Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change	Non nist comments
SLND-1	63-Base			490	Does NIST have suggestions that go beyond FedRAMP and 27001?		
SLND-2	63-Base			554	Does Equity include an intentional effort to support digital identification for underserved communities and how is that aligned with raising the evidence standards?		
SLND-3	63-Base			921	This section should contextualize or qualify the applicability of the risk management to CSP vendors who may not or cannot know the users, transactions and data their system will support until they engage with a client. They would typically start at 3.3 by identifying an assurance level for market reasons.		
SLND-4	63A			491	CSPs or other commercial organizations may only offer one option and should not be required to provide options (although certainly an agency could solicit for a package deal)	~~CSPs and organizations~~ Federal agencies SHALL provide options when implementing their identity proofing services and processes to promote access for applicants with different means, capabilities, and technology access.	
SLND-5	63A			556	Is risk based decision the correct phrasing? While all "decisions" are risk based, this phrase was not used in previous versions and could be construed to mean that Proofing Agents are allowed to deviate from their training or procedures. The ability to deviate from procedures would appear to be the intended distinction between Proofing agents and trusted refs and this ambiguity could create confusion.	Proofing Agent - An agent of the CSP who is trained to perform identity proofing, either onsite or remotely, following documented identification procedures, such as visual inspection and data collection.	
SLND-6	63A			559	It should be noted that the "Trusted Referee" will be a difficult role to implement in the context of a compliance framework like Kantara, with out very specific criteria regarding how they are trained or how they make risk based decisions.		
SLND-7	63A			572	It is assumed that notaries would be an applicant reference and representative of the applicant; but if this is not intended, then 63-4 should say so.		
SLND-8	63A			611	CSPs or other commercial organizations may only offer one option and should not be required to provide options (although certainly an agency could solicit for a package deal)	Federal agencies ~~CSPs~~ that offer IAL1 & IAL2 services SHALL provide a Remote Unattended identity proofing process and SHALL offer at-least one attended identity proofing process option. (or reference 2.4.2.1)	
SLND-9	63A	2.2		622	Use of "SHOULD" here is confusing, as each IAL requires "The CSP SHALL collect all Core Atributes."		
SLND-10	63A	2.2		633	Trust agreements are understood to be a compoennt of federation. Requieremtnts for federation should be consolidated in 63C.		
SLND-11	63A			662	Very glad to have Appendix A added to the body of 800-63. In the previous version; there were instances where the evidence strength definitions and the evidence example tables did not always align. It is assumed that the table would be "guidance" and evidence show to meet the definitions are valid for the strength. If the intention is otherwise, 63-4 should say so.		
SLND-12	63A			689	The phrase "written procedures" is tricky, although it is one of the distinctions between FAIR and STRONG. It is noted that "written procedures" must be assumed. We assume the DMV has procedures for the applicant, but does not release procedures that can be referenced to show they have high confidence that it knows the real-life identity of the subject.		
SLND-13	63A			717	The requirement to cryptographically validate evidence will make Superior evidence unvalidatable for almost all implementations. (1 STRONG + 1 FAIR will be the near universal implementation for the foreseeable future)		
SLND-14	63A	2.4.2.3		755	The criteria requires the validation of all core attributes described in 2.2. However 2.2 specifically does not reqiuire the collection of any attributes, "the following attributes SHOULD be collected by CSPs"		
SLND-15	63A			756	If you only SHOULD collect core attributes(2.2), but SHALL validate them, is there a perverse incentive to not collect them at all? This appears to make the collection or validation of attributes completely optional.		
SLND-16		2.4.2.4		761	It is noted that in these definitions AAMVA and maybe the The Social Security Number Verification Service would appear to be the ONLY authoritative source available to CSPs. Repeated mentions of the FCRA suggest that only credit bureaus can at as credible sources. It is unclear the MNO data aggregators would be credible sources, these would be critical for using phones as fair evidence.		
SLND-17	63A			831	The phrase "practices statement" may have specific connotations exceeding the goal of this criteria	The CSP SHALL conduct its operations according to a documented procedures or practices ~~statement~~ that details all identity proofing processes	
SLND-18	63A			1148	Clarify that address and evidence may overlap, but are separate	They ~~are also~~ may also be used as an identity verification option at IALs 1 and 2, as described in Sec. 2.5.1.	

SLND-19	63A			1256	Should a personnel and "manual review" be required or would offering options be sufficient.	CSPs that make use of 1:N biometric matching for either resolution or fraud prevention purposes SHALL NOT decline a user's enrollment without providing other enrollment options. ~~a manual~~ 1257 ~~review by a trained proofing agent or trusted referee to confirm the automated~~ 1258 ~~matching results and confirm the results are not a false positive identification (for~~ 1259 ~~example, twins submitting for different accounts with the same CSP).~~
SLND-20	63A			1310	Without a standard format or criteria making data public may result in inconsistent results. Perhaps a specific criteria result format should be specified.	
SLND-21	63A			1925	Use of the phrase "when the setting allows" introduces ambiguity to the applicability. The setting requiring tools should be identified specifically. The typical face-to-face configuration, like a PIV issuance workstation would "allow" tools, but would not typically have any. The tools should be specified - as written, this could be met with a flashlight. (I am now imagining the GSA procurement for thousands of USACCESS magnifying glasses)	All attended ~~When the setting allows for it (e.g., onsite attended~~ proofing events ~~), proofing agents and trusted referees~~ SHALL be provided with specialized tools and equipment to support the visual inspection of evidence (e.g., magnifiers, ultraviolet lights, barcode readers).
SLND-22	63A			1336	"Certification" of proofers is both a high and ambiguous criteria. Perhaps training and testing should be called for.	Proofing agents and trusted referees SHALL be trained on their ~~reviewed regarding their~~ ability to visually inspect evidence on an ongoing basis, and be assessed ~~and certified with~~ at least annual ~~evaluations~~.
SLND-23	63A			1437	Trust agreements are understood to be a component of federation and 63C. Criteria regarding their use should be kept in 63C and possible references there (as in line 875)	
SLND-24	63A			1509	The types of proofing required would seem to belong to a federal agency or possibly an organization, not a CSP. The requirement for a mandatory unattended option is confusing. Face-to-face would seem like the default; while some form of remote may address equity issues.	
SLND-25	63A			1525	The requirement to colect all core attributes conflicts with 2.2 which says CPS SHOULD collect.	
SLND-26	63A	4.1.10 & 4.1.11		1621	Call me crazy, but I really want to switch these two sections, just to stay aligned with the other assurance levels.	
SLND-27	63A	4.2		1643	A VERY rough analysis suggests that DLs will still be the primary ID at IAL2 (and IAL3) and some folks will struggle to find a suitable 2nd ID. (See tab "IAL2 example"). Agencies have had and will continue to have a hard time with students and younger applicants (and history suggests they will bend the rules). A quick google through the always trustworthy internet finds analysis of voter ID laws that suggest 9% of US citizens will not have a license and underrepresented racial and ethnic groups were less likely to have a current driver's license. I have no sense if having an ID or biased biometric comparisons are the bigger obstacle to equity. My general sense is that we have rearranged the ID requirements, but they are not significantly harder or easier than in 63-3; however, if 9% of US citizens struggle to get to government services, there could be an issue. I don't think this is really an argument for anything, just a data point based on cursory analysis at best.	
SLND-28	63A			1655	The types of proofing required would seem to belong to a federal agency or possibly an organization, not a CSP. The requirement for a mandatory unattended option is confusing. Face-to-face would seem like the default; while some form of remote may address equity issues.	2. ~~CSPs~~ Federal Agencies SHALL offer Unattended Remote identity proofing as an option AND ~~.~~ ~~CSPs SHALL offer~~ at least one method of Attended (Remote or Onsite) identity proofing as an option.
SLND-29	63A	4.2.4 & 4.3.4		1672	There seems some likelihood that implementations will substitute simple "visual inspection" for "confirming security features," as described in C&D. If "confirming security features" is the goal, the language should make that quite clear.	
SLND-30	63A			1685	As noted above, the requirement to cryptographically validate evidence will make Superior evidence unvalidatable for almost all implementations. (1 STRONG + 1 FAIR will be the near universal implementation for the foreseeable future)	
SLND-31	63A	4.2.6		1701	The discussion of pathways is informative, but the organization may be awkward. These discussions could be consolidated at 4.2.6, and then the various verification methods presented as simple list.	
SLND-32	63A			1715 (and 1741 and 1765)	As written, a visual facial comparrison of a single piece of STRONG evidence is suffiencent for IAL3 (line 1845); BUT IAL2 requires the STRONG facial compare AND ADDITIONAL verification of a 2nd piece of evidence. Verifying the applicants ownership of the strongest piece of evidence should be sufficient at both IAL2 and IAL3	

SLND-33	63A			1720	Appendix A includes verification methods that do not meet these critiera (e.g., "Must be presented with other evidence containing a photo (if there is no image on the card).") If this is an acceptable practice, it must be included in the verification sections; or the verification sections should reference appendix a as acceptable verification meothds.	(b) Visually comparing the applicant's facial image to a facial portrait on evidence, or in records associated with the evidence, during either an onsite attended session (in-person with a proofing agent), a remote attended session (live video with a proofing agent), or an asynchronous process (i.e., visual comparison made by a proofing agent at a different time). If there is no image on the card, then visual inspection of the card is sufficient if it is presented with other STRONG evidence containing a photo.
SLND-34				1720	Describing comparison of a facial image as "non-biometric" maybe confusing	
SLND-35	63A			1799	It is unclear if "One piece of STRONG and one piece of FAIR (or better)," is intended to mean anything different than ""One piece of FAIR and one piece of STRONG as described in 4.2.2. The parenthetical "(or better)" should be removed, unless better evidence is actually not allowed in other instances. FIPS 201 includes a waiver for this criteria, based on a back-ground check. Should that waiver be made standard here?	
SLND-36	63A	4.3.2		1802	The requirement to collect ALL core attributes in in conflict with 2.2	
SLND-37	63A	4.3.8		1879	It is not clear why a remote agent could not still "have the proofing agent view the source of the collected biometric for the presence of any non-natural materials."?	
SLND-38	63A	5.2		1958	It is noted that some systems may perform identification and account creation well before then need for a higher level of identification or authentication is required and may not be able to support this.	
SLND-39	63B	2.2		556	This uneven description of passwords vs biometrics as a factor is confusing and suggests an unnecessary distinction between them. Is there any reason to identify a biometric characteristic as not recognized as an authenticator by itself, if it is not identified as approved in the document?. The lengthier biometric discussion could be consolidated in 3.2.3	When a combination of two single-factor authenticators is used, the combination SHALL include a password (Sec. 3.1.1) or a biometric characteristic (Sec. 3.2.3) and one physical authenticator (i.e., "something you have") from the following list: •Look-up secret (Sec. 3.1.2) •Out-of-band device (Sec. 3.1.3) •Single-factor OTP (Sec. 3.1.4) •Single-factor cryptographic authentication (Sec. 3.1.6) ~~A biometric characteristic is not recognized as an authenticator by itself. When biometric 563~~ ~~authentication meets the requirements in Sec. 3.2.3, a physical authenticator is 564~~ ~~authenticated along with the biometric.~~ The physical authenticator then serves as "something you have," while the password serves as "something you know" or biometric match serves as "something you are." When a biometric comparison is used as an activation factor for a multi-factor authenticator, the authenticator itself serves as the physical authenticator.
SLND-40	63B			605		Single-factor cryptographic authentication (Sec. 3.1.6) used in conjunction with a password (Sec. 3.1.1) or a biometric characteristic (Sec. 3.2.3)
SLND-41	63B	2.3.3		626	Should the reauthentication criteria be assigned to the RP? Or is it best left ambiguous?	
SLND-42	63B	2.4.3		656	Should this be a condition of the authentication service, since it is 63B, or the service in general?	CSPs SHALL NOT make consent for the additional processing a condition of the ~~identity~~ service.
SLND-43	63B	3.1.2.2		833	Use of the term "next" secret implies that only one look-up may be valid at a time. This is not always the implementation. If there is a limit on the number allowed to be valid, then it should be identified	Verifiers of look-up secrets SHALL prompt the claimant for a ~~the next~~ secret ~~from their authenticator or a specific (e.g., numbered) secret~~
SLND-44				899	It may be useful to note that this does not apply to confirmation codes used to verify addresses.	Email SHALL NOT be used for out-of-band authentication because it may be vulnerable to: •Accessibility using only a password •Interception in transit or at intermediate mail servers •Rerouting attacks, such as those caused by DNS spoofing (this doe not prohibit the use of confirmation codes to validate email addresses, as described in ...)

SLND-45	63B	3.1.3.3		956	Somewhere between 3.1.3.3 and 3.2.9 a stronger SHALL statement is needed. This exception seems to get missed often.	Use of the PSTN for out-of-band verification is restricted as described in this section and SHALL address the requirements of Sec. 3.2.9.
SLND-46	63B	3.1.6.1		1106	Passkeys may be used as one factor of a multifactor authentication, as described in 2.2.1 and would be a single factor cryptographic authenticator. As such, then reference to the syncable authenticator appendix B should also be added here.	private or symmetric keys SHALL 1106 be strongly protected against unauthorized disclosure by using access controls that limit 1107 access to the key to only those software components that require access. 1108 Some cryptographic authenticators, referred to as "syncable authenticators," can manage their private keys using a sync fabric (cloud provider). Additional requirements for using syncable authenticators are in Appendix B. External (i.e., non-embedded) cryptographic authenticators SHALL meet the 1109 requirements for connected authenticators in Sec. 3.2.11.
SLND-47	63B	3.1.7.1		1146	The criteria is confusing. Is there some other criteria that would demand non-exportability invoking this criteria? (i.e., the "IF" part of this "if-then-shall" statement is unclear)	
SLND-48	63B	3.2.2		1211	Throttling limits attempts on an account to 100, but does not identify a next step. It could be concluded that the CSP is now no longer allowed to support a given user. Less severly, perhaps a CSP must reidentify them, or must perform recovery. A next step or options should be called out. It is noted that implementing an attempt count for throttling at the account level is complicated for multifactor implementations, where tracking each factor versus the overall account is intricate.	
SLND-49				1812	The criteria may wish to establish a method for determining that a suspended authenticator should be reactivated. A phone call saying, "I found it," may not suffice	
SLND-50	63B	5			Do we need a separate role for this? (Session Manager)	
SLND-51	63A				Attached only for information; in the tab "Cost impacts," I tried to identify significant cost impacts. These may not directly impact the update, but should certainly be considered.	

IAL2 Identification requires:
-1 STRONG and 1 FAIR
or
-1 SUPERIOR - all SUPERIOR evidence must be authenticated using digital signature verification; so 1 STRONG and 1 FAIR in most cases
-(The difference at IAL3 is the collection of a biometric sample)
-Draft 63-4 identifies Driver's license, State ID, Green Card, Military ID, and Veteran Health Card, as STRONG evidence examples. PIV cards and passports, acting as STRONG also seem like potential likely evidence.
--STRONG evidence is verified by: confirmation codes, visual facial compare, AAL2 authentication, automated biometric comparison (Of these only codes and visual or biometric compare are widely implemented)
--If 63-4 Tables 4,5 & 6 identify the most likely examples of evidence (and that seems reasonable), only Driver's licenses and perhaps passports would be widely available in the public
--and would be verified by visual or automated biometric compare
-Draft 63-4 identifies a Financial Account, Phone Account, Student ID, Corporate Health card, VA Health card, credit or debit card, snap card or social security card as FAIR evidence examples
--FAIR evidence is verified by: confirmation codes, visual facial compare, micro transaction, AAL2 authentication, automated biometric comparison (Of these only codes and visual or biometric compare are widely implemented – so phone and picture ID (student, corporate) are likely
--At IAL2 you shall verify ALL presented evidence, at IAL3 you verify only the strongest (although you have less options for methods of verification)

•I suspect that at IAL2 typical evidence will be:
o1st: Driver's license, passports maybe Military ID, PIV, State ID (gun, adult ID), Green Card
o2nd: phone, passports maybe Military ID, PIV, State ID (gun, adult ID) or picture ID (student, corporate),

(According to the internet ??!?! ~40-56% of Americans have a passport. 9%, or 20.76 million people, who are U.S. citizens aged 18 or older do not have a non-expired driver's license))

(Members of underrepresented racial and ethnic groups were less likely to have a current driver's license or other government-issued photo ID.)
https://cdce.umd.edu/sites/cdce.umd.edu/files/pubs/Voter%20ID%202023%20survey%20Key%20Results%20Jan%202024%20%281%29.pdf
https://www.voteriders.org/analysis-millions-lack-voter-id/

•attribute validation - The process or act of confirming that a set of attributes are accurate and associated with a real-life identity.

The attribute validation is a bit mysterious. While section 4 requires the validation of ALL core attributes, but 2.2 is structured to allow CSPs complete flexibility in what they identify as core attributes.

There was some initial concern about the ability to access "authoritative sources" as there don't seem to be many. Attribute validation would fall, significantly to data aggregators. But this is less critical if there are no specific core attributes to be validated.

Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)		
63-Base			1835	NISTAIRMF		COST IMPACT: AI and machine learning now has its own Risk Mgmt Framework
63A			491	CSPs or other commercial organizations may only offer one option and should not be required to provide	~~CSPs and organizations~~	COST IMPACT: Currently requires "CSPs" toprovide multiple proofint types
63A			559	It should be noted that the "Trusted Referee" will be a difficult role to implement in the context of a compliance		COST IMPACT: Traiing for proofing, and especially for Trusted refs ust got much more stringent. (Some
63A	3.1.2.1		885			COST IMPACT: NEW FRUAD MGMT REQUIEMENT
63A			1235			COST IMPACT: Biometric testing
63A			1336	"Certification" of proofers is both a high and ambiguous criteria. Perhaps training and testing should be called	Proofing agents and	COST: certification of proofers and refs
63A			1679			COST: Traiing and/or crypto verification of superor
63B			743			COST IMPACT: password, verifiers SHALL compare 743 the prospective secret against a blocklist that contains
63B			1273			COST IMPACT: Biometric authentication technologies SHALL provide similar performance for 1273
63B	4.2.2.2					COST IMPACT: Recovery functions at AAL2