional seventh step to bind the newly proofed digital identity to an authenticator in possession of the identified individual. The six steps plus the one optional step are:

1. User Notification/Education and Acceptance
2. Core Attributes/Personally Identifiable Information (PII) Collection
3. Resolve to a Unique Identity
4. Identity Evidence Collection
5. Validation of Identity Evidence
6. Verification of Applicant to Claimed Identity
7. Binding (optional)

Section 1 of the document is the introduction discussing the purpose and use of the document. Section 2 describes the refined process flows for a CSP to be successful at remotely proofing the identity of applicants to Identity Assurance Levels 2 and 3, as defined in NIST SP 800-63A. Section 2 also presents a summary of the requirements identified by NIST SP 800-63A to drive the remote identity proofing processes. For detailed requirements for both remote-proofing processes, see Appendix A. Section 3 describes the templates that a CSP should use based on the requirements within each of the first six steps listed above.

The final portion of the document is the appendices containing Enrollment and Identity Proofing Requirements from NIST SP 800-63A for IAL2 Unsupervised Remote and IAL3 Supervised Remote In-Person Identity Proofing, Identity Evidence to include Strength, Validation and Verification Guidance, General References, Definitions, and Abbreviations and Acronyms.

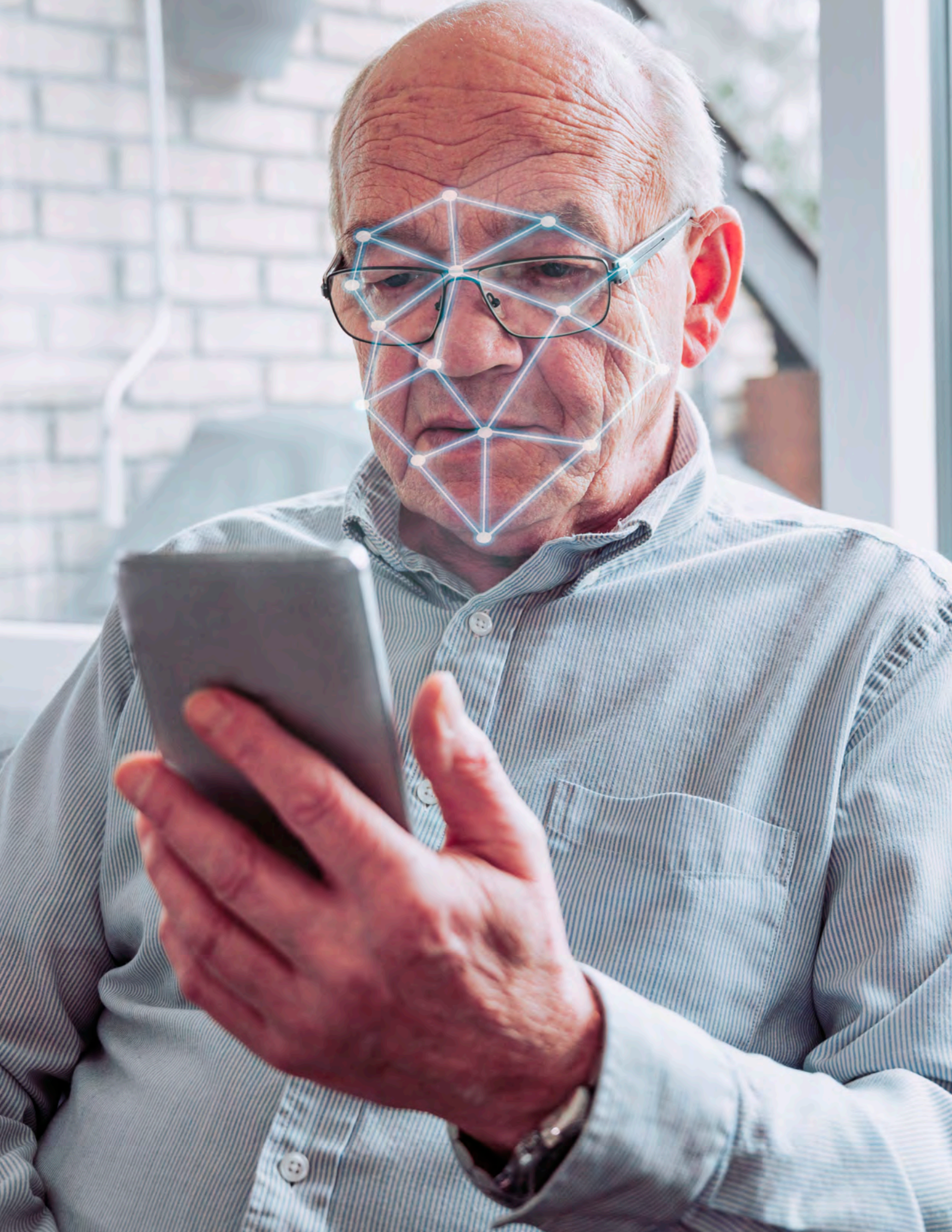


Table of Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF TABLES (CONTINUED)

Requirements Notation and Conventions

The terms “SHALL” and “SHALL NOT” indicate requirements to be followed strictly in order to conform to the publication and from which no deviation is permitted.

The terms “SHOULD” and “SHOULD NOT” indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited.

The terms “MAY” and “NEED NOT” indicate a course of action permissible within the limits of the publication.

The terms “CAN” and “CANNOT” indicate a possibility and capability, whether material, physical or causal or, in the negative, the absence of that possibility or capability.

1 INTRODUCTION

In June 2017, National Institute of Standards and Technology (NIST) published the third revision to Special Publication (SP) 800-63 (designated as SP 800-63-3), in which they not only retitled the guidance *(formally known as E-Authentication Guidance)* but also made significant changes from the previous version.

The Office of Management and Budget published M-19-17 titled *Enabling Mission Delivery through Improved Identity, Credential, and Access Management* and, dated May 21, 2019. M-19-17 states, "Agencies must be able to identify, credential, monitor, and manage user access to information and information systems across their enterprise in order to ensure secure and efficient operations."

M-19-17 also states, "To set the foundation for identity management and its usage to access physical and digital resources, agencies must
implement National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3 and any successive versions.

NIST SP 800-63-3 introduces individual components of digital authentication assurance to support mitigation of the negative impacts induced by an authentication error. For non-federated systems, agencies will now select two components:

- *Identity Assurance Level (IAL)* refers to the identity proofing process and the binding between one or more authenticators and the records pertaining to a specific subscriber.
- *Authenticator Assurance Level (AAL)* refers to the authentication process itself.

For federated systems, a third component is included:

- *Federation Assurance Level (FAL)* refers to the assertion protocol utilized in a federated environment to communicate authentication and attribute information (if applicable) to a relying party (RP).

Although many systems will have the same numerical level for each of the three components, IAL, AAL, and FAL, it is not a requirement, and agencies should not assume the numerical levels will be the same in any given system.

> "Agencies must be able to identify, credential, monitor, and manage user access to information and information systems across their enterprise in order to ensure secure and efficient operations."

Finally, NIST SP 800-63-3 has been split into a suite of four documents. The suite as a whole is referred to as "the guidelines," with the individual documents referred to as "volumes." RPs are required to use NIST SP 800-63; the remaining three volumes may be used independently or in an integrated fashion, depending on the component service(s) that an agency requires.

The four volumes are:

1. **NIST SP 800-63-3, Digital Identity Guidelines** provides an overview of general identity frameworks; using authenticators, credentials, and assertions together in a digital system; and a risk-based process of selecting the appropriate assurance levels.
2. **NIST SP 800-63A, *Enrollment and Identity Proofing*** addresses how applicants can prove their identities and become enrolled as valid subscribers within an identity system. It provides requirements by which applicants can both identity-proof and enroll at one of three different levels of risk mitigation in both remote and physically present scenarios. NIST SP 800-63A sets requirements to achieve a given IAL.
3. **NIST SP 800-63B, *Authentication and Lifecycle Management*** for services in which return visits are applicable, a successful authentication provides reasonable risk-based assurances that the subscriber accessing the service today is the same as that which accessed it previously. The robustness of this confidence is described by an AAL categorization. NIST SP 800-63B addresses how an individual can securely authenticate to a Credential Service Provider (CSP) to access a digital service or set of digital services. NIST SP 800-63B sets requirements to achieve a given AAL.
4. **NIST SP 800-63C, *Federation and Assertions*** provides requirements when using federated identity architectures and assertions to convey the results of authentication processes and relevant identity information to an agency application. In addition, this volume offers privacy-enhancing techniques to share information about a valid, authenticated subject and describes methods that allow for strong multi-factor authentication (MFA) while the subject remains pseudonymous to the digital service. NIST SP 800-63C sets requirements to achieve a given FAL.

All four volumes contain both normative and informative material. The three assurance levels for identity, authenticators, and federation reflect the options agencies can select based on their risk profile and the potential harm caused by an attacker either making a successful false claim of an identity, taking control of an authenticator and accessing agencies' systems, or taking control of federated transactions. The NIST SP 800-63-3 document set can be obtained from https://pages.nist.gov/800-63-3/.

This document focuses on the enrollment and proofing process of NIST SP 800-63A, *Enrollment and Identity Proofing,* including ***identification*** of applicable requirements to assist CSPs in documenting their enrollment and identity proofing process.

1.1 Purpose

This document aims to provide templates that will assist CSPs in consistently documenting their process for enrollment and remotely identity proofing of applicants who require access to U.S. government agencies' online services. Section 2 presents the general three-step process presented in NIST SP 800-63A and then refines the resolution step to separate collection of core attribute or personally identifiable information (PII). This uniquely resolves the claimed identity in those attributes to a single identity within a given population or context, and the collection/capture of physical identity evidence to validate and verify that the claimed identity belongs to the applicant presenting it. Section 2 also provides a high-level summary of the requirements for IAL2 Unsupervised Remote and IAL3 Supervised Remote In-Person Identity Proofing. For detailed requirements for both, please see Appendix A. Section 3 provides the templates to document the process and identity data required by the CSP to successfully enroll and identity proof applicants at either:

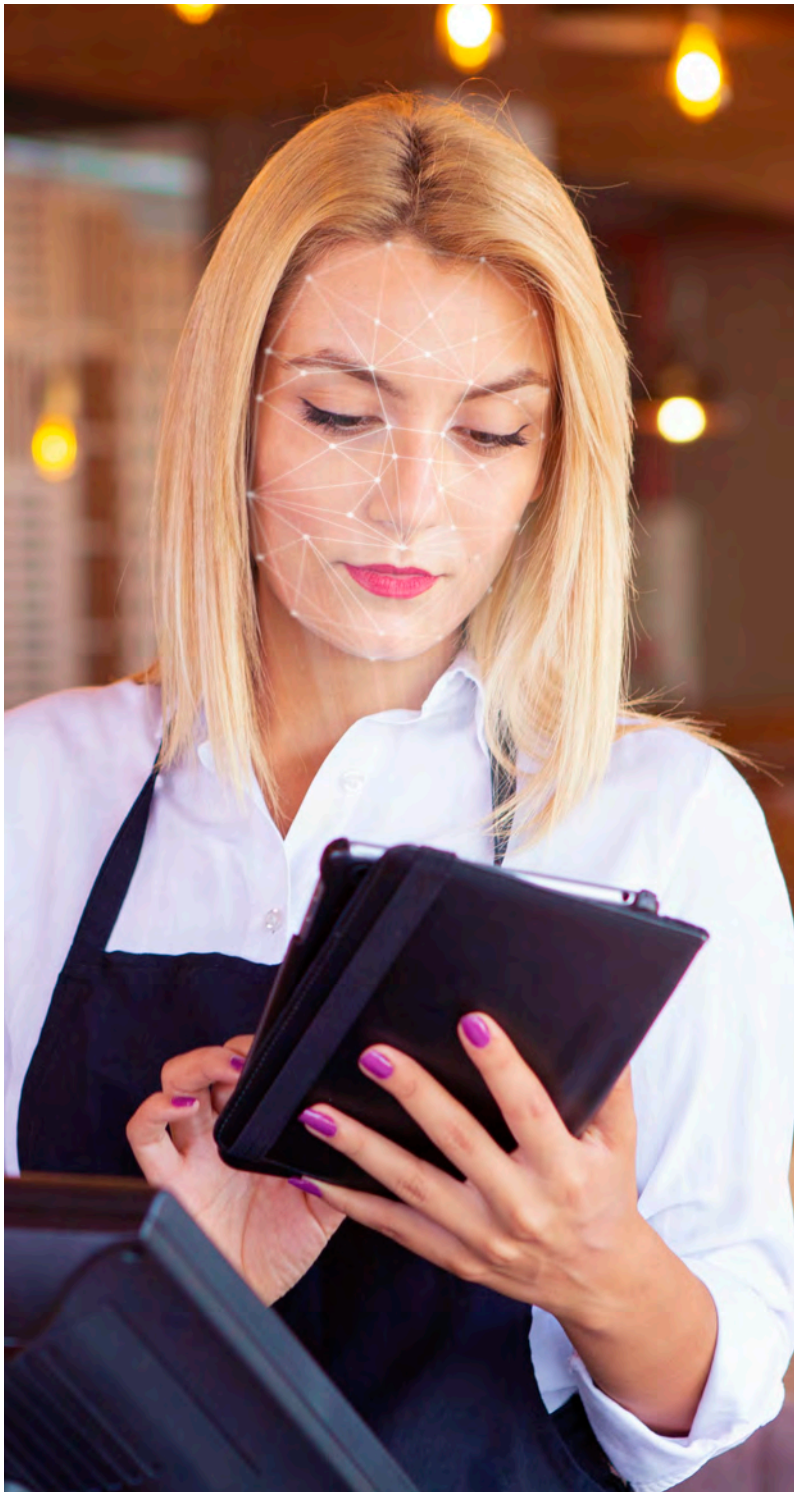
- IAL2 Unsupervised Remote Identity Proofing
- IAL3 Supervised Remote In-Person Identity Proofing

By providing the information requested in the templates, a CSP can fulfill the NIST SP 800-63A, Section 4.2 Requirement 6 for written policy specifying the steps taken to resolve, validate, and verify digital identities. A subset of this information can also be used to meet the requirement of NIST SP 800-63A, Section 4.2 Requirement 3 for notice and consent to applicants.

1.2 Using This Document

This document provides the tools necessary to capture the practices implemented by a CSP, related to enrollment and identity proofing of applicants wishing to gain access to federal government systems and resources. Organizations can use the templates provided in Section 3 of this document to capture their processes and the associated required identity information, and to successfully complete the enrollment and identity proofing required by the CSP. Specifically, for each of the two proofing methods addressed in this document (IAL2 Unsupervised Remote Identity Proofing and IAL3 Supervised Remote In-Person Identity Proofing), the templates assist in documenting these six items:

- User notification explains why identity proofing is required, the type of information requested, how the information will be protected while stored at the CSP, and will capture the applicant's consent to collect and store that information
- The list of core attributes/PII collected and used to resolve the applicant to a unique individual within a given context
- The steps used to resolve those attributes to a unique individual or how the CSP handles identities it cannot resolve, including options the applicant can pursue to successfully complete enrollment and proofing
- The list of physical identity evidence required, including strength, quantity of evidence, and the requirements for that evidence
- The processes the CSP uses to validate that the identity evidence is authentic and relates to a real-life subject
- The processes to verify the identity evidence by linking the claimed identity to the subject presenting evidence



The templates also identify the required baseline set of security controls from NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations,* that are applicable to the assurance level of the template's identity proofing solutions. Note that NIST SP 800-63A allows equivalent federal (FedRAMP) or industry standards to be used in place of NIST SP 800-53. CSPs are encouraged to review the appropriate sections of NIST SP 800-53 or other equivalent standard for the applicable security controls baseline to be applied.

Section 8 of NIST SP 800-63A provides additional information regarding Section 4.2, from a privacy perspective. It provides added information so CSPs can better understand why a minimal set of PII should be requested from the applicant. It also states that notice is given to applicants regarding the purpose for collecting and maintaining identity records and that the CSP must capture the applicant's consent to collect and store that information. Information on attribute use limitations and redress mechanisms is also provided.

It is important that a CSP use attributes collected only for the purposes intended. Failure to do so could instill a lack of trust in the CSP by current and potential subscribers. A CSP must also offer an effective mechanism for resolving applicant complaints or problems that occur during the identity proofing process. This includes alternative methods to complete the identity proofing process. Any mechanisms should be easy for the applicant to find and access.

Much of this information was taken into consideration in developing the templates in Section 3 of this document. In refining the process flow, adding a specific step for notification and consent gives CSPs a clear reminder to provide notice and get consent. This is important information to include in the Enrollment and Identity Proofing Practice Statement (EIPPS) and is therefore included in the templates. They are designed to assist CSPs in giving the level of information needed to fulfill their obligations to provide written policy or practice statements specifying the step-by-step processes to verify the identity of an applicant.

Templates will be provided to support the following:

- IAL2 Unsupervised Remote Identity Proofing
- IAL3 Supervised Remote In-Person Identity Proofing

The templates focus solely on the enrollment and identity proofing processes required when collecting core attributes to resolve to a unique identity, and when collecting identity evidence to validate and verify as proof of a claimed identity belonging to a specific individual. The

practice statement templates also include placeholders for control information detailing how the CSP handles proofing errors that result in unsuccessful enrollment for an applicant—for example, the number of retries allowed, proofing alternatives (e.g., in-person if remote fails), or fraud countermeasures when anomalies are detected.

When a subject is identity proofed, the expected outcomes include:

- Resolve a claimed identity to a single, unique identity within the context of the population of users that the CSP serves
- Validate that all supplied evidence is correct and genuine (e.g., not counterfeit or misappropriated)
- Validate that the claimed identity exists in the real world
- Verify that the claimed identity is associated with the real person supplying the identity evidence

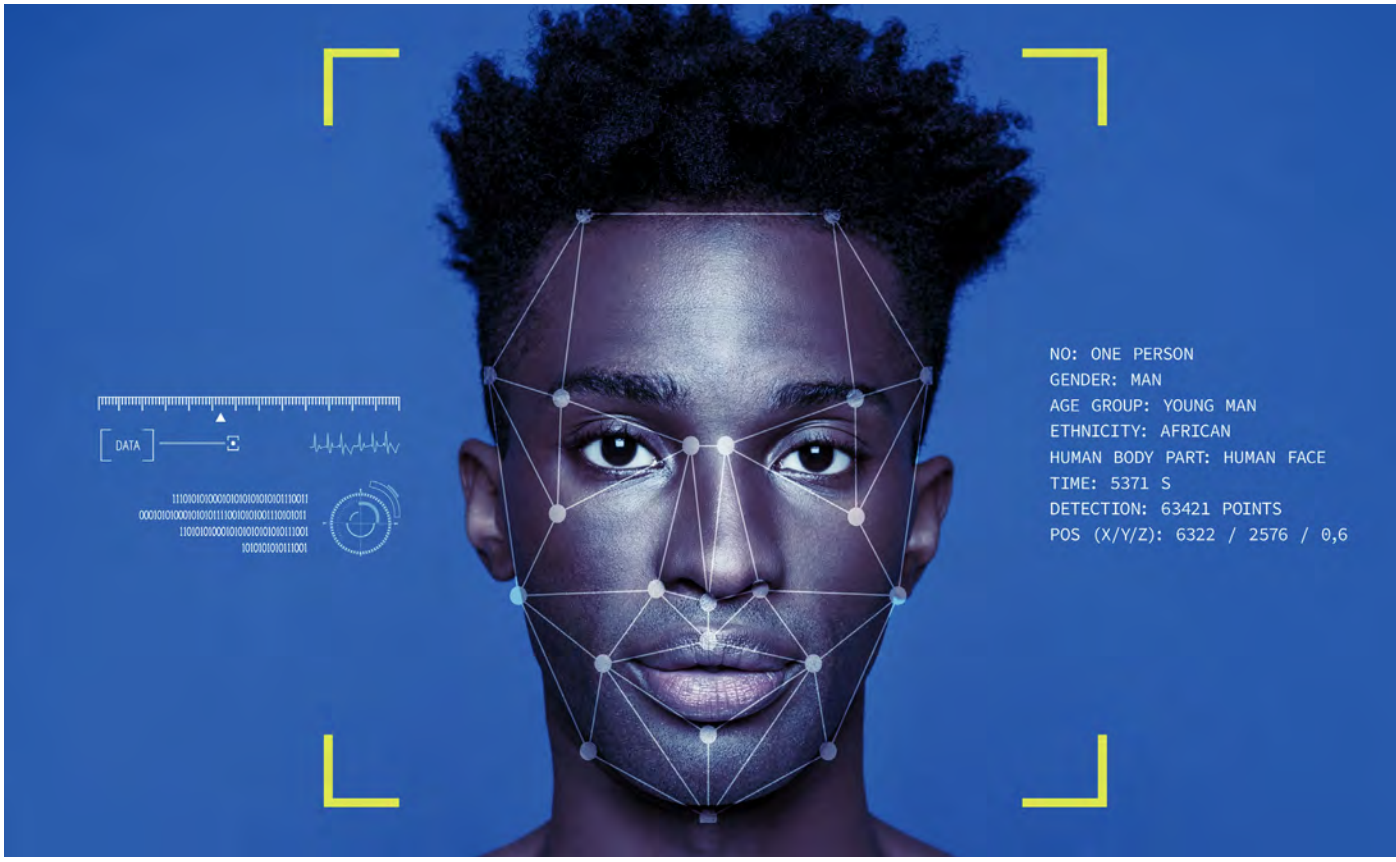
Identity proofing's sole objective is to ensure the applicant is who they claim to be, to a stated level of certitude. NIST SP 800-63A lists requirements that must be met to achieve one of the Identity Assurance Levels in Table 1-1.

- It is assumed an agency has performed the required risk assessments of the e-services being offered and has determined the IAL needed as either IAL2 or IAL3 and that remote proofing is acceptable to the service provider. This document provides the templates and identifies the requirements from NIST SP 800-63A for remotely proofing an applicant's identity at IAL2 and IAL3.

Section 2 of this document provides the basic three-step process flow as described in Section 4 of NIST SP 800-63A. The first step, called "Resolution" in Section 4 of NIST 800-63A, is refined into three individual steps: 1) collect core attributes or PII, 2) resolve the claimed identity from the core attributes to a unique identity in the context of that CSP, and 3) collect or capture physical identity evidence to be used in the validation and verification steps of the identity proofing process. The refinement also adds a step for notification and consent of the identity proofing process, and an optional step at the end to bind a successfully proofed

Table 1-1. Identity Assurance Levels

LEVEL	DESCRIPTION
IAL 1	At IAL 1, attributes, if any, are self-asserted or should be treated as self-asserted.
IAL2	At IAL2, either remote or in-person identity proofing is required. IAL2 requires identifying attributes to have been verified in person or remotely using, at a minimum, the procedures given in SP 800-63A.
IAL3	At IAL3, in-person identity proofing is required. Identifying attributes must be verified by an authorized CSP representative through examination of physical documentation as described in SP 800-63A.



identity or digital identity to an authenticator. Section 2 also provides a high-level summary of requirements for IAL2 Unsupervised Remote Identity Proofing and IAL3 Supervised Remote In-Person Identity Proofing. Detailed requirements can be found in Appendix A.

Section 3 presents two basic templates (IAL2 —Unsupervised Remote Identity Proofing and IAL3—Supervised Remote In-Person Identity Proofing) a CSP could use to provide documentation of its proofing process, per NIST SP 800-63A, Section 4.2 Requirement 6. The text used in the templates has been written by using the refined process flow. It represents the steps and information needed to achieve successful identity proofing at the required assurance level of IAL2 or IAL3. A CSP would use the templates much like an annotated outline and provide the specific details they chose to implement for each part of their particular proofing process. The requirements from NIST SP 800-63A IAL2 —Unsupervised Remote Identity Proofing and IAL3—Supervised Remote In-Person Identity Proofing have been mapped into the corresponding template and process flow, to assist in verifying compliance with NIST SP 800-63A to achieve the desired assurance level.

1.3 Digital Identity Acceptance Statement

The agency SHALL develop a Digital Identity Acceptance Statement, in accordance with NIST SP 800-53 IA-1 a.1. An agency will complete an overall risk assessment based on the selected identity proofing assurance level and documented processes and technologies it will employ. NIST SP 800-63-3 provides details on the necessary content of a Digital Identity Acceptance Statement. It states:

The statement SHALL include, at a minimum:

- Assessed xAL
- Implemented xAL
- Rationale, if implemented xAL differs from assessed xAL
- Comparability demonstration of compensating controls when the complete set of applicable 800-63 requirements are not implemented
- If not accepting federated identities, rationale

Agencies SHOULD include this information in existing artifacts required to achieve a security authorization and accreditation.

THIS PAGE INTENTIONALLY LEFT BLANK

2 IDENTITY PROOFING PROCESS FLOWS AND IAL REQUIREMENTS

To successfully identity proof an applicant, a CSP needs the right process in place to gather all the required identity data (attributes and evidence). It must be able to resolve the claimed identity to a single unique identity within a given population or context by validating the evidence, and validating the applicant identified by the evidence does in fact exist and can be verifiably linked to the identity claimed in the evidence.

To provide clarification and assistance to CSPs and their applicants, this document refines the steps in resolution and validation to distinguish between core attribute or PII collection, resolution of identity, and collection/capture of physical identity evidence in the process. It also adds two additional steps, one at each end of the process.

2.1 Basic Identity Proofing Process Flow

NIST developed an IAL decision tree, shown in Figure 2-1, which uses the results of a CSP's risk assessment of the digital services being offered, to assign the assurance level provided by the identity proofing process. The risk assessment determines the extent to which risk must be mitigated by the identity proofing process. Once the assurance level is assigned, the CSP can follow a common general process flow to implement the required identity proofing steps.

The general process flow for enrollment and identity proofing described and depicted in NIST SP 800-63A, Section 4.1 is broken down into three major steps—resolution, validation, and verification—and is replicated in Figure 2-2.

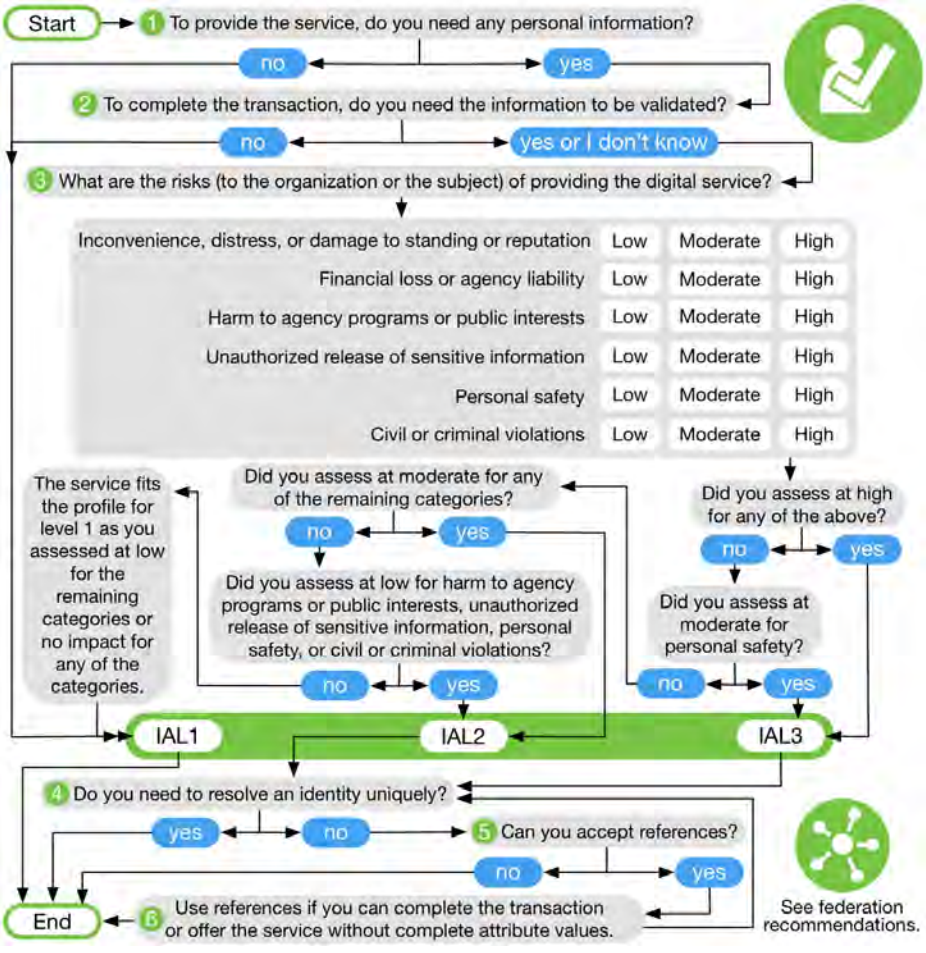


Figure 2-1. NIST Identity Assurance Decision Tree

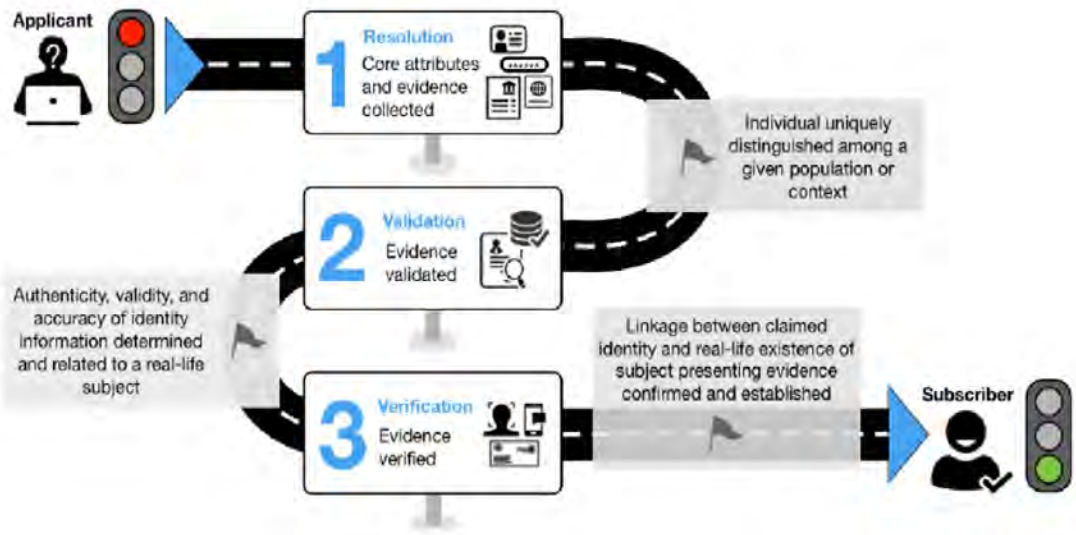


Figure 2-2. NIST's Basic Flow for Enrollment and Identity Proofing

2.2 Identity Proofing Process Flow

To provide clarification and assistance to CSPs and their applicants, this document refines the steps in resolution and validation to distinguish between core attribute or PII collection, resolution of identity, and collection/capture of physical identity evidence in the process. It also adds two additional steps, one at each end of the process.

2.2.1 Enrollment and Proofing Process

When an applicant starts the CSP's enrollment and identity proofing process, the CSP is obligated to notify the applicant with respect to what the identity proofing process is about and to educate them on the process. This should include the purpose for collecting and maintaining a record of the attributes necessary for identity proofing, how long this record will be kept, whether such attributes are voluntary or mandatory to complete the proofing process, and the consequences for not providing the attributes. This education/notification should be given in easy-to-understand language describing what is being collected, why it is being collected, and the measures being used to protect identity data stored at the CSP. Finally, the applicant SHALL be required to acknowledge they have received notification and have reviewed the CSP's presented material on its proofing process (website acknowledgement key selection, wet signature on paper form, etc.).

Identity proofing ends with the successful resolution, validation, and verification of an applicant and the creation of a digital identity record at the CSP. The CSP can then use that record to establish binding between the subscriber's authenticator(s) and identity.

2.2.2 Optional Authenticator Binding at Enrollment

Although enrollment and identity proofing ends at the successful creation of a digital identity record, many CSPs will optionally allow the subscriber to continue into the beginning of the authenticator lifecycle with the binding of the digital identity to at least one authenticator. Should the CSP wish to include binding to an authenticator, the CSP should consult NIST SP 800-63B, Section 6.1.1 Binding at Enrollment, for instructions on binding authenticators to subscribers. This refined process flow of the steps in the identity proofing process to include optional binding at enrollment is shown in Figure 2-3.

1. **User Notification/Education and Acceptance**
    a. What is collected and why?
    b. What will be done with the data collected?
    c. How will the data be protected?
    d. Record applicant acceptance.
2. **Minimal Core Attribute/PII Collection**
    a. Applicant provided identity data/PII claiming an identity.
3. **Resolve to a Unique Identity**
    a. CSP resolves claimed identity to a single, unique identity within the context of its population of users.
    b. KBV MAY be used to resolve to a unique, claimed identity.
4. **Identity Evidence Collection/Capture**
    a. Physical identity evidence is collected or captured.
5. Validation of Identity Evidence
    a. Identity evidence is genuine and authentic
    b. Contains information that is correct
    c. Contains information that pertains to a real-life subject.
6. **Verification of Applicant to Claimed Identity**
    a. Confirm and establish a linkage between the claimed identity and the real-life existence of the subject presenting the evidence.

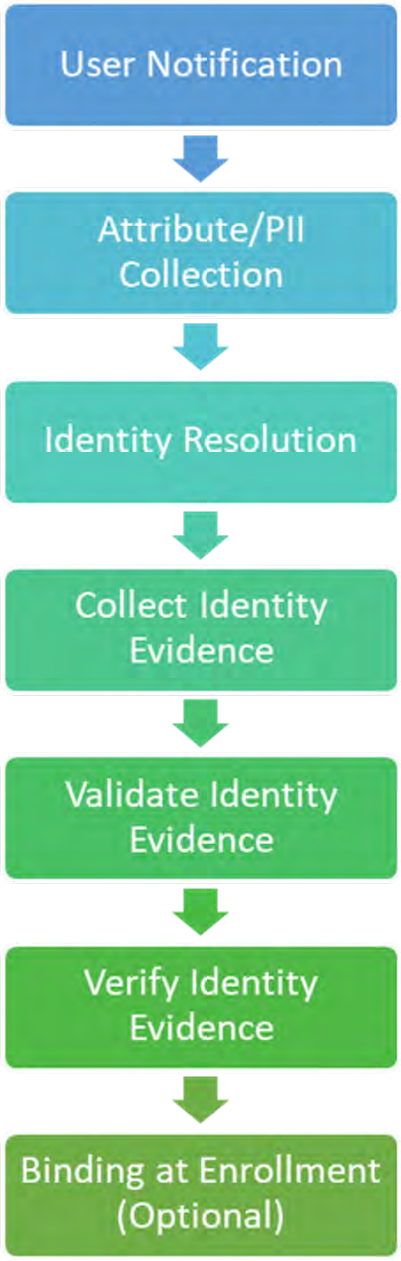


Figure 2-3. Refined Flow for Enrollment and Identity Proofing

2.3 IAL2 and IAL3 Requirements

This document addresses remote identity proofing requirements at IAL2 and IAL3. General requirements for all assurance levels are provided in NIST SP 800-63A, Section 4.2. IAL2 requirements are described in NIST SP 800-63A, Section 4.4, while Section 4.5 provides the requirements for IAL3. Section 5 of NIST SP 800-63A presents the detailed requirements for identity resolution, identity evidence quality, validating identity evidence, and identity verification at both IAL2 and IAL3. Appendix A lists all requirements from NIST SP 800-63A that a CSP would need to meet when offering enrollment and identity proofing services at IAL2 Unsupervised Remote Identity Proofing or IAL3 Supervised Remote In-Person Identity Proofing. The requirements for IAL3 Supervised Remote Identity Proofing have been developed to allow that it be considered equivalent to IAL3 In-Person Identity Proofing. Therefore, to help reinforce that equivalence, this document uses the term IAL3 Supervised Remote In-Person Identity Proofing.

These templates specifically DO NOT address in-person proofing for IAL2 or IAL3, nor do they address Remote Supervised Proofing at IAL2. Finally, the IAL2 template does not address IAL2 Trusted Referee, because the preferred method is to do conventional identity proofing (remote or in-person). Future versions of this document may include a template of Trusted Referee with additional guidance based on federal agency input.

Table 2-1 provides a summary of the IAL2 Unsupervised Remote Identity Proofing and the IAL3 Supervised Remote In-Person Identity Proofing requirements that a CSP would need to achieve to be compliant. A complete list of these requirements taken from NIST SP 800-63A can be found in Appendix A of this document.

Table 2-1. Summary of IAL2 Unsupervised Remote and IAL3 Supervised Remote In-Person Identity Proofing Requirements

CATEGORY	IAL2 UNSUPERVISED REMOTE IDENTITY PROOFING REQUIREMENTS	IAL3 SUPERVISED REMOTE IN-PERSON IDENTITY PROOFING REQUIREMENTS
Notification, Education, and Acceptance	• 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. • Record applicant acceptance.	Same as IAL2

CATEGORY	IAL2 UNSUPERVISED REMOTE IDENTITY PROOFING REQUIREMENTS	IAL3 SUPERVISED REMOTE IN-PERSON IDENTITY PROOFING REQUIREMENTS
Core Attribute Collection	• Collection of core attributes/PII should be limited to the minimum necessary to resolve a unique identity record. This MAY include collection of attributes assisting in data queries.	• At a minimum, the applicant's Same as IAL2
Identity Resolution	• Uniquely distinguish an individual within a given population or context by using the minimum attributes necessary. • MAY employ matching algorithms, which should be publicly available or included in a practice statement. • KBV MAY be used to resolve to a unique, claimed identity.	• Uniquely distinguish an individual within a given population or context by using the minimum attributes necessary. • MAY employ matching algorithms, which should be publicly available or included in a practice statement. • KBV MAY be used to resolve to a unique, claimed identity.
Identity Evidence Collection	• One (1) piece of SUPERIOR or STRONG evidence, depending on strength of original proof, and validation occurs with issuing source *OR* • Two (2) pieces of STRONG evidence *OR* • One (1) piece of STRONG evidence plus two (2) pieces of FAIR evidence	• Two (2) pieces of SUPERIOR evidence *OR* • One (1) piece of SUPERIOR evidence plus one (1) piece of STRONG evidence, depending on strength of original proof, and validation occurs with issuing source *OR* • Two (2) pieces of STRONG evidence plus one (1) piece of FAIR evidence
Identity Evidence Validation	• Each piece of evidence must be validated with a process that can achieve the same strength as the evidence presented. For example, if two forms of STRONG identity evidence are presented, each evidence will be validated at a strength of STRONG. • Training requirements for personnel validating evidence SHALL be based on the policies, guidelines, or requirements of the CSP or RP.	• Each piece of evidence must be validated with a process that can achieve the same strength as the evidence presented. • Training requirements for personnel validating evidence SHALL be based on the policies, guidelines, or requirements of the CSP or RP.

CATEGORY	IAL2 UNSUPERVISED REMOTE IDENTITY PROOFING REQUIREMENTS	IAL3 SUPERVISED REMOTE IN-PERSON IDENTITY PROOFING REQUIREMENTS
Identity Evidence Verification	• At a minimum, the applicant must be verified by a process that can achieve a strength of STRONG. • The applicant's ownership of the claimed identity has been confirmed by: - Physical comparison, using appropriate technologies, to a photograph, to the strongest piece of identity evidence provided to support the claimed identity. Physical comparison performed remotely SHALL adhere to all requirements as specified in NIST SP 800-63B, Section 5.2.3, Use of Biometrics, *OR* - Biometric comparison, using appropriate technologies, of the applicant to the strongest piece of identity evidence provided to support the claimed identity. Biometric comparison performed remotely SHALL adhere to all requirements as specified in NIST SP 800-63B, Section 5.2.3, Use of Biometrics.	• 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. • KBV SHALL NOT be used for in-person (supervised remote) identity verification. • The applicant's ownership of the claimed identity has been confirmed by: - Biometric comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity, using appropriate technologies. - Biometric comparison performed remotely SHALL adhere to all requirements as specified in NIST SP 800-63B, Section 5.2.3, Use of Biometrics.
Presence	• Remote Unsupervised	• Remote Supervised

CATEGORY	IAL2 UNSUPERVISED REMOTE IDENTITY PROOFING REQUIREMENTS	IAL3 SUPERVISED REMOTE IN-PERSON IDENTITY PROOFING REQUIREMENTS
Address Confirmation & Enrollment Code	• Valid records to confirm address SHALL be issuing source(s) or authoritative source(s). • The CSP SHALL confirm address of record. - The CSP SHOULD confirm address of record through validation of the address contained on any supplied, valid piece of identity evidence. - 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. • Self-asserted address data that has not been confirmed in records SHALL NOT be used for confirmation. • The CSP SHALL send an enrollment code to a confirmed address of record for the applicant. • The applicant SHALL present a valid enrollment code to complete the identity proofing process. • The CSP SHOULD send the enrollment code to the postal address that has been validated in records. - The CSP MAY send the enrollment code to a mobile telephone (short message service (SMS) or voice), landline telephone (voice), or email address, if the address has been validated in authoritative records. • If the enrollment code is also intendedto be an authentication factor, it SHALL be reset upon first use. • Enrollment codes SHALL have the following maximum validities: - 10 days when sent to a postal address of record within the contiguous U.S. - 30 days when sent to a postal address of record outside the contiguous U.S. - 10 minutes when sent to a telephone of record (SMS or voice) - 24 hours when sent to an email address of record • The CSP SHALL ensure the enrollment code and notification of proofing are sent to different addresses of record.	• The CSP SHALL confirm address of record. - The CSP SHOULD confirm address of record through validation of the address contained on any supplied, valid piece of identity evidence. - The CSP MAY confirm address of record by validating information supplied by the applicant, not contained on any supplied, valid piece of identity evidence. • Self-asserted address data SHALL NOT be used for confirmation. • A notification of proofing SHALL be sent to the confirmed address of record. • The CSP MAY provide an enrollment code directly to the subscriber if binding to an authenticator will occur at a later time. - The enrollment code SHALL be valid for a maximum of seven (7) days.

CATEGORY	IAL2 UNSUPERVISED REMOTE IDENTITY PROOFING REQUIREMENTS	IAL3 SUPERVISED REMOTE IN-PERSON IDENTITY PROOFING REQUIREMENTS
Biometric Collection	• The CSP MAY collect biometrics for the purposes of non-repudiation and re-proofing. See NIST SP 800-63B, Section 5.2.3, Use of Biometrics, for more detail on biometric collection.	• The CSP SHALL collect and record a biometric sample at the time of proofing (e.g., facial image, fingerprints) for the purposes of non-repudiation and re-proofing. See NIST SP 800-63B, Section 5.2.3, Use of Biometrics, for more detail on biometric collection.
Security Controls	• The CSP SHALL employ appropriately tailored security controls, including control enhancements, from the moderate or high baseline of security controls defined in NIST 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.	• The CSP SHALL employ appropriately tailored security controls, including control enhancements, from the high baseline of security controls defined in NIST SP 800-53 or an equivalent federal (e.g., FedRAMP) or industry standard. • The CSP SHALL ensure that the minimum assurance-related controls for ***high-impact*** systems or equivalent are satisfied.

THIS PAGE INTENTIONALLY LEFT BLANK

3 ENROLLMENT AND IDENTITY PROOFING PRACTICE STATEMENT TEMPLATES

This section provides templates that can be used by a CSP as a basis for documenting its enrollment and identity proofing processes in an Enrollment and Identity proofing Practice Statement (EIPPS) required by NIST SP 800-63A, Section 4.2 Requirement 6. The text has been written to provide the basic process flow to proof an applicant at either IAL2 Unsupervised Remote or IAL3 Supervised Remote In-Person identity proofing levels. The applicable requirements from NIST SP 800-63A, Sections 4 and 5, have been consolidated and are presented in Appendix A to provide a single list of requirements for the two remote assurance levels addressed in this document. These requirements are mapped into the process described in each template, which follows. Each agency, however, must consider its needs, resources, and capabilities carefully to ensure all requirements can be met.

Section 3.1 contains the template for IAL2 Unsupervised Remote Identity Proofing, and Section 3.2 contains the template for IAL3 Supervised Remote In-Person Identity Proofing. Where appropriate, the specific information required by the CSP should be documented within the EIPPS template. For example, the names of the core attributes along with definitions should be provided in the EIPPS. Each template is designed to document all processes used in enrollment and identity proofing as required by NIST SP 800-63A, Section 4.2 Requirement 6 by using the refined process flow shown below.

1. User Notification/Education and Acceptance
    a. What is collected and why?
    b. What will be done with the data collected?
    c. How will the data be protected?
    d. Record applicant acceptance.
2. Minimal Core Attribute/PII Collection
    a. Applicant provided identity data/PII claiming an identity.
3. Resolve to a Unique Identity
    a. CSP resolves claimed identity to a single, unique identity within the context of its population of users.
    b. KBV MAY be used to resolve to a unique, claimed identity.
4. Identity Evidence Collection/Capture
    a. Physical identity evidence is collected or captured.
5. Validation of Identity Evidence
    a. Identity evidence is genuine and authentic
    b. Contains information that is correct
    c. Contains information that pertains to a real-life subject.
6. Verification of Applicant to Claimed Identity
    a. Confirm and establish a linkage between the claimed identity and the real-life existence of the subject presenting the evidence.

3.1 IAL2 Unsupervised Remote Identity Proofing Template

This document is the <CSP Name> Enrollment and Identity Proofing Practices Statement (EIPPS) for documenting the processes used to enroll and proof applicants by using the IAL2 Unsupervised Remote Identity Proofing process requirements of NIST SP 800-63A. Upon successful completion of the processes described in this EIPPS, the applicant becomes a subscriber of <CSP> with a recorded digital identity at IAL2 that can be bound to AAL2 authenticators. This EIPPS was first approved for publication on <Approval date> by the <Approving Authority>. The following revisions have been made to the original document:

DATE	CHANGES	VERSION

This EIPPS has been certified as compliant with the IAL2 Unsupervised Remote Identity Proofing requirements of NIST SP 800-63A by <certifying organizations>.

Action: Document the organizations (such as a certifying organization like Kantara Initiative[1]) that have evaluated this identity assurance service, if any.

This EIPPS addresses the process that <CSP> follows to enroll and proof the identity of applicants at IAL2 in accordance with NIST SP 800-63A, IAL2 Unsupervised Remote Identity Proofing. <CSP> SHALL perform IAL2 Unsupervised Remote Identity Proofing with the applicant over a Transport Layer Security (https) encrypted channel initiated by the <CSP> when an applicant starts a session by using the following uniform resource locator (URL) in their browser:

<https://CSP/<remote.unsupervised.proofing.url>

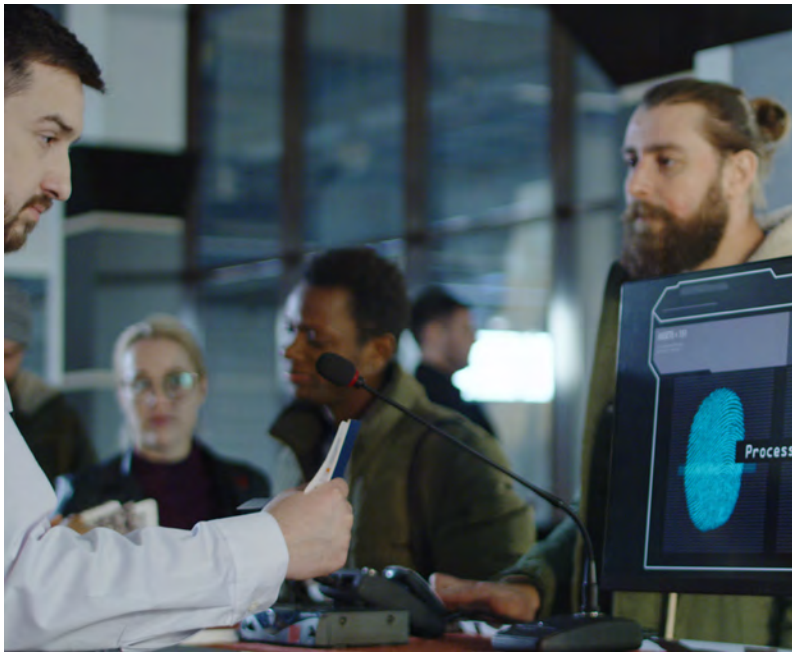
<CSP> maintains a record of all audit logs and steps taken to verify the identity of an applicant, capture a digital copy of the record, and record the types of identity evidence presented in the identity proofing process. For remote identity proofing, audit log files are generated for all security-relevant events relating to the identity proofing system, including capturing applicant input and the identity proofing system's handling of that data. it maintains records of which identity proofing system administrator (by name) accesses which records, including date and time. Security audit logs are automatically generated and collected. Collected logs are available for review for as long as <Time Period>. Security audit logs SHALL be retained and made available during all compliance audits.

Action: <CSP> maintains a risk management process, including assessments of privacy and security risks. In conducting the assessment of privacy and security risk for the identity proofing system solutions, the following points have been determined:

- <CSP> [will perform the additional steps listed below | will not perform any additional steps] to verify the identity of the applicant beyond the mandatory requirements specified in NIST SP 800-63.
- <CSP> will maintain a record of the identity proofing session and associated PII, including any biometrics, images, scans, or other copies of the identity evidence presented. (Note: Specific federal requirements [do | do not] apply.)
- The schedule of retention (e.g., current retention policies) for these records is in accordance with applicable laws, regulations, or policies.[2]

It is critical for a CSP to involve the sponsoring agency's senior agency official for privacy in the earliest stages of development of the identity-assurance proofing system, to assess and mitigate privacy risks. <CSP> has advised the agency on compliance requirements, such as whether the core attributes/PII collected during the identity proofing process trigger the Privacy Act of 1974 (Privacy Act) or the E-Government Act of 2002 (E-Gov) requirement to conduct a Privacy Impact Assessment (PIA).

Action: Per NIST SP 800-63A, Section 8, Privacy Considerations, document how <CSP> protects the PII of identity proofing applicants, subscribers, and other participants. Documentation should specifically address the following, to the extent pertinent under applicable law:



- Provide title and availability, including URL for downloading the applicable privacy plan applying to a participant's activities, if required by applicable law or policy
- Information that is or is not considered private
- Any responsibility of participants receiving private information to secure it and to refrain from using it and from disclosing it to third parties
- Any requirements as to notices to or consent from individuals regarding use or disclosure of private information
- Any circumstances under which a participant is entitled or required to disclose private information pursuant to judicial, administrative process in a private or governmental proceeding, or in any legal proceeding

3.1.1 Applicant Notification/ Education and Acceptance

This section explains what information will be requested from the applicant, why the information is being requested, how it will be used, how long it will be kept, and how it will be protected. It also explains what could happen if an applicant fails to provide all requested information, including possible unsuccessful identity proofing and what remediation steps the applicant may exercise. Finally, it asks the applicant to acknowledge they received notification and education on the enrollment and proofing process. Note applicant's notification, education and acceptance of the applicant SHALL be provided, including making this EIPPS accessible before the applicant is required to provide any identity information. This is depicted in Table 3-1 Applicant Notification/Education and Acceptance.

Action: Document the following details:

- How the applicant is notified of the need for the enrollment and identity proofing event
- How the applicant is educated about the enrollment and identity proofing event, including the information being requested, whether it is mandatory or optional, and what could happen should requested information not be provided
- Ensure the applicant understands the enrollment and identity proofing process, and capture/record their consent/ acceptance of the enrollment and identity proofing terms of service through, for example, a web acknowledgment form or a wet signature on hard-copy form.

Table 3-1. Applicant Notification/Education and Acceptance

DATE	CHANGES	VERSION

3.1.2 Core Attributes/PII Collection

<CSP> collects the core attributes from the applicant to establish a unique representation of the applicant's identity, which will be used as the basis to validate and verify that claimed identity to the individual presenting the information. Collection of these core attributes is intended to help resolve an applicant to a single, unique identity and to enable the appropriate level of verification and validation to support system risk mitigation and to meet appropriate IAL requirements.

Action: Using Table 3-2 as guidance, select a core attribute set that provides effective identity resolution, limits the number of attributes requested, and best balances the applicant's privacy and usability needs. Each attribute must be shown as mandatory or optional.

Table 3-3 depicts core attributes collected.

Table 3-2. Estimated Resolution Effectiveness for Various Attribute Combination Scenarios[3]

CORE ATTRIBUTES	SET 1	SET 2	SET 3	SET 4	SET 5
First Name	Y	Y	Y	Y	Y
Last Name		Y	Y	Y	Y
Middle Initial					Y
Full Date of Birth (DOB)			Y		Y
Partial DOB (YYYY or MMDD)		Y			
Year of Birth	Y				
Partial Address (Zip or City/State)		Y		Y	
Full Address					Y
Last 4 Digits of Social Security Number (SSN)				Y	Y
Estimated Resolution Effectiveness (%)	2.56	98.73	96.29	96.65	99.89

Table 3-3. Core Attributes Collected

ATTRIBUTE	DEFINITION	MANDATORY OR OPTIONAL	RETENTION PERIOD	PROTECTION

Attribute: Attribute collected

Definition: The meaning of the attribute being requested and any formats that must be used (e.g., date must be MM/DD/YYYY)

Mandatory or Optional:

- Mandatory: required to successfully complete process
- Optional: provides additional information that may assist in successful completion of process

Retention Period:

- Initial: just for identity proofing event
- Life: for the life of any issued credentials
- Other: Document any other retention period[4]
- Protection: How is the attribute protected to ensure the applicant's privacy?

Document any errors that may occur in this process and how they may be resolved.

- Document Errors Identified: As depicted in Table 3-4, document all errors that may occur, what technology or process will be used to resolve each error, and the Result/Outcome. Include format errors and incomplete data.

Table 3-4. Identified Errors and Resolutions

ERROR IDENTIFIED	TECHNOLOGY USED TO RESOLVE THE ERROR	RESULT/EXPECTED OUTCOME

3.1.3 Identity Resolution to Unique Individual

Action: As depicted in Table 3-5, document the CSP's procedures used to resolve the applicant to a unique identity based on the minimum set of core attributes/PII collected. One must also document any errors that may occur in this process and how they can be resolved.

Table 3-5. Identity Resolution Procedures

ATTRIBUTE	RESOLUTION TECHNIQUE	ISSUING/AUTHORITATIVE DATA SOURCES	RESOLVED (Y/N)?
		Resolved to Unique Identity (Y/N)?	

Attribute: Attribute collected

Resolution Technique: Resolution algorithm/rule or public database for KBV

Issuing/Authoritative Data Sources: Data sources to aid in identity resolution

Resolved (Y/N): Did core attribute collected assist in resolving the applicant to a unique identity?

Unique Identity Resolved (Y/N): Did the combination of core attributes collected resolve the applicant to a unique identity?

If yes, proceed to Collection of Identity Evidence.
If no: Was applicant already enrolled? Can the individual produce the enrollment code tied to the enrollment record? Is the enrollment code expired? Does another enrollment code need to be sent to address of record? *OR* is there a conflict? Is a fraudster attempting to use identity data to claim an identity belonging to someone else?

In the event an applicant fails identity proofing and/or is denied an authenticator based on the results of the identity proofing process, the CSP documents the mechanism for appeal or redress of the decision. (This is specified by NIST SP 800-63A, Section 4.2 Requirement 6)

Action: Describe the CSP's mechanisms for appeal or redress of the decision. What must the applicant do to continue the identity proofing process? Include control information detailing how the CSP handles proofing errors, for example, when an applicant is not successfully enrolled. Include information such as the number of retries allowed, proofing alternatives (e.g., in-person if remote fails), or fraud countermeasures when anomalies are detected.

Per NIST SP 800-63A, Section 4.2 Requirement 5, the CSP should also describe its process to receive and address applicant complaints about the proofing process.

Document Errors Identified: As depicted in Table 3-6, document all errors that may occur, what technology or process will be used to resolve each error, and the Result/Outcome. Example errors include missing or incomplete data, format errors, inability to confirm data with an authoritative source, and unresolved identity.

Table 3-6. Identified Errors and Resolutions

ERROR IDENTIFIED	TECHNOLOGY USED TO RESOLVE THE ERROR	RESULT/EXPECTED OUTCOME

3.1.4 Collection of Identity Evidence

To meet the goal of identity validation, collection or capture[5] of the most appropriate identity evidence (e.g., a passport or driver's license) from the applicant is required. Additionally, that identity evidence must meet the requirements for IAL2. (Reference: NIST SP 800-63A, Section 4.4.1.2, Evidence Collection Requirements, and Section 5.2.1, Identity Evidence Quality Requirements). See Appendix B for information on acceptable identity evidence.

Action: Document the evidence collected and its strength, the issuing agency, and the method of collection/capture, by using one of the three options below.

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

Examples of identity evidence for the three strengths of identity evidence that are acceptable at IAL2 are shown in Table 3-7. These examples were gathered from various federal government agencies in their preparation for implementing NIST SP 800-63A at the time this document was developed and does not represent NIST normative text for SP 800-63A or its accompanying volumes. MITRE highly recommends that the appropriate organization within the federal government interpret the quality of evidence requirements in NIST SP 800-63A and publish an official list of acceptable evidence at each level of strength to avoid conflicting interpretation by different CSPs.

Use Table 3-8 to document the identity evidence collected. Refer to Appendix B for justification of the strength of the evidence collected.

Table 3-7. Examples of Identity Evidence Based on Strength

STRENGTH OF IDENTITY EVIDENCE	EXAMPLES
Superior Identity Evidence	• U.S. Passport • Permanent Resident Card (issued on or after May 11, 2010) • Transportation Worker Identification Credential (TWIC) • Native American Enhanced Tribal Card • Personal Identity Verification (PIV) Card • Common Access Card (CAC)
Strong Identity Evidence	• Permanent Resident Card (issued prior to May 11, 2010) • State Driver's License or ID card (RealID-compliant) • Uniformed Services ID Card (includes Uniformed Services Dependent ID Cards)
Fair Identity Evidence	• Driver's License or ID card (non-RealID-compliant) • School ID Card with photograph • Utility Account Statement • Credit Card • Bank statement

Table 3-8. Collection of Identity Evidence

TYPE OF EVIDENCE COLLECTED	STRENGTH OF EVIDENCE	ISSUING ENTITY	COLLECTION/ CAPTURE METHOD

Type of Evidence Collected: List one, two, or three evidence type(s) based on actions 1-3 in Section 3.1.4.

Strength of Evidence: Record the strength of evidence as superior, strong, or fair based on actions 1-3 in Section 3.1.4.

Issuing Entity: Examples are U.S. agency, state agency, and a company that validates identity evidence.

Collection/Capture Method: As depicted in Table 3-9, document the methods used for collecting/capturing the identity evidence. Examples are an applicant's camera, flatbed scanner, and barcode scanner; and should include device manufacturer, model, and method of capture.

Table 3-9. Digital Identity Evidence Collection Methods

METHOD	DEVICE	INFORMATION
Photo Capture	Camera	This can be used to capture an applicant's photo or the image of evidence such as a driver's license. Agencies can consider pictures at 300 dpi or above to be of sufficient resolution.
Document Capture	Scanner	This can capture a document, which is compared against a known template by automated software to extract information. For optical character recognition, scans at high than 300 dpi are typically considered to be of sufficient quality.
Barcode	Scanner	Commercial off-the-shelf scanners can capture and extract information from standardized barcodes embedded on identity evidence.

The CSP must also document any errors identified in this process, if the errors were resolved, and how they were resolved.

Document Errors Identified: Based on Table 3-10, document all errors that may occur, what technology or process will be used to resolve the error, and the expected Result/Outcome. Examples are unacceptable image capture, inability to capture image, an applicant unable to produce acceptable identity evidence, and inability to read barcode.

Table 3-10. Identified Errors and Resolution

ERRORIDENTIFIED	TECHNOLOGY USED TO RESOLVE THE ERROR	RESULT/OUTCOME

3.1.5 Validation of Identity Evidence

This section documents the processes used to confirm that the evidence is authentic and that the data contained on the identity evidence is valid, current, and related to a real-life subject. The CSP will examine the identity evidence provided by the applicant and validate it against authoritative sources to determine that the presented evidence:

- Is authentic and not a counterfeit, fake, or a forgery
- Contains information that is correct
- Contains information that relates to a real-life subject

Validation of the accuracy, authenticity, and integrity of the type and strength of the identity evidence provided will be accomplished as described in Table 3-11.

Table 3-11. Methods of Validating Identity Evidence Based on Strength

STRENGTH	METHOD(S) OF VALIDATION
Fair	· Attributes contained in the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s) OR · The evidence has been confirmed as genuine: - By using appropriate technologies, confirm the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified *OR* - By trained personnel *OR* - By confirmation of the integrity of cryptographic security features
Strong	· The evidence has been confirmed as genuine: - By using appropriate technologies, confirm the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified *OR* - By trained personnel and appropriate technologies, confirm the integrity of the physical security features and that the evidence is not fraudulent or inappropriately modified *OR* - By confirmation of the integrity of cryptographic security features · All personal details and evidence details have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).
Superior	· The evidence has been confirmed as genuine by trained personnel and appropriate technologies, including the integrity of any physical and cryptographic security features. · All personal details and details from the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).

Action: Based on the strength of the identity evidence collected, document the method(s) used to validate the accuracy, authenticity, and integrity of the evidence against authoritative sources to determine it is authentic, correct, and relates to the unique individual.

Document whether existence of real-life subject has been verified by consulting vital statistic repositories such as the Death Master File (DMF).[6] Must also document any errors identified in this process and how or if they were resolved.

Table 3-12. Authenticity and Integrity of Identity Evidence

STRENGTH OF EVIDENCE COLLECTED	AUTHENTICITY/ INTEGRITY OF IDENTITY EVIDENCE	IDENTITY INFORMATION IS CORRECT	IDENTITY INFORMATION IS CONFIRMED TO REAL-LIFE SUBJECT

Strength of Evidence Collected: List the identity evidence collected in previous step.

Authenticity/Integrity of Identity Evidence: Based on Table 3-11, document the method(s) used to validate the authenticity of the identity evidence, including authoritative sources consulted; methods used to confirm integrity of identity evidence, such as evidence of tampering; validation of cryptographic security features; and whether trained personnel are responsible for validating the authenticity of the identity evidence presented. If trained personnel are used, the CSP should include documentation of the policies, guidelines, and requirements for those personnel.

Identity Information Is Correct: Based on Table 3-12, document the method(s) used to validate the accuracy of identity information contained in the identity evidence presented, including authoritative sources consulted.

Identity Information Is Confirmed to Real-Life Subject: Document the authoritative sources consulted to confirm existence of real-life subject, including any vital statistic repositories.

<CSP> has also identified the following errors that may occur during this process and will utilize the identified technologies to attempt to resolve the errors and provide any Results/ Outcomes the applicant can expect.

Document Errors Identified: Based on Table 3-13, document all errors that may occur, what technology or process will be used to resolve the errors, and the expected Result/Outcome. Examples are inability to validate authenticity, inability to validate integrity, and inability to confirm existence of real-life subject.

Table 3-13. Identified Errors and Resolutions

ERROR IDENTIFIED	TECHNOLOGY USED TO RESOLVE THE ERROR	RESULT/ OUTCOME	IDENTITY INFORMATION IS CONFIRMED TO REAL-LIFE SUBJECT

3.1.6 Verification of Applicant to Claimed Identity

At a minimum, the applicant's binding to identity evidence will be verified by a process that can achieve a strength of STRONG. KBV SHALL NOT be used to verify a claimed identity.

Action: <CSP> SHALL perform <choose one of the following> to verify the applicant's ownership of the claimed identity:

[physical comparison, using appropriate technologies, to a photograph, to the strongest piece of identity evidence provided to support the claimed identity. Physical comparison performed remotely SHALL adhere to all requirements as specified in NIST SP 800-63B, Section 5.2.3.]
OR
[biometric comparison, using appropriate technologies, of the applicant to the strongest piece of identity evidence provided to support the claimed identity. Biometric comparison performed remotely SHALL adhere to all requirements as specified in NIST SP 800-63B, Section 5.2.3.]

<CSP> has also identified the following errors may occur during this process and will utilize the identified technologies to attempt to resolve each error and provide any Results/Outcomes the applicant can expect.

Document Errors Identified: Based on Table 3-14, document all errors that may occur, what technology or process will be used to resolve each error, and the expected Result/Outcome. Examples are inability to capture acceptable image of applicant, inability to verify integrity, and inability to confirm existence of real-life subject.

Table 3-14. Identified Errors and Resolutions

ERROR IDENTIFIED	TECHNOLOGY USED TO RESOLVE THE ERROR	RESULT/OUTCOME

3.1.7 Address Confirmation and Enrollment Code

<CSP> will confirm the address of record; however, it will not accept a self-asserted address to verify a claimed identity. The address of record should be confirmed through validation of the address contained on any supplied valid piece of identity evidence. At <CSP> discretion, an address of record can be confirmed by validating information supplied by the applicant that is not part of the identity evidence presented by the applicant.

Action: <CSP> will send an enrollment code to a confirmed address of record for the applicant. The confirmed address of record for this CSP will be [postal address | mobile phone (SMS) | landline phone | email] for sending the enrollment code, which has been validated in records. NIST 800-63A, Section 4.4.1.6 states enrollment codes SHALL have the following maximum validities:

- 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 (mobile or landline)
- 24 hours when sent to an email address of record

The enrollment code is [intended to be an authentication factor and will be reset upon first use | not intended to be an authentication factor and does not need to be reset].

<CSP> will send a notification of proofing to [postal address | mobile phone via SMS | landline telephone | email], which is a different address of record from where the enrollment code was sent. (For example, if <CSP> sends an enrollment code to a phone number validated in records, the proofing notification will be sent to the postal address validated in records or obtained from validated and verified identity evidence.)

To complete the identity proofing process, the applicant must present a valid enrollment code within the validity periods below:

- 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 (mobile or landline)
- 24 hours when sent to an email address of record

Note: NIST SP 800-63A designates postal address as the preferred method of sending any communications, including enrollment code and notifications, to the applicant. However, to comply with the requirement to send enrollment code and notification of proofing to separate addresses of record, multiple verified addresses of record must be obtained to allow the applicant to complete the proofing process. Therefore, the guidelines will support any confirmed physical or digital address of record.

<CSP> has also identified the following errors that may occur during this process and will utilize the identified technologies to attempt to resolve each error and provide any results/outcomes that the applicant can expect.

Document Errors Identified: Based on Table 3-15, document all errors that may occur, what technology or process will be used to resolve each error, and the expected Result/Outcome. Examples are enrollment code not received by applicant, enrollment code received outside validity period, and postal mail returned as undeliverable.

Table 3-15. Identified Errors and Resolutions

ERROR IDENTIFIED	TECHNOLOGY USED TO RESOLVE THE ERROR	RESULT/OUTCOME

3.1.8 (Optional) Biometric Collection

A CSP may collect a biometric for nonrepudiation or reproofing, and to reestablish a link between an applicant and their enrollment record. See NIST SP 800-63B, Section 5.2.3 for more details on biometric collection.

Action: <CSP> SHALL document the process used to collect and record a biometric sample during the identity proofing process (e.g., facial image, fingerprints). See NIST SP 800-63B, Section 5.2.3 for more details. <CSP> must also document any errors identified in this process and how they were resolved.

3.1.9 Security Controls

As a CSP for the federal government, <CSP> SHALL satisfy federal system security requirements for the system(s) used to perform enrollment and identity proofing. Per requirements defined in the E-Government Act of 2002, Federal Information Processing Standards (FIPS) Pub 199, FIPS Pub 200, and NIST SP 800-53, <CSP> will document:

- FIPS Pub 199 security category of the enrollment and identity proofing system based on the security objectives and potential impacts to organizations and individuals
- Satisfactory execution for meeting minimum security requirements in FIPS Pub 200 based on the security system categorization
- Security controls employed in meeting a ***moderate-impact*** system, per NIST SP 800-53, and a copy of the System Security Plan <URL> describing all the security controls.

Note: NIST SP 800-63A allows for use of federal standards such as FedRAMP in place of NIST SP 800-53. The CSP should provide evidence that the system meets or exceeds ***moderate impact*** by using a documented set of controls from FedRAMP Security Assessment Framework.

3.2 IAL3 Supervised Remote In-Person Identity Proofing Template

This document is the <CSP Name> EIPPS for documenting the processes used to enroll and proof applicants by using the IAL3 Supervised Remote In-Person Identity Proofing process requirements of NIST SP 800-63A. Upon successful completion of the processes described in this EIPPS, the applicant becomes a subscriber of <CSP> with a recorded digital identity at IAL3 that can be bound to an AAL2 and AAL3 authenticator. This EIPPS was first approved for publication on <Approval date> by the <Approving Authority>. The following revisions have been made to the original document:

DATE	CHANGES	VERSION

This EIPPS has been certified as compliant with the IAL2 Unsupervised Remote Identity Proofing requirements of NIST SP 800-63A by <certifying organizations>.

Action: Document the organizations (such as certifying organization like Kantara Initiative[7]) that have evaluated this identity assurance service, if any.

IAL3 adds additional rigor to the steps required at IAL2, including providing further identity evidence of superior strength, and is subject to additional and specific processes (including the required 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 and duplicate enrollments and to reestablish binding to a credential. A CSP can employ remote proofing processes to achieve comparable levels of confidence and security for in-person events by adhering to the requirements provided in NIST SP 800-63A, Section 5.3.3.2.

This EIPPS addresses the process the <CSP> follows to enroll and proof the identity of applicants at IAL3 in accordance with NIST SP 800-63A, IAL3 Supervised Remote In-Person Identity Proofing. <CSP> SHALL perform IAL3 Supervised Remote In-Person Identity Proofing with the applicant over a mutually authenticated protected channel. Supervised Remote In-Person Identity Proofing by <CSP> is performed at the following locations:

<CSP facility and location>
<CSP kiosk and location>

High-resolution cameras will be used by a remote operator at these locations, to observe the applicant during the enrollment and proofing process. Once the applicant enters the enrollment and identity proofing area and initiates the session, they will not be allowed to leave the area until the session is completed. All actions taken by the applicant must be clearly visible to the remote operator. Failure to do so will result in the step having to be repeated or the session terminated.

<CSP> [will | will not] have integrated scanners and sensors for digital verification of identity evidence (e.g., chip reader or wireless technologies). Additionally, <CSP> employs physical tamper detection and resistance features appropriate for the environment in which the applicant enrollment kiosk is located.

<CSP> requires operators to undergo a training program to detect potential fraud and to properly perform a supervised remote proofing session. Document the location where all training documentation can be found.

<CSP> will document all processes used in enrollment and identity proofing per NIST SP 800-63A, Section 4.2 Requirement 6, and will maintain a record, including audit logs, of all steps taken to verify the identity of the applicant. <CSP> captures a digital copy and records the types of identity evidence presented in the identity proofing process. For remote identity proofing, audit log files are generated for all relevant security events relating to the identity proofing system, including capturing applicant input and the identity proofing system's handling of that data. It maintains records of which identity proofing system administrator (by name) accessed which records, including date and time. Security audit logs are automatically generated and collected. Collected logs are available for review for as long as <Time Period>. Security audit logs SHALL be retained and made available during all compliance audits.

Action: <CSP> maintains a risk management process, including assessments of privacy and security risks. In conducting the assessment of privacy and security risk for the identity proofing system solutions, the following has been determined:

- <CSP> [will perform the additional steps listed below | will not perform any additional steps] to verify the identity of the applicant beyond the mandatory requirements specified in NIST SP 800-63.
- <CSP> will maintain a record of the identity proofing session and associated PII, including any biometrics, images, scans, or other copies of the identity evidence presented. (Note: Specific federal requirements [do | do not] apply.)
- The schedule of retention (e.g., current retention policies) for these records is in accordance with applicable laws, regulations, or policies.[8]

A CSP must involve the sponsoring agency's senior agency official for privacy in the earliest stages of development of the identity assurance proofing system, to assess and mitigate privacy risks. <CSP> has advised the agency on compliance requirements, such as whether the core attributes/PII collected during the identity proofing process triggers the Privacy Act or the E-Gov requirement to conduct a PIA.

Action: Per NIST SP 800-63A, Section 8, Privacy Considerations, document how <CSP> protects the PII of identity proofing applicants, subscribers, and other participants. Documentation should specifically address the following, to the extent pertinent under applicable law:

- Provide title and availability, including URL for downloading applicable privacy plan applying to a participant's activities, if required by applicable law or policy
- Information that is or is not considered private

- Any responsibility of participants receiving private information to secure it and refrain from using and disclosing it to third parties
- Any requirements as to notices to or consent from individuals regarding use or disclosure of private information
- Any circumstances under which a participant is entitled or required to disclose private information pursuant to judicial or administrative process in a private or governmental proceeding, or in any legal proceeding

3.2.1 Applicant Notification/ Education and Acceptance

This section explains what information will be requested from the applicant, why the information is being requested, how it will be used, how long it will be kept, and how it will be protected. It also explains what could happen if an applicant fails to provide all requested information, including possible unsuccessful identity proofing and what remediation steps the applicant may exercise. Finally, it asks the applicant to acknowledge they received notification and education on the enrollment and proofing process. Note the applicant's notification and education and record the applicant's consent. This SHALL be provided, including making this EIPPS accessible before the applicant is required to provide any identity information.

Action: Per Table 3-16, document the following:

- How the applicant is notified of the enrollment and identity proofing event
- How the applicant is educated about the enrollment and identity proofing event, including the information being requested, whether it is mandatory or optional, and what could happen should requested information not be provided
- Ensure the applicant understands the enrollment and identity proofing process and capture/record their consent/acceptance of the enrollment and identity proofing terms of service through, for example, a web acknowledgment form or a wet signature on hard-copy form

Table 3-16. Applicant Notification/Education and Acceptance

APPLICANT	NOTIFICATION METHOD	EDUCATION METHOD	ACCEPTANCE METHOD

3.2.2 Core Attributes/PII Collection

<CSP> collects the core attributes from the applicant to establish a unique representation of the applicant's identity, which will be used as the basis to validate and verify that claimed identity to the individual presenting the information. Collection of these core attributes is intended to help resolve applicants to a single unique identity, and to enable the appropriate level of verification and validation to support system risk mitigation and to meet appropriate IAL requirements.

Action: Using Table 3-17 as guidance, select a core attribute set that provides effective identity resolution from the community, limits the number of attributes requested, and best balances the applicant's privacy and usability needs. Each attribute must be shown as mandatory or optional. Use Table 3-18 to document the core attributes collected.

Table 3-17. Estimated Resolution Effectiveness for Various Attribute CombinationScenarios[9]

CORE ATTRIBUTES	SET 1	SET 2	SET 3	SET 4	SET 5
First Name	Y	Y	Y	Y	Y
Last Name		Y	Y	Y	Y
Middle Initial					Y
Full DOB			Y		Y
Partial DOB (YYYY or MMDD)		Y			
Year of Birth	Y				
Partial Address (Zip or City/State)		Y		Y	
Full Address					Y
Last 4 Digits of SSN				Y	Y
Estimated Resolution Effectiveness (%)	2.56	98.73	96.29	96.65	99.89

Table 3-18. Core Attributes Collected

ATTRIBUTE	DEFINITION	MANDATORY OR OPTIONAL	RETENTION PERIOD	PROTECTION

Attribute: Attribute collected

Definition: the meaning of the attribute being requested and any formats that must be used (e.g., date must be MM/DD/YYYY)

- **Mandatory or Optional**
  - Mandatory: required to successfully complete process
  - Optional: provides additional information that may assist in successful completion of process
- **Retention Period**
  - Initial: just for identity proofing event
  - Life: for the life of any issued credentials
  - Other: Document any other retention period[10]
- **Protection:** How is the attribute protected to ensure the applicant's privacy?

Document any errors that may occur in this process and how they may be resolved.

Document Errors Identified: Based on Table 3-19, document all errors that may occur, what technology or process will be used to resolve the errors, and the Result/Outcome. Examples are format errors and incomplete data.

Table 3-19. Identified Errors and Resolutions

ERROR IDENTIFIED	TECHNOLOGY USED TO RESOLVE THE ERROR	RESULT/EXPECTED OUTCOME

3.2.3 Resolution to Unique Identity

Action: Based on Table 3-20, document CSP's procedures used to resolve the applicant to a unique identity based on the minimum set of core attributes/PII collected. Must also document any errors that may occur in this process and how they can be resolved.

Table 3-20. Identity Resolution Procedures

ATTRIBUTE	RESOLUTION TECHNIQUE	ISSUING/AUTHORITATIVE DATA SOURCES	RESOLVED (Y/N)?
		Resolved to Unique Identity (Y/N)?	

Attribute: Attribute collected

Resolution Technique: Resolution algorithm/ rule used, or public database used for KBV

Issuing/Authoritative Data Sources: Data sources used to aid in identity resolution

Resolved (Y/N): Did core attribute collected assist in resolving the applicant to a single, unique identity within the context of the population of users the CSP serves?

Unique Identity Resolved (Y/N): Did the combination of core attributes collected resolve the applicant to a unique identity?

If yes, proceed to Collection of Identity Evidence.
If no: Was applicant already enrolled? Can the individual produce the enrollment code tied to the enrollment record? Is the enrollment code expired? Does another enrollment code need to be sent to address of record?
OR is there a conflict?
Is a fraudster attempting to use identity data to claim an identity belonging to someone else?

In the event an applicant fails identity proofing and/or is denied an authenticator based on the results of the identity proofing process, a CSP must document the mechanism for appeal or redress of the decision. (This is required by NIST SP 800-63A, Section 4.2 Requirement 6.)

Action: Describe the CSP's mechanisms for appeal or redress of the decision. What must the applicant do to continue the identity proofing process? Include control information detailing how the CSP handles proofing errors, for example, when an applicant is not successfully enrolled. Include information such as the number of retries allowed, proofing alternatives (e.g., in-person if remote fails), or fraud countermeasures when anomalies are detected.

Per NIST SP 800-63A, Section 4.2 Requirement 5, the CSP should also describe its process to receive and address applicant complaints about the proofing process.

Document Errors Identified: As shown in Table 3-21, document all errors that may occur, what technology or process will be used to resolve each error, and the Result/Outcome. Example errors include missing or incomplete data, format errors, inability to confirm data with authoritative source, and unresolved identity.

Table 3-21. Identified Errors and Resolutions

ERROR IDENTIFIED	TECHNOLOGY USED TO RESOLVE THE ERROR	RESULT/OUTCOME

3.2.4 Collection of Identity Evidence

To meet the goal of identity validation, collection or capture[11] of the most appropriate identity evidence (e.g., a passport or driver's license) from the applicant is required. Additionally, that identity evidence must meet the requirements for IAL3 Identity Evidence Quality. (Reference: NIST SP 800-63A, Section 4.5.2 and Section 5.2.1). See Appendix B for information on acceptable identity evidence.

Action: Document the evidence collected and its strength, the issuing agency, and the method of collection/capture by using one of the following three options:

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.

Table 3-22 provides examples of identity evidence based on the strengths acceptable for IAL3. These examples were gathered from various federal government agencies in their preparation for implementing NIST SP 800-63A at the time this document was developed and does not represent NIST normative text for SP 800-63A or its accompanying volumes. MITRE highly recommends that the appropriate organization within the federal government interpret the quality of evidence requirements in NIST SP 800-63A and publish an official list of acceptable evidence at each level of strength to avoid conflicting interpretation by different CSPs.

Table 3-22. Examples of Identity Evidence Based on Type

STRENGTH OF IDENTITY EVIDENCE*	EXAMPLES
Superior Identity Evidence	• U.S. passport • Permanent Resident Card (issued on or after May 11, 2010) • TWIC • Native American Enhanced Tribal Card • PIV Card • CAC
Strong Identity Evidence	• Permanent Resident Card (issued prior to May 11, 2010) • State driver's license or ID card (RealID-compliant) • Uniformed Services ID Card (includes Uniformed Services Dependent ID Cards)
Fair Identity Evidence	• Driver's license or ID card (non-RealID-compliant) • School ID card with photograph • Utility account statement • Credit card • Bank statement

* See Appendix B for justification of strength of identity evidence.

Table 3-23. Collection of Identity Evidence

TYPE OF EVIDENCE COLLECTED	STRENGTH OF EVIDENCE	ISSUING ENTITY	COLLECTION/CAPTURE METHOD

Type of Evidence Collected: As shown in Table 3-23, list one, two, or three evidence type(s) based on actions 1–3 in section 3.2.4. Examples of identity evidence for the three types of identity evidence are shown in Table 3-22.

Strength of Evidence: Record the strength of evidence as superior, strong, or fair based on actions 1–3 in Section 3.2.4.

Issuing Entity: Examples are U.S. agency, state agency, and a company that validates identity evidence.

Collection/Capture Method: Document the methods used for collecting/capturing the identity evidence. Examples are an applicant's camera, flatbed scanner, and barcode scanner, and should include device manufacturer, model, and method of capture.

The CSP must also document any errors identified in this process, if the errors were resolved, and how they were resolved.

Document Errors Identified: Based on Table 3-24, document all errors that may occur, what technology or process will be used to resolve each error, and the expected Result/Outcome. Examples are unacceptable image capture, inability to capture image, an applicant unable to produce acceptable identity evidence, and inability to read barcode.

Table 3-24. Identified Errors and Resolutions

ERROR IDENTIFIED	TECHNOLOGY USED TO RESOLVE THE ERROR	RESULT/OUTCOME

3.2.5 Validation of Identity Evidence

This section documents the processes used in confirming that the evidence is authentic and that the data contained on the identity evidence is valid, current, and related to a real-life subject. The CSP will examine the identity evidence provided by the applicant and validate it against authoritative sources to determine that the presented evidence:

- Is authentic and not a counterfeit, fake, or a forgery
- Contains information that is correct
- Contains information that relates to a real-life subject

Validation of the accuracy, authenticity, and integrity of the identity evidence provided for the types of identity evidence provided will be accomplished as described in Table 3-25.

Table 3-25. Methods of Validating Identity Evidence Based on Strength

STRENGTH	METHOD(S) OF VALIDATION
Fair	• Attributes contained in the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s) *OR* • The evidence has been confirmed as genuine: - By using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified *OR* - By trained personnel *OR* - By confirmation of the integrity of cryptographic security features.
Strong	• The evidence has been confirmed as genuine: - By using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified *OR* - By trained personnel and appropriate technologies, confirming the integrity of the physical security features and that the evidence is not fraudulent or inappropriately modified *OR* • By confirmation of the integrity of cryptographic security features. All personal details and evidence details have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).
Superior	• The evidence has been confirmed as genuine by trained personnel and appropriate technologies, including the integrity of any physical and cryptographic security features. • All personal details and details from the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).

Action: Based on the strength of the collected identity evidence, document the method(s) used to validate the accuracy, authenticity, and integrity of the evidence against authoritative sources to determine that it is authentic and correct and that it relates to the unique identity.

Per Table 3-26, document whether existence of a real-life subject has been verified by consulting vital statistic repositories such as the DMF.[12] Must also document any errors that may occur in this process and how they can be resolved.

Table 3-26. Authenticity and Integrity of Identity Evidence

STRENGTH OF EVIDENCE COLLECTED	AUTHENTICITY/ INTEGRITY OF IDENTITY EVIDENCE	IDENTITY INFORMATION IS CORRECT	IDENTITY INFORMATION IS CONFIRMED TO REAL-LIFE SUBJECT

Strength of Evidence Collected: List the identity evidence collected in the previous step.

Authenticity/Integrity of Identity Evidence: Based on Table 3-26, document the method(s) used to validate the authenticity of the identity evidence, including authoritative sources consulted; methods used to confirm integrity of identity evidence, such as evidence of tampering; validation of cryptographic security features; and whether trained personnel are responsible for validating the authenticity of the identity evidence presented. If trained personnel are used, the CSP should include documentation of the policies, guidelines, and requirements for those personnel.

Identity Information Is Correct: Based on Table 3-26, document the method(s) used to validate that the identity information contained in the identity evidence presented is correct, including authoritative sources consulted.

Identity Information Is Confirmed to Real-Life Subject: Document the authoritative sources consulted to confirm existence of real-life subject, including any vital statistic repositories.

<CSP> has also identified the following errors that may occur during this process and will utilize the identified technologies to attempt to resolve each error and provide any Results/ Outcomes the applicant can expect.

Document Errors Identified: Per Table 3-27, document all errors that may occur, what technology or process will be used to resolve each error, and the expected result/outcome. Examples are inability to validate authenticity, inability to validate integrity, and inability to confirm existence of real-life subject.

Table 3-27. Identified Errors and Resolutions

ERROR IDENTIFIED	TECHNOLOGY USED TO RESOLVE THE ERROR	RESULT/OUTCOME

3.2.6 Verification of Applicant to Claimed Identity

At a minimum, the applicant's binding to identity evidence will be verified by a process that can achieve a strength of SUPERIOR. KBV SHALL NOT be used for Supervised Remote In-Person Identity Proofing to verify a claimed identity.

Action: To verify the applicant's ownership of the claimed identity, <CSP> SHALL perform biometric comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity, using appropriate technologies. Biometric comparison will adhere to all requirements as specified in NIST SP 800-63B, Section 5.2.3, Use of Biometrics.

<CSP> has also identified the following errors that may occur during this process and will utilize the identified technologies to attempt to resolve each error and provide any Results/Outcomes the applicant can expect.

Document Errors Identified: Based on Table 3-28, document all errors that may occur, what technology or process will be used to resolve each error, and the expected result/outcome. Examples are inability to capture acceptable image of applicant, inability to verify integrity, and inability to confirm existence of real-life subject.

Table 3-28. Identified Errors and Resolutions

ERROR IDENTIFIED	TECHNOLOGY USED TO RESOLVE THE ERROR	RESULT/OUTCOME

3.2.7 Address Confirmation and Enrollment Code

<CSP> will confirm the address of record; however, it will not accept a self-asserted address to verify a claimed identity. The address of record should be confirmed through validation of the address contained on any supplied valid piece of identity evidence. At <CSP> discretion, an address of record can be confirmed by validating information supplied by the applicant that is not part of the identity evidence presented by the applicant.

Action: <CSP> will provide an enrollment code directly to the subscriber if binding to an authenticator will occur later. If an enrollment code is provided, it will be valid for a maximum of only seven days. <CSP> will also send a notification of proofing to the postal address of record that has been validated in records or obtained from validated and verified identity evidence.

<CSP> has also identified the following errors that may occur during this process and will utilize the identified technologies to attempt to resolve each error and provide any Results/ Outcomes the applicant can expect.

Document Errors Identified: Based on Table 3-29, document all errors that may occur, what technology or process will be used to resolve each error, and the expected result/outcome. Examples are enrollment code not received by applicant, enrollment code received outside validity period, and postal mail returned as undeliverable.

Table 3-29. Identified Errors and Resolutions

ERROR IDENTIFIED	TECHNOLOGY USED TO RESOLVE THE ERROR	RESULT/OUTCOME

3.2.8 Biometric Collection

Action: <CSP> will collect and record a biometric sample at the time of proofing for nonrepudiation, reproofing, and to reestablish a link between an applicant and their enrollment record. The biometric to be collected will be <chosen biometric>. Consult NIST SP 800-63B, Section 5.2.3 for more detail on biometric collection.

<CSP> has also identified the following errors that may occur during this process and will utilize the identified technologies to attempt to resolve each error and provide any Results/ Outcomes the applicant can expect.

Document Errors Identified: Based on Table 3-30, document all errors that may occur, what technology or process will be used to resolve each error, and the expected Result/Outcome. Examples are enrollment code not received by applicant, enrollment code received outside validity period, and postal mail returned as undeliverable.

Table 3-30. Identified Errors and Resolutions

ERROR IDENTIFIED	TECHNOLOGY USED TO RESOLVE THE ERROR	RESULT/OUTCOME

3.2.9 Security Controls

As a CSP for the federal government, <CSP> SHALL satisfy federal system security requirements for the system(s) used to perform enrollment and identity proofing. Per requirements defined in the E-Government Act of 2002, FIPS Pub 199, FIPS Pub 200, and NIST SP 800-53, <CSP> will document:

- Security category of the enrollment and identity proofing system based on the security objectives and potential impacts to organizations and individuals on the criteria in FIPS Pub 199
- Satisfactory execution for meeting minimum security requirements in FIPS Pub 200 based on the security system categorization
- Security controls employed in meeting a ***high-impact*** system as defined in NIST SP 800-53. A copy of the System Security Plan describing all the security controls used is located at <URL>.

Note: NIST SP 800-63A allows for the use of federal standards such as FedRAMP in place of NIST SP 800-53. The CSP should provide evidence that the system meets or exceeds ***high impact*** by using a documented set of controls from FedRAMP Security Assessment Framework.

4 SUMMARY

This document provided templates that will assist CSPs in documenting their processes for enrollment and remotely identity proofing of applicants requiring access to U.S. government online resources. The two assurance levels below were documented in this Identity Proofing Practice Statement.

- IAL2 Unsupervised Remote Identity Proofing
- IAL3 Supervised Remote In-Person Identity Proofing

By following the procedures in this Enrollment and Identity Proofing Practice Statement and documenting the information requested in the templates, a CSP can fulfill the NIST SP 800-63A, Section 4.2 Requirement 6 for written policy specifying the steps taken to resolve, validate, and verify digital identities. These templates document a consistent repeatable process and provide evidence of processes leading to one of the required identity assurance levels above.
The templates also serve as source information to applicants for acceptable identity proofing practices, the type of acceptable identity evidence they should provide, and the steps to take should the identity evidence provided be rejected.

Appendix A | Requirements for IAL2 Unsupervised Remote and IAL3 Supervised Remote In-Person Identity Proofing

This appendix provides the requirements for enrolling and proofing the identity of an applicant at either Identity Assurance Level (IAL) 2 Unsupervised Remote or IAL3 Supervised Remote In-Person identity proofing levels (see Table A-1). The applicable requirements from the National Institute of Standards and Technology Special Publication 800-63A, Sections 4 and 5, have been consolidated and are presented in Appendix A to provide a single list of requirements for the two identity assurance levels addressed in this document. These requirements are mapped into the processes described in each template in Section 3.

Table A-1. Consolidated Requirements for IAL2 and IAL

CATEGORY	IAL2 UNSUPERVISED REMOTE IDENTITY PROOFING REQUIREMENTS	IAL3 SUPERVISED REMOTE IN-PERSON IDENTITY PROOFING REQUIREMENTS
Notification, Education, and Acceptance	• 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. • Record applicant acceptance.	Same as IAL2
Core Attribute Collection	• Collection of core attributes/PII should be limited to the minimum necessary to resolve a unique identity record. This MAY include collection of attributes assisting in data queries.	Same as IAL2
Identity Resolution	• Uniquely distinguish an individual within a given population or context by using the minimum attributes necessary. • MAY employ matching algorithms, which should be publicly available or included in practice statement. • Knowledge-based verification (KBV) MAY be used to resolve to a unique, claimed identity.	Same as IAL2
Identity Evidence Collection	• One (1) piece of SUPERIOR or STRONG evidence, depending on strength of original proof, and validation occurs with issuing source *OR* • Two (2) pieces of STRONG evidence *OR* • One (1) piece of STRONG evidence plus two (2) pieces of FAIR evidence	• Two (2) pieces of SUPERIOR evidence *OR* • One (1) piece of SUPERIOR evidence plus one (1) piece of STRONG evidence, depending on strength of original proof, and validation occurs with issuing source *OR* • Two (2) pieces of STRONG evidence plus one (1) piece of FAIR evidence

CATEGORY	IAL2 UNSUPERVISED REMOTE IDENTITY PROOFING REQUIREMENTS	IAL3 SUPERVISED REMOTE IN-PERSON IDENTITY PROOFING REQUIREMENTS
Qualities of Identity Evidence – FAIR	• The issuing source of the evidence confirmed the claimed identity through an identity proofing process. • The issuing process for the evidence means that it can reasonably be assumed to have been delivered into the possession of the person to whom it relates. • The evidence contains at least one (1) reference number that uniquely identifies the person to whom it relates *OR* • Contains a photograph or biometric template (any modality) of the person to whom it relates *OR* • Can have ownership confirmed through KBV • Where the evidence includes digital information, that information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed. • Where the evidence includes physical security features, it requires proprietary knowledge to be able to reproduce it. • The issued evidence is unexpired.	Same as IAL2
Qualities of Identity Evidence – STRONG	• The issuing source of the evidence confirmed the claimed identity through written procedures designed to enable it to form a reasonable belief that it knows the real-life identity of the person. • The issuing process for the evidence ensured it was delivered into the possession of the subject to whom it relates. • The issued evidence contains at least one reference number that uniquely identifies the person to whom it relates. • The full name on the issued evidence must be the name that the person was officially known by at the time of issuance. • The issued evidence contains a photograph or biometric template (of any modality) of the person to whom it relates *OR* • The applicant proves possession of an AAL2 authenticator, or equivalent, bound to an IAL2 identity, at a minimum. • Where the issued evidence includes digital information, that information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed. • Where the issued evidence contains physical security features, it requires proprietary knowledge and proprietary technologies to be able to reproduce it. • The evidence is unexpired.	Same as IAL2

CATEGORY	IAL2 UNSUPERVISED REMOTE IDENTITY PROOFING REQUIREMENTS	IAL3 SUPERVISED REMOTE IN-PERSON IDENTITY PROOFING REQUIREMENTS
Qualities of Identity Evidence – SUPERIOR	• The issuing source of the evidence confirmed the claimed identity by following written procedures designed to enable it to have high confidence that the source knows the real-life identity of the subject. • The issuing source visually identified the applicant and performed further checks to confirm the existence of that person. • The issuing process for the evidence ensured it was delivered into the possession of the person to whom it relates. • The evidence contains at least one reference number that uniquely identifies the person to whom it relates. • The full name on the evidence must be the name that the person was officially known by at the time of issuance. • The evidence contains a photograph of the person to whom it relates. • The evidence contains a biometric template (of any modality) of the person to whom it relates. • The evidence includes digital information, the information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the issuing source to be confirmed. • The evidence includes physical security features that require proprietary knowledge and proprietary technologies to be able to reproduce it. • The evidence is unexpired.	Same as IAL2
Identity Evidence Validation	• 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 evidence will be validated at a strength of STRONG. • Training requirements for personnel validating evidence SHALL be based on the policies, guidelines, or requirements of the CSP or RP.	• Each piece of evidence must be validated with a process that is able to achieve the same strength as the evidence presented. • Training requirements for personnel validating evidence SHALL be based on the policies, guidelines, or requirements of the CSP or RP.
Identity Evidence Validation – FAIR	• The evidence details have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s) *OR* • Has been confirmed as genuine using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified *OR* • Has been confirmed as genuine by trained personnel *OR* • Has been confirmed as genuine by confirmation of the integrity of cryptographic security features.	Same as IAL2

CATEGORY	IAL2 UNSUPERVISED REMOTE IDENTITY PROOFING REQUIREMENTS	IAL3 SUPERVISED REMOTE IN-PERSON IDENTITY PROOFING REQUIREMENTS
Identity Evidence Validation – STRONG	• The evidence has been confirmed as genuine using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified *OR* • By trained personnel and appropriate technologies, confirming the integrity of the physical security features and that the evidence is not fraudulent or inappropriately modified *OR* • By confirmation of the integrity of cryptographic security features. • All personal details and evidence details have been confirmed as valid by comparison with information held.	Same as IAL2
Identity Evidence Validation – SUPERIOR	• The evidence has been confirmed as genuine by trained personnel and appropriate technologies including the integrity of any physical and cryptographic security features. • All personal details and evidence details from the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).	Same as IAL2
Identity Evidence Verification	• At a minimum, the applicant must be verified by a process that is able to achieve a strength of STRONG • The applicant's ownership of the claimed identity has been confirmed by: - Physical comparison, using appropriate technologies, to a photograph, to the strongest piece of identity evidence provided to support the claimed identity. Physical comparison performed remotely SHALL adhere to all requirements as specified in NIST SP 800-63B, Section 5.2.3, Use of Biometrics, *OR* - Biometric comparison, using appropriate technologies, of the applicant to the strongest piece of identity evidence provided to support the claimed identity. Biometric comparison performed remotely SHALL adhere to all requirements as specified in NIST SP 800-63B, Section 5.2.3, Use of Biometrics.	• 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. • KBV SHALL NOT be used for in-person (supervised remote) identity verification. • The applicant's ownership of the claimed identity has been confirmed by: - Biometric comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity, using appropriate technologies. - Biometric comparison performed remotely SHALL adhere to all requirements as specified in NIST SP 800-63B, Section 5.2.3, Use of Biometrics.
Identity Evidence Verification – STRONG	• Biometric comparison of the applicant to the identity evidence. Biometric comparison performed remotely SHALL adhere to all requirements as specified in NIST SP 800-63B, Section 5.2.3, Use of Biometrics.	N/A

CATEGORY	IAL2 UNSUPERVISED REMOTE IDENTITY PROOFING REQUIREMENTS	IAL3 SUPERVISED REMOTE IN-PERSON IDENTITY PROOFING REQUIREMENTS
Presence	Remote Unsupervised	• Supervised Remote In-person Proofing • 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. • The CSP SHALL have a live operator participate remotely with the applicant for the entirety of the identity proofing session. • The CSP SHALL require all actions taken by the applicant during the identity proofing session to be clearly visible to the remote operator. • The CSP SHALL require that all digital verification of evidence (e.g., via chip or wireless technologies) be performed by integrated scanners and sensors. • The CSP SHALL require operators to have undergone a training program to detect potential fraud and to properly perform a supervised remote proofing session. • The CSP SHALL employ physical tamper detection and resistance features appropriate for the environment in which it is located. For example, a kiosk located in a restricted area or one where it is monitored by a trusted individual requires less tamper detection than one in a semi-public area such as a shopping mall concourse. • The CSP SHALL ensure all communications occur over a mutually authenticated protected channel.

CATEGORY	IAL2 UNSUPERVISED REMOTE IDENTITY PROOFING REQUIREMENTS	IAL3 SUPERVISED REMOTE IN-PERSON IDENTITY PROOFING REQUIREMENTS
Address Confirmation and Enrollment Code	• Valid records to confirm address SHALL be issuing source(s) or authoritative source(s). • The CSP SHALL confirm address of record. - The CSP SHOULD confirm address of record through validation of the address contained on any supplied, valid piece of identity evidence. - 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. • Self-asserted address data that has not been confirmed in records SHALL NOT be used for confirmation. • The CSP SHALL send an enrollment code to a confirmed address of record for the applicant. • The applicant SHALL present a valid enrollment code to complete the identity proofing process. • The CSP SHOULD send the enrollment code to the postal address that has been validated in records. - The CSP MAY send the enrollment code to a mobile telephone (short message service (SMS) or voice), landline telephone (voice), or email address, if the address of the mobile phone, landline phone number, or email address has been validated in authoritative records. • If the enrollment code is also intended to be an authentication factor, it SHALL be reset upon first use. • Enrollment codes SHALL have the following maximum validities: - 10 days when sent to a postal address of record within the contiguous U.S. - 30 days when sent to a postal address of record outside the contiguous U.S. - 10 minutes when sent to a telephone of record (SMS or voice) - 24 hours when sent to an email address of record • The CSP SHALL ensure the enrollment code and notification of proofing are sent to different addresses of record.	• The CSP SHALL confirm address of record. - The CSP SHOULD confirm address of record through validation of the address contained on any supplied, valid piece of identity evidence. - The CSP MAY confirm address of record by validating information supplied by the applicant, not contained on any supplied, valid piece of identity evidence. • Self-asserted address data SHALL NOT be used for confirmation. • A notification of proofing SHALL be sent to the confirmed address of record. • The CSP MAY provide an enrollment code directly to the subscriber if binding to an authenticator will occur at a later time. - The enrollment code SHALL be valid for a maximum of seven (7) days.
Biometric Collection	• The CSP MAY collect biometrics for the purposes of non-repudiation and re-proofing. See NIST SP 800-63B, Section 5.2.3, Use of Biometrics, for more detail on biometric collection.	• The CSP SHALL collect and record a biometric sample at the time of proofing (e.g., facial image, fingerprints) for the purposes of non-repudiation and re-proofing. See NIST SP 800-63B, Section 5.2.3, Use of Biometrics, for more detail on biometric collection.

CATEGORY	IAL2 UNSUPERVISED REMOTE IDENTITY PROOFING REQUIREMENTS	IAL3 SUPERVISED REMOTE IN-PERSON IDENTITY PROOFING REQUIREMENTS
Security Controls	• The CSP SHALL employ appropriately tailored security controls, including control enhancements, from the moderate or high baseline of security controls defined in NIST 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.	• The CSP SHALL employ appropriately tailored security controls, including control enhancements, from the high baseline of security controls defined in NIST SP 800-53 or an equivalent federal (e.g., FedRAMP) or industry standard. • The CSP SHALL ensure that the minimum assurance-related controls for ***high-impact*** systems or equivalent are satisfied.

Appendix B | Identity Evidence

Table B-1. provides examples of evidence from each category of strength defined in the identity evidence quality table in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63A. For each example at strength levels superior through fair, justifications for the strength level have been provided.

Please note, examples of unacceptable and weak evidence are presented here for the sake of completeness. They should not be used for identity proofing at Identity Assurance Level (IAL) 2 and IAL3.

Agencies are cautioned to review guidance on international or common names and name changes while considering evidence for strength.

Table B-1. Evidence Strengths and Examples

EXAMPLE	STRENGTH	JUSTIFICATION
U.S. Passport	SUPERIOR	• Issuing source confirmed claimed identity by following written procedures. • Issuing source visually identified applicant. • Issuing process ensured it was delivered into possession of the person. • Contains at least one reference number. • Contains full name. • Contains photograph. • Contains biometric template. • Includes digital information. • Includes physical security features. • Unexpired.
Permanent Resident Card (Issued on or after May 11, 2010)	SUPERIOR	• Issuing source confirmed claimed identity by following written procedures. • Issuing source visually identified applicant. • Issuing process ensured it was delivered into possession of the person. • Contains at least one reference number. • Contains full name. • Contains photograph. • Contains biometric template. • Includes physical security features. • Unexpired.

EXAMPLE	STRENGTH	JUSTIFICATION
Transportation Worker Identification Credential	SUPERIOR	• Issuing source confirmed claimed identity by following written procedures. • Issuing source visually identified applicant. • Issuing process ensured it was delivered into possession of the person. • Contains at least one reference number. • Contains full name. • Contains photograph. • Contains biometric template. • Includes digital information. • Includes physical security features. • Unexpired.
Native American Enhanced Tribal Card	SUPERIOR	• Issuing source confirmed claimed identity by following written procedures. • Issuing source visually identified applicant. • Issuing process ensured it was delivered into possession of the person. • Contains at least one reference number. • Contains full name. • Contains photograph. • Can contain biometric template. • Includes digital information. • Includes physical security features. • Unexpired.
Personal Identity Verification (PIV) Card	SUPERIOR	• Issuing source confirmed claimed identity by following written procedures. • Issuing source visually identified applicant. • Issuing process ensured it was delivered into possession of the person. • Contains at least one reference number. • Contains full name. • Contains photograph. • Contains biometric template. • Includes digital information. • Includes physical security features. • Unexpired.
Common Access Card (CAC)	SUPERIOR	• Issuing source confirmed claimed identity by following written procedures. • Issuing source visually identified applicant. • Issuing process ensured it was delivered into possession of the person. • Contains at least one reference number. • Contains full name. • Contains photograph. • Contains biometric template. • Includes digital information. • Includes physical security features. • Unexpired.

EXAMPLE	STRENGTH	JUSTIFICATION
PIV-Interoperable Card	SUPERIOR	• Issuing source confirmed claimed identity by following written procedures. • Issuing source visually identified applicant. • Issuing process ensured it was delivered into possession of the person. • Contains at least one reference number. • Contains full name. • Contains photograph. • Contains biometric template. • Includes digital information. • Includes physical security features. • Unexpired.
Permanent Resident Card (Issued prior to May 11, 2010)	STRONG	• Issuing source confirmed claimed identity by following written procedures. • Issuing source visually identified applicant. • Issuing process ensured it was delivered into possession of the person. • Contains at least one reference number. • Contains full name. • Contains photograph. • Includes physical security features. • Unexpired.
Driver's License or ID Card (RealID-compliant)	STRONG	• Issuing source confirmed claimed identity by following written procedures. • Issuing source visually identified applicant. • Issuing process ensured it was delivered into possession of the person. • Contains at least one reference number. • Contains full name. • Contains photograph. • Includes digital information. • Includes physical security features. • Unexpired.
Uniformed Services ID Card (includes Uniformed Services Dependent ID Card)	STRONG	• Issuing source confirmed claimed identity by following written procedures. Issuing source visually identified applicant. • Issuing process ensured it was delivered into possession of the person. • Contains at least one reference number. • Contains full name. • Contains photograph. • Includes digital information. • Includes physical security features. • Unexpired.

EXAMPLE	STRENGTH	JUSTIFICATION
Native American Tribal Photo ID Card	STRONG	• Issuing source confirmed claimed identity by following written procedures. • Issuing source visually identified applicant. • Issuing process ensured it was delivered into possession of the person. • Contains at least one reference number. • Contains full name. • Contains photograph. • Includes digital information. • Includes physical security features. • Unexpired.
Driver's License or ID Card (non-RealID-compliant)	FAIR	• Issuing source confirmed claimed identity by following written procedures. • Issuing source visually identified applicant. • Issuing process means it can be reasonably assumed that the card was delivered into possession of the person. • Contains at least one reference number. • Contains full name. • Contains photograph. • Includes physical security features. • Unexpired.
School ID Card with photograph	FAIR	• Issuing source confirmed claimed identity by following written procedures. • Issuing source visually identified applicant. • May contain at least one reference number. • Contains full name. • Contains photograph.
Utility Account Statement	FAIR	• Issuing source confirmed claimed identity. • Issuing process means it can be reasonably assumed that the card was delivered to the person. • The evidence contains a unique reference number.
Credit Card	FAIR	• Issuing source confirmed claimed identity. • Issuing process means it can be reasonably assumed that the card was delivered to the person. • The evidence contains a unique reference number.
Bank Statement	FAIR	• Issuing source confirmed claimed identity. • Issuing process means it can be reasonably assumed that the card was delivered to the person. • The evidence contains a unique reference number.
U.S. Social Security Card	WEAK	• Issuing source confirmed claimed identity. • Issuing process means it can be reasonably assumed that the card was delivered to the person. • The evidence contains a unique reference number.
Original or certified copy of a birth certificate issued by a state, county, or municipal authority or by an outlying possession of the U.S. and bearing an official seal	WEAK	• Issuing source confirmed claimed identity. • Issuing process means it can be reasonably assumed that the card was delivered to the person. • Contains at least one reference number.

B.1 Strength of Identity Evidence

NIST SP 800-63A, Section 5.2.1 is the source for requirements in validating identity evidence.

For definitions of superior, strong, and fair identity evidence, refer to Table 5-1, Strengths of Identity Evidence, on page 17 of NIST SP 800-63A (see Table B-2 and Table B-3).

Table B-2. List of Acceptable Documents and Their Strength

ACCEPTABLE DOCUMENTS	STRENGTH
U.S. Federal Government Employee PIV Card	SUPERIOR
Department of Defense Employees' CAC	SUPERIOR
National Health Card with chip	STRONG
Bank Account (e-proofed)	STRONG
Notary Act	STRONG
Bank Statement	FAIR
Tax Return	FAIR
Voter Registration Card	FAIR

Table B-3. Additional Acceptable Documents from U.S. Citizenship and Immigration Services

ADDITIONAL ACCEPTABLE DOCUMENTS	STRENGTH
U.S. Passport or **U.S. Passport Card**	SUPERIOR
Permanent Resident Card or Alien Registration Receipt Card (Form I–551)	SUPERIOR
Employment Authorization Document Card (Form I–766)	SUPERIOR
Foreign Passport with Form I–94 or Form I–94A with arrival–departure record and containing an endorsement to work	SUPERIOR
Passport from the Federated States of Micronesia or **the Republic of the Marshall Islands** with Form I–94 or Form I–94A	SUPERIOR
Foreign Passport containing a Form I–551 stamp or Form I–551 printed notation	SUPERIOR
Driver's License	STRONG
School Record or **Report Card** (under 18 years of age)	STRONG
Clinic, Doctor, or **Hospital Record** (under 18 years of age)	STRONG
Day Care or **Nursery School Record** (under 18 years of age)	STRONG
U.S. Social Security Account Number Card that is unrestricted	FAIR
Consular Report of Birth Abroad (Form FS–240)	FAIR
Certification of Birth Abroad issued by the U.S. Department of State (Form FS–545)	FAIR
Certificate of Report of Birth issued by the U.S. Department of State (Form DS–1350)	FAIR
U.S. Birth Certificate original or certified copy issued by a state, county, or municipal authority or by an outlying territory of the U.S. and bearing an official seal)	FAIR
Native American Tribal Document	FAIR
U.S. Citizen ID Card (Form I–197)	FAIR
ID for Use of Resident Citizen in the U.S. (Form I–179)	FAIR
Employment Authorization Document issued by the Department of Homeland Security	FAIR

B.2 Validation of Identity Evidence

NIST SP 800-63A, Section 5.2.2 Is Requirement Source for Validating Identity Evidence

<CSP> will validate the identity evidence based on the requirements listed above. Identity evidence deemed unacceptable will not be considered as valid identity evidence for IAL2 or IAL3 identity proofing. Each individual piece of identity evidence will be validated as weak, fair, strong, or superior. At a minimum, <CSP> will validate identity evidence as:

- Weak if all personal details from the evidence have been confirmed as valid by comparison with information held or published by an authoritative source
- Fair if attributes contained in the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s)
- Strong if the evidence has been confirmed as genuine by using appropriate technologies or confirming physical security or cryptographic features
- Superior if the evidence has been confirmed as genuine by trained personnel and appropriate technologies, including the integrity of any physical and cryptographic security features

B.3 Verification of Identity Evidence

NIST SP 800-63A, Section 5.3 Is Requirement Source for Validating Identity Evidence

The goal of identity verification is to confirm and establish a link between the claimed identity and the real-life existence of the subject presenting the evidence. Unacceptable evidence as described in NIST SP 800-63A, Section 5.3 will not be considered.

Weak evidence has been confirmed as having access to the evidence provided to support the claimed identity.

Fair evidence is confirmed by any of the steps below:

- KBV
- Physical comparison to the strongest piece of identity evidence provided
- Physical comparison performed remotely
- Biometric comparison of the applicant to the identity evidence
- Biometric comparison performed remotely SHALL adhere to all requirements as specified in NIST SP 800-63B, Section 5.2.3.

Strong evidence is confirmed by:

- Physical comparison, using appropriate technologies, to a photograph or to the strongest piece of identity evidence provided to support the claimed identity
- Physical comparison performed remotely SHALL adhere to all requirements as specified in NIST SP 800-63B, Section 5.2.3.
- Biometric comparison, using appropriate technologies, of the applicant to the strongest piece of identity evidence provided to support the claimed identity. Biometric comparison performed remotely SHALL adhere to all requirements as specified in NIST SP 800-63B, Section 5.2.3.

Superior evidence is confirmed by biometric comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity, using appropriate technologies. Biometric comparison performed remotely SHALL adhere to all requirements as specified in NIST SP 800-63B, Section 5.2.3.

Appendix C | General References

[A-130] OMB Circular A-130, *Managing Federal Information as a Strategic Resource,* July 28, 2016. Available at: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a13.

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

[EO 9397] Executive Order 9397, *Numbering System for Federal Accounts Relating to Individual Persons,* November 22, 1943. Available at: https://www.ssa.gov/foia/html/EO9397.htm.

[EO 13681] Executive Order 13681, *Improving the Security of Consumer Financial Transactions,* October 21, 2014. Available at: https://www.federalregister.gov/documents/2014/10/23/2014-25439/improving-the-security-of-consumer-financial-transactions

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

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

[FedRAMP] General Services Administration, Federal Risk and Authorization Management Program. Available at: https://www.FedRAMP.gov/.

Appendix D | Definitions

Access
To contact one or more discrete functions of an online, digital service.

Address of Record
The validated and verified location (physical or digital) where an individual can receive communications by using approved mechanisms.

Applicant
A subject undergoing the processes of enrollment and identity proofing.

Approved Cryptography
Federal Information Processing Standards (FIPS)-approved or National Institute of Standards and Technology (NIST) recommended.

An algorithm or technique that is either 1) specified in a FIPS or NIST recommendation or 2) adopted in a FIPS or NIST recommendation.

Attribute
A quality or characteristic ascribed to someone or something.

Attribute Reference
A statement asserting a property of a subscriber without necessarily containing identity information, independent of format. For example, for the attribute "birthday," a reference could be "older than 18" or "born in December."

Attribute Value
A complete statement asserting a property of a subscriber, independent of format. For example, for the attribute "birthday," a value could be "12/1/1980" or "December 1, 1980."

Authentication
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources.

Authentication Factor
The three types of authentication factors are something you know, something you have, and something you are. Every authenticator has one or more authentication factors.

Binding
An association between a subscriber identity and an authenticator or given subscriber session.

Biometrics
Automated recognition of individuals based on their biological and behavioral characteristics.

Claimant
A subject whose identity is to be verified by using one or more authentication protocols.

Claimed Address
The physical location asserted by a subject where they can be reached. It includes the individual's residential street address and may also include their mailing address.

For example, a person with a foreign passport living in the U.S. will need to give an address when going through the identity proofing process. This address would not be an "address of record" but a "claimed address."

Claimed Identity
An applicant's declaration of unvalidated and unverified personal attributes.

Credential
An object or data structure that authoritatively binds an identity—via an identifier or identifiers—and (optionally) additional attributes to at least one authenticator possessed and controlled by a subscriber. While common usage often assumes that the subscriber maintains the credential, these guidelines also use the term to refer to electronic records maintained by the credential service provider that establish binding between the subscriber's authenticator(s) and identity.

Credential Service Provider (CSP)
A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. A CSP may be an independent third party or may issue credentials for its own use.

Cryptographic Authenticator
An authenticator in which the secret is a cryptographic key.

Cryptographic Key
A value used to control cryptographic operations, such as decryption, encryption, signature generation, and signature verification. For the purposes of these guidelines, key requirements SHALL meet the minimum requirements stated in Table 2-1 of NIST Special Publication 800-57, Part 1.

Cryptographic Module
A set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation).

Data Integrity
The property that data has not been altered by an unauthorized entity.

Derived Credential
A credential issued based on proof of possession and control of an authenticator associated with a previously issued credential so as not to duplicate the identity proofing process.

Digital Authentication
The process of establishing confidence in user identities presented digitally to a system Electronic Authentication (E-Authentication) See Digital Authentication.

Enrollment
The process through which an applicant applies to become a subscriber of a CSP, and the CSP validates the applicant's identity.

Federal Information Processing Standards (FIPS)
Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves the standards and guidelines that NIST develops for federal computer systems. NIST issues these standards and guidelines as FIPS for government-wide use. NIST develops FIPS when there are compelling federal government requirements, such as for security and interoperability, and there are no acceptable industry standards or solutions.

FIPS documents are available online on the FIPS home page: http://www.nist.gov/itl/fips.cfm

Federation
A process that allows conveyance of identity and authentication information across a set of networked systems.

Federation Assurance Level
A category describing the assertion protocol utilized in a federated environment to communicate authentication and attribute information (if applicable) to a relying party (RP).

Identity
An attribute or set of attributes that uniquely describe a subject within a given context. Identity Assurance Level. A category that conveys the degree of confidence that the applicant's claimed identity is their real identity.

Identity Evidence
Information or documentation provided by the applicant to support the claimed identity. Identity evidence may be physical (e.g., a driver license) or digital (e.g., an assertion generated and issued by a CSP based on the applicant successfully authenticating to the CSP).

Identity Proofing
The process by which a CSP collects, validates, and verifies information about a person.

Identity Provider
The party that manages the subscriber's primary authentication credentials and issues assertions derived from those credentials. This is commonly the CSP as discussed within this document.

Issuing Source
An authority responsible for generating data, digital evidence (such as assertions), or physical documents that can be used as identity evidence.

Knowledge-Based Verification (KBV)
Identity-verification method based on knowledge of private information associated with the claimed identity. This is often referred to as knowledge-based authentication or knowledge-based proofing.

Manageability
Per NIST Internal Report 8062, providing the capability for granular administration of personally identifiable information, including alteration, deletion, and selective disclosure.

Multi-factor
A characteristic of an authentication system or an authenticator that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed by using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.

Multi-factor Authentication (MFA)
An authentication system that requires more than one distinct authentication factor for successful authentication. MFA can be performed by using a multi-factor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.

Multi-factor Authenticator
An authenticator that provides more than one distinct authentication factor, such as a cryptographic authentication device with an integrated biometric sensor required to activate the device.

Network
An open communications medium, typically the internet, used to transport messages between the claimant and other parties. Unless otherwise stated, no assumptions are made about the network's security; it is assumed to be open and subject to active (e.g., impersonation, man-in-the-middle, session hijacking) and passive (e.g., eavesdropping) attack at any point between the parties (e.g., claimant, verifier, CSP, RP).

Personal Data
See Personally Identifiable Information.

Personal Information
See Personally Identifiable Information.

Personally Identifiable Information (PII)
As defined by Office of Management and Budget Circular A-130, PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Possession and Control of an Authenticator
The ability to activate and use the authenticator in an authentication protocol.

Practice Statement
A formal statement of the practices followed by the parties to an authentication process (e.g., CSP or verifier). It usually describes the parties' policies and practices and can become legally binding.

Predictability
Per NIST Interagency/Internal Report 8062, enabling reliable assumptions by individuals, owners, and operators about PII and its processing by an information system.

Private Credentials
Credentials that cannot be disclosed by the CSP because the contents can be used to compromise the authenticator.

Private Key
The secret part of an asymmetric key pair that is used to digitally sign or decrypt data.

Processing
Per NIST Interagency/Internal Report 8062, operation or set of operations performed upon PII that can include collection, retention, logging, generation, transformation, use, disclosure, transfer, and disposal of PII.

Public Credentials
Credentials that describe the binding in a way that does not compromise the authenticator.

Public Key
The public part of an asymmetric key pair that is used to verify signatures or encrypt data.

Public Key Certificate
A digital document issued and digitally signed by the private key of a certificate authority that binds an identifier to a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key.

Reauthentication
The process of confirming the subscriber's continued presence and intent to be authenticated during an extended usage session.

Registration
See Enrollment. Additional information in NIST SP 800-63-3

Relying Party
An entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.

Remote
In the context of remote authentication or remote transaction, an information exchange between network-connected devices where the information cannot be reliably protected end to end by a single organization's security controls.

Risk Assessment
The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations, resulting from operation of a system.

It is part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

Risk Management
The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and includes (i) establishing the context for risk-related activities, (ii) assessing risk, (iii) responding to risk once determined, and (iv) monitoring risk over time.

Session
A persistent interaction between a subscriber and an end point, either an RP or a CSP.

A session begins with an authentication event and ends with a session termination event.

A session is bound by use of a session secret that the subscriber's software (a browser, application, or operating system) can present to the RP or CSP in lieu of the subscriber's authentication credentials.

Shared Secret
A secret used in authentication that is known to thesubscriber and the verifier.

Single-Factor
A characteristic of an authentication system or an authenticator that requires only one authentication factor (something you know, something you have, or something you are) for successful authentication.

Special Publication (SP)
A type of publication issued by NIST. Specifically, the SP 800 series reports on the Information Technology Laboratory's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

Subject
A person, organization, device, hardware, network, software, or service.

Subscriber
A party who has received a credential or authenticator from a CSP.

Symmetric Key
A cryptographic key used to perform both the cryptographic operation and its inverse, for example, to encrypt and decrypt or create a message authentication code and to verify the code.

Transaction
A discrete event between a user and a system that supports a business or programmatic purpose. A government digital system may have multiple categories or types of transactions, which may require separate analysis within the overall digital-identity risk assessment.

Usability
Per ISO/IEC 9241-11, extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use.

Verifier
An entity that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators by using an authentication protocol.

To do this, the verifier may also need to validate credentials that link the authenticator(s) to the subscriber's identifier and to check their status.

Virtual In-Person Proofing
A remote identity proofing process that employs physical, technical, and procedural measures that provide sufficient confidence that the remote session can be considered equivalent to a physical in-person identity proofing process.

Appendix E | Acronyms

ABBREVIATION	TERM
AAL	Authenticator Assurance Level
CAC	Common Access Card
CSP	Credential Service Provider
DMF	Death Master File
EIPPS	Enrollment and Identity Proofing Practice Statement
EO	Executive Order
FAL	Federation Assurance Level
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
IAL	Identity Assurance Level
IdP	Identity Provider
IDPV	Identity Proofing and Verification
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
KBV	Knowledge-Based Verification
MFA	Multi-factor authentication
NARA	National Archives and Records Administration
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
RP	Relying Party
SMS	Short Message Service
SP	Special Publication

Appendix F | Footnotes

1 Kantara Initiative provides strategic vision and real-world innovation for the transformation of digital identity and agency over personal data. Kantara Initiative link is at https://kantarainitiative.org/

2 Including any National Archives and Records Administration (NARA) records retention schedules that may apply.

3 Different sets and combinations of core attributes have been assessed and documented in North American Security Products Organization (NASPO) Identity Proofing and Verification (IDPV) working group in NASPO-IDPV-60, *Establishment of Core Identity Attribute Sets and Supplemental Identity Attributes,* Report of the IDPV Identity Resolution Project, February 17, 2014.

4 This may include any NARA requirements for records retention.

5 Capture refers to the electronic capture of identity evidence during remote identity proofing.

6 Information related to access requirements for the Social Security Administration's full file of death information and the public file of death information (also known as the Death Master File [DMF]) available from the Department of Commerce's National Technical Information Service (NTIS) is available at https://www.ssa.gov/dataexchange/request_dmf.html.

7 Kantara Initiative provides strategic vision and real-world innovation for the transformation of digital identity and agency over personal data. Kantara Initiative link is at https://kantarainitiative.org/.

8 including any NARA records retention schedules that may apply

9 Different sets and combinations of core attributes have been assessed and documented in NASPO IDPV working group in NASPO-IDPV-60, Establishment of *Core Identity Attribute Sets and Supplemental Identity Attributes,* Report of the IDPV Identity Resolution Project, February 17, 2014.

10 This may include any NARA requirements for records retention.

11 Capture refers to the electronic capture of identity evidence during remote identity proofing.

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

THIS PAGE INTENTIONALLY LEFT BLANK


MITRE
SOLVING PROBLEMS
FOR A SAFER WORLD™