Comment Template for: NIST SP 800-63-4 Suite (Initial Public Draft)

Please submit responses to dig-comments@nist.gov by March 24, 2023

Organization:	*The Slandala Company*
Name of Subm	*Jimmy Jung*
Email Address	[REMOVED]

Comme	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
2	BASE	5.2.3		1240	Organizations may select an assurance level for marketing reasons (i.e., they wish to offer an IAL2 service); and would there fore not need a documented process for selecting an assurance level.	The document should note this.
3	BASE	5.3.4			The Digital Identity Acceptance Statement appears to be an SSP for the 800-63 process?	
4	63A	4		426	It may be helpful to indicate that section 4 is Normative except where indicated otherwise (i.e., 4.1.1, and kinda 4.2)	"Section 4 is normative except where indicated otherwise"
5	63A	4.3.3			63A should identify the strength of evidence requirements for typical identification; like those found in the I9. These items are currently identified in the "Digital Identity Guidelines: Implementation Resources" (Table A-3-2. Notional Strength of Evidence). Common IDs (e.g., US Passport and Cards, PIV Cards, REAL ID Cards, non-Real Driver's License, Social Security Cards) should have identified specific strengths, rather than "notional" strengths identified.	Provide a strength of evidence table (perhaps as an appendix or in 4.3.3) for typical well-known IDs. Most likely a subset of "Digital Identity Guidelines: Implementation Resources" Table A-3-2. Notional Strength of Evidence.
6	63A	4.3.4.4		647	Credible sources is a useful addition; however, there is no criteria that distinguishes between authoritative and credible sources (ether is acceptable) . So ther terms utility is limited.	none, I guess?
7	63A	4.4.1		663	Do enrollment codes link claimed IDs to applicants? Or only confirm access to an address as described in 5.1.6?	Consider removing
8	63A	4.4.1		668	In general, consistency of terms and usage would alleviate confusion. Here, the phrase "remote (attended and unattended) physical facial image comparison" is confusing and probably isn't needed, as it's the image comparison that is important. The text goes on to explain the attended or unattended part. Here, and section 5.4 are the only normative sections where the terms attended and unattended are used, suggesting they are unnecessary (and therefore confusing; especially as you transition away from "unsupervised")	Remote (attended and unattended) Physical facial image comparison. The CSP operator performs a physical comparison of the facial portrait presented on identity evidence to the facial image of the applicant engaged in the identity proofing event. The CSP operator may interact directly with the applicant during some or all of the identity proofing event (attended) or may conduct the comparison at a later time (unattended) using a captured video or photograph and the uploaded copy of the evidence. If the comparison is performed at a later time, steps are taken to ensure the captured video or photograph was taken from the live applicant present during the identity proofing event.
9	63A	5.1.1		699	Here, and throughout, where CSPs are required to document things; should we be calling out specific documents, like a "practice statement," or should we only identify a requirement to "document?" If the intention is a formal process where we want a policy that is traceable to a practice statement, for example, then this language makes sense. But if we only want things documented, we should only say that. If some documentation should be available to users or others, then that requirement should also be identified.	The CSP SHALL document its operations detailing all identity proofing processes as they are implemented to achieve the defined IAL. The documentation SHALL include, at a minimum: …
10	63A	5.1.1.1			As a subset of 5.1.1, why not just add it to the list there?	10. The CSP's policy and plan for when it ceases its operations, including whether the CSP's identity service is subject to retention requirements and how it will protect any sensitive data (including identity attributes, and information contained in subscriber accounts and audit logs) during the period of retention and how the CSP disposes of or destroys all sensitive data at the end of any required retention period,
11	63A	5.1.1.2		732	It is not clear why this is under Identity Service Documentation and Records. Should it have its own section?	5.1.x Fraud Mitigation Measures
12	63A	5.1.1.2		737	That being said, it would be nice to consolidate all the Risk Assessment stuff in one spot, maybe in the 5.1.2.1 list?	In 5.1.2.1: 5. The CSP SHALL include any fraud mitigation measures, including any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography). 6. The CSP SHALL make a summary of its privacy risk assessment available to any organizations that use its services. The summary SHALL be in sufficient detail to enable such organizations to do due diligence.
13	63A	5.1.2.1		762	A requirement that "the CSP SHALL consult the NIST Privacy Framework is confusing. Do we mean for them to follow it? Or merely to have glanced at it? This should either be strengthened (to a measurable criteria) or removed. (or perhaps this is a good place for a "should" - which of course means it is NOT required)	In determining such measures, the CSP SHOULD consult the NIST Privacy Framework [NIST-Privacy] and NIST Special Publication [SP800-53].
14	63A	5.1.2.1		762	A requirement to review risk assessments periodically is fine, as long as we are comfortable with potentially very long periods. Or we could quantify this to no more than, "at least annually."	"at least annually." (?)
16	63A	5.1.6		864	WE do not define "validated address." Would using an enrollment codes to confirm an applicant has access to a address, validate the address?	"Enrollment codes are used to validate an address by confirming an applicant has access"

17	63A	5.1.6		870	WE do not define "validated address." Telephone numbers may be validated by phone companies; but it is unclear what issuing or authoritative source exists for postal addresses or email addresses. It is also unclear if "validating" an address to assure access has any relationship to "validating" an address as an attribute of identity. Within the "Enrollment code" discussion, it would seem only the first should apply.	1. Enrollment codes SHALL be sent to validate the applicants access to an addresses (e.g., postal address, telephone number, or email address).
18	63A	5.1.6		871	The requirement to "present a valid enrollment code to complete the identity proofing process" is not consistent with the definition of enrollment codes that only confirm access to an address. Confirming access to an address could occur at anytime in the lifecycle; potentially, well before proofing. It should be noed that an account could be created tying an applicant to an address; later one or more proofings, at various IALs could be performed to elevate an account to a given level.	Remove "2. The applicant shall present a valid enrollment code to complete the identity proofing process."
19	63A	5.1.6		874	My math is suspect, but my understanding was that a random six digit number had less than 20 bits of entropy? If we have said that it is a random six digit number, do we have to define the entropy? Can we have more than 6 digits? (can we use the old wording?)	"Minimally, a random six digit number or equivalent entropy"
20	63A				There will certainly be performance differences, perhaps we mean performance inequities (which we also should probably define).	9. CSPs SHALL employ biometric technologies that provide similar performance characteristics for applicants of different demographic groups (racial background, gender, ethnicity, etc.). If performance inequities across demographic groups are discovered, CSPs SHALL act expeditiously to provide redress options to affected individuals and to close performance gaps.
21	63A	5.1.8		943	Is 10 intended to be different than 12?	~~10. CSPs SHALL make all performance and operational test results publicly available.~~
22	63A	5.1.8		943	Does "make all performance and operational test results publicly available" align with proprietary corporate concerns?	
23	63A	5.1.9		969-982	This is a change of the definition of "trusted referee." They are now an "agents of the CSP or its partners," but were "notaries, legal guardians, medical professionals, conservators, persons with power of attorney, or some other form of trained and approved or certified individuals," (in 63-3). These "applicant references." This would be clearer, if the old examples were included.	Applicant references are individuals who participate in the identity proofing of an applicant in order to assist the applicant in meeting the identity proofing requirements, such as notaries, legal guardians, medical professionals, conservators, persons with power of attorney, or some other form of trained and approved or certified individuals. Such assistance may include vouching for the applicant's circumstances and actively assisting the applicant in completing the identity proofing process.
24	63A	5.1.9.2		1004	IF "Applicant references are individuals who participate in the identity proofing of an applicant in order to assist the applicant in meeting the identity proofing requirements. Such assistance may include vouching for the applicant's circumstances and actively assisting the applicant in completing the identity proofing process" but IAL3 requires in-person (or remote in-person); it is unclear what role an applicant reference would have in the proofing. That is to say applicant references would not work at IAL3	The following requirements apply to the use of applicant references at any IAL: CSPs SHALL provide the option for the use of applicant references at IALs 1 and 2: Applicant reference SHALL NOT be used at IAL3.
25	63A	5.2		1027	The term "CSP operator-assisted remote process" is confusing. This is understood to be a supervised remote process, albeit without the requirements of 5.5.8. WAIT, WAIT, I take it back - its "supervised" that's confusing. Lets call them BOTH "remote interactions", but identify the specific additional requirements of IAL3. Can we link this back to the old terms? The term "supervised" seems to be a distraction. What is the difference between "supervised by an operator" and "with an operator"? (we use both)	5.2. Identity Proofing Process This document provides requirements that apply to several different identity proofing methods. These possible methods include: • A fully automated, remote process (or unsupervised); • A remote interaction with the applicant and a CSP operator • A combination of automated and remote interaction; • An in-person process, where the operator is physically co-located with the applicant; and • An IAL3 remote interaction with the applicant and a CSP operator (conforming to the IAL3 remote interaction requirements). Identity proofing at IAL1 and IAL2 is allowed for any of the these processes
26	63A	5.3.1		1046	A comparison of 5.3.1, 5.4.1 and 5.5.1 suggests that this is a general requirement?	

28		5.4.4, 5.5.4			5.4.4 and 5.5.4 should align and use the same terms. (This was a confusion in 63-3 and should be clarified here). In-person should always mean in-person. "Remote" should always mean remote. The phrase "in-person remote" is amusingly oxymoronic, but pretty confusing as well. Suggest the phrase "physically co-located". These should also align with the processes identified in 5.2. What is the difference between "supervised by an operator" and "with an operator"? Suggest removing "supervised." I went a little overboard trying to reorg and clarify.	5.4.4. Identity Verification Requirements Proofing at IAL2 SHALL always be conducted in one of the following ways: • A fully automated, remote process (or unsupervised); • A remote interaction with the applicant and a CSP operator • A physically co-located interaction between the applicant and a CSP operator, or • A combination of these; 5.4.4.2. In-person (co-located) Identity Proofing The CSP SHALL verify the binding of the applicant to the claimed identity by physical or biometric comparison of the facial image of the applicant to the facial portrait contained on a piece of presented SUPERIOR or STRONG evidence. 5.4.4.1.Remote Identity Proofing (unsupervised or with an operator) The CSP SHALL verify the binding of the applicant to the claimed identity by one of the following: 1. Comparison of a collected biometric characteristic, such as a facial image, to the associated reference biometric contained on a piece of presented SUPERIOR or STRONG evidence 2. Demonstrated association with a digital account through an AAL2 authentication or an AAL2 and FAL2 federation protocol 5.4.5. Notification of Proofing Requirement … … 5.5.4. Identity Verification Requirements In-person Proofing at IAL3 SHALL always be in-person conducted in one of two ways: • A in-person ¬physically co-located interaction between the applicant and a CSP operator, or • A remote interaction with the applicant , supervised by an and a CSP operator, based on the requirements in Sec. 5.5.8, IAL3 Supervised Remote Identity Proofing. Regardless of which of the two methods the CSP employs, the following requirements apply to identity proofing at IAL3: 1. The CSP SHALL have the operator view the biometric source (e.g., fingers, face) for the presence of any non-natural materials. 2. The CSP SHALL collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject. 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. The CSP SHALL verify the binding of the applicant to the claimed identity by one of the following: 1. Comparison of a collected biometric characteristic, such as a facial image, to the associated reference biometric characteristic contained on a piece of presented SUPERIOR or STRONG evidence 2. Demonstrated association with a digital account through, at a minimum, an AAL2 authentication or an AAL2 and FAL2 federation protocol 5.5.8. Requirements for IAL3 Supervised Remote Identity Proofing … 5.5.5. Notification of Proofing Requirement …
28		5.4.4, 5.5.4			CONTINUED FROM ABOVE	Regardless of which of the two methods the CSP employs, the following requirements apply to identity proofing at IAL3: 1. The CSP SHALL have the operator view the biometric source (e.g., fingers, face) for the presence of any non-natural materials. 2. The CSP SHALL collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject. 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. The CSP SHALL verify the binding of the applicant to the claimed identity by one of the following: 1. Comparison of a collected biometric characteristic, such as a facial image, to the associated reference biometric characteristic contained on a piece of presented SUPERIOR or STRONG evidence 2. Demonstrated association with a digital account through, at a minimum, an AAL2 authentication or an AAL2 and FAL2 federation protocol 5.5.8. Requirements for IAL3 Supervised Remote Identity Proofing … 5.5.5. Notification of Proofing Requirement …
29	63A	5.4.4.1		1130	"Comparison of a collected biometric characteristic, such as a facial image, to the associated reference biometric contained on a piece of presented SUPERIOR or STRONG evidence" Is IAL2 required to "collect" a biometric? IAL3 includes this requirement in a specific clause (5.5.6) but IAL2 does not. Since 5.4.3 allows visual inspection (comparing someone to the picture on this license), it is assumed there is no need to collect. Collecting also may have privacy impacts.	"Comparison of a collected biometric characteristic, such as a facial image, to the associated reference biometric contained on a piece of presented SUPERIOR or STRONG evidence"
30	63A	5.5.3.1, 5.5.3.2		1165, 1176	It is unclear why 5.5.3 divides evidence and Core attributes and 5.4.3 does not? In general, it may be clearer if the description of each level align.	
31	63A	5.5.8		1221	Does the biometric capture require an integrated scanner? If not, it may be possible to perform 5.5.4 with just video.	
32	63A	5.5.8		1226	Could equipment delivered by the organization to a user/applicant (e.g., a company laptop or phone) meet this requirement?	
33	63A	5.6		1234	Suggest "IAL3 Remote Identity Proofing" vs "Supervised"	

34	63A	6.1		1262	Move to 5.1.2.1 (consolidate all the Risk Assessment stuff in one spot)	In 5.1.2.1: 5. The CSP SHALL conduct a include any fraud mitigation measures, including any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography). 6. The CSP SHALL include the processing, retention, or disclosure of any personal information maintained in the subscriber account described in 6.1 7. The CSP SHALL make a summary of its privacy risk assessment available to any organizations that use its services. The summary SHALL be in sufficient detail to enable such organizations to do due diligence.
35	63A	6.2		1265	Should this apply at IAL1, where user may only have an AAL1 authenticator?	