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

Please submit responses to dig-comments@nist.gov by October 7, 2024.

Organization:	*CLEAR*
Name of Submitter/POC:	*Brian Worth*
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63A	2.1.	5	507	Verification that the applicant is a real-life person comes occurs in Step 3, not Step 1.	Remove "and is a real life person" from line 509 because subsequent steps outlined accomplish this step (specifically step 3) and include it on line 514. New sentence on 514 "The third step, identity verification, confirms that the applicant presenting the identity evidence is the same individual to whom the validated evidence was issued and with whom the validated attributes are associated and is a real-life person."
2	63A	2.1.1.	6	534	The term "Valid" needs more clarification and may have different implications under different use cases and in different locales. For example, a revoked DL or State ID doesn't mean the identity document isn't valid, but instead refers to revoked privileges.	Add clarity on "valid" or remove the text "(e.g., not revoked)"
3	63A	2.1.2.	8	582	Given the definitions of roles immediately preceding this statement, it is possible that a CSP may identity as none of the above roles.	Insert "if any" in line 582. New language in line 582 "CSPs SHALL identify which, if any, of above roles are applicable to their identity service and SHALL provide training and support resources consistent with the requirements and expectations provided in Sec. 3.
4	63A	2.2.	9	623	It would be helpful if NIST wrote or referenced more detailed specifications for what constitutes name parts and how parts that are ambiguous should be standardized by CSPs. This may seem out of scope for this document but would be of high practical value for implementators and would be one actionable way to improve equity (i.e., not biasing calculation of name parts or character sets to specific demographic groups)	Recommend referencing ISO standards for names/name parts.
5	63A	2.4.1.1.	10	666	Comment is too vague to be actionable by a CSP	Remove or make stronger
6	63A	2.4.1.1.	11	677	A facial portrait on its own does not uniquely identify a person	Add "is an issued document containing" to facial portrait New Language line 677-678: 3. The evidence contains at least one reference number, is an issued document containing a facial portrait, or has sufficient attributes to uniquely identify the person to whom it relates.
7	63A	2.4.1.1.	11	679	These requirements do not as written apply to examples in the A.1 Fair Evidence examples such as the phone account.	Explain how this applies to phone accounts or add an exception for this in the requirements.
8	63A	2.4.1.1.	11	681	It is unclear what determines a credible/authoritative source here. Is there any gradient defined that says one source is more credible than another and would that affect whether or not the evidence is FAIR vs. STRONG?	Clarify what is a credible/authoritative source, by adding a reference to the document and/or adding examples.
9	63A	2.4.1.1.	11	688	More clarity is needed regarding oversight of the written procedures. In practical terms, how would a CSP audit these procedures?	Clarify an acceptable process for auditing these procedures.
10		2.4.1.2.	11	703	Same as Comment #7 It is unclear what determines a credible/authoritative source here. Is there any gradient defined that says one source is more credible than another and would that affect whether or not the evidence is FAIR vs. STRONG?	Clarify what is a credible/authoritative source, by adding a reference to the document and/or adding examples.
11	63A	2.4.1.3.	12	720	This should either include a timeframe or explicitly declare that attended enrollment only need be done once per lifetime.	Add "at least once" New language lines 720-721 The issuing source had the subject participate in an attended enrollment and identity proofing process at least once that confirmed their physical existence.
12	63A	2.4.2.2.	14	749	This is overly focused on document. Phone accounts are not included and do not meet the requirements, but phone accounts are an example listed in A.1. How do the verification methods listed in 2.4.2.2 apply?	As the requirements do not align completely with the examples, clarification is needed here
13	63A	2.4.2.2.	14	749	The acceptable methods for validating presented evidence does NOT include validation of the data with a credible source (e.g., DLDV)	Include verification of self attested data with a credible source as an additional acceptable method
14	63A	3.1.3.2.	22	1031	"Mitigate fraud" leaves significant leeway to collect significant levels of PII (e.g., shall one retrieve and record a subject's yearly income, because it is a good predictor of fraud?). This is too vague and invites overcollection of data	Elaborate on fraud mitigation or remove the reference to it from the sentence.

15	63A	3.1.4.	23	1076	Does inequitable access include more friction or does it amount to complete denial of a demographic group? If it's the former we SHALL assess the friction. Otherwise we just point to the fallbacks.	Clarification on what is considered the definition of inequitable access
16	63A	3.1.4.	23	1085	Certain elements of the equity assessment are difficult to measure/log. For example, how would one determine the race, gender and age of a friction-related abandoned enrollment? Any assessment would have the potential for a huge error.	"SHALL" becomes "SHOULD" in bullet 5, lines 1085-1086
17	63A	3.1.11.	28	1242	This approach is in direct contradiction to what ISO 29795-10:2024 asks for. The ISO standard on how to measure demographic effects, requires us to ignore the specific demographic distribution of the user base.	Replace "in conditions that are substantially similar to the operational environment and user base of the system. The user base is defined by both the demographic characteristics of the expected users as well as the devices they are expected to use." by "following ISO/IEC 19795-10:2024."
18	63A	3.1.11.	28	1246	This biometric performance requirement lacks a specification of the demographic groups or mix it targets. Does it apply to the aggregate error rates or to the worst-performing group, or some other demographic distribution? If it refers to the worst-performing group, the given FMR and FNMR requirements are overly demanding and should be relaxed. Discuss two options: (1) demanding the existing performance requirements to hold for the worst performing demographic group and loosen the FNMR requirement to something >2%, or (2) qualify that the performance requirements are required in aggregate for the given gallery and applicant demographic distribution.	Qualify that the performance requirements are required in aggregate for the given gallery and applicant demographic distribution.
19	63A	3.1.11.	28	1249	An FNMR requirement should say whether or not it includes the FTAR. For some SDKs and circumstances these two error rates are in the same ballpark.	Add either ", where False non-matches include Failure-to-enrolls" or another bullet item with a separate FTAR requirement, such as "Failure-to-enroll rate 1:100 or lower."
20	63A	3.1.11.	28	1250	The distinction between open and closed False Positive Rate is not made. Presumably, the open set version is intended, because it poses the bigger security risk. Change "for false" to "for open-set false".	Change "for false" to "for open-set false"
21	63A	3.1.11.	28	1250	False Positive Error rate measurements depend on how narrow or broad demographic cohorts are chosen. Without defining the demographic cohorts, any False Positive error rate requirement can be weakened by broadening the cohorts.	Discuss the introduction of an additional SHALL on what demographic attributes and quantization shall be used when measuring the differentials; add such a requirement.
22	63A	3.1.11.	28	1261	This may have been held vague on purpose. There are no agreed upon tolerable demographic differentials published within the biometric community. The standard ISO/IEC 19795-10:2024 defines how to measure demographic effects and what metrics to use. But it does not contain guidance or requirements on what differentials can be tolerated as fair.	Discuss in the committee whether or not concrete numeric differential requirements should be added here.
23	63A	3.1.12.	29	1292	It should be clarified that this is not required when optical capture of the MRZ is part of a PKI-based validation process (eg. ePassport Basic Access Control).	Add the following: "This is not required when optical capture of the MRZ is part of a PKI-based validation process (e.g., ePassport Basic Access Control (BAC)).
24	63A	4.2.4.	41	1673	Clarify: For MNO / Phone Account listed in A1 Fair Evidence examples, how do any of these techniques apply?	Clarify how you reconcile for phone accounts.
25	63A	4.2.4.	41	1675	This language regarding signature needs to be stronger to prevent circumvention.	Add to the end of bullet (a): "A negative authenticity check of a signature should override any other sort of check listed here (i.e., if signature is invalid, a physical inspection should not be sufficient validation).
26	63A	4.2.6.3.	43	1768	It is unclear why non-portrait biometric comparison would NOT be an approved method for FAIR in particular.	Combine Points 2 and 3 into one section "Approved biometric methods for verifying FAIR, STRONG, and SUPERIOR evidence at IAL2 include: (a) Comparing the applicant's facial image to a facial portrait on evidence via an automated comparison (b) Comparing, via automated means, a non-facial portrait biometric stored on identity evidence, or in-records associated with the evidence, to a live sample provided by the applicant
27	63A	4.4.	49	1920	A CSP that does not have access to federal databases (e.g. for pulling and verifying SSN) would be very limited in its ability to proof. Evidences are harder to come by when looking at this practically - there are not many available sources to use, so, in an effort to be equitable, this might need to be looser until better tools are in place.	Remove 'core' from "Government Identifier is one of the Core Attributes: SSN, DL #, Passport, etc."
28	63B	1.	2	412	It is unclear what would be considered "phishing-resistant" for authentication options.	Provide references or examples to phishing-resistant methods (e.g., passkeys).
29	63B	3.1.1.2.	15	777	The language as written is too broad and leaves too much room for the CSP's interpretation. This should be limited to the exception for whitespaces.	Remove entire section and replace with "Verifiers MAY make allowances for removing leading and trailing whitespace characters before verification provided that passwords remain at least the required minimum length after such processing.
30	63B	3.1.3.3	21	961	"SHALL" is prescriptive but "alternative authentication options" requirements are not defined or clear.	Replace "SHALL" with "SHOULD" or describe and include examples of "alternative authentication options"
31	63B	3.2.3.	30	1248	This statement is inaccurate. Testing a digital signature is as probabilistic in nature as biometric comparison.	Delete entire sentence on lines 1248-1249
32	63B	3.2.3.	30	1273	We acknowledge that "similar performance" is hard to quantify at this point in time. Is an FMR ratio of 100 between the most and least affected demographic group acceptable? Or does it need to be 10? If there are no quantitative performance tolerances, then similar performance can't be a requirement. "SHALL" is prescriptive but "similar" is vague and leaves too much open to interpretation. This will make determination and implementation too subjective.	Replace "SHALL" with "SHOULD" or quantify "similar"

33	63B	3.2.3	31	1298	This is a strong bias towards local storage and comparison and ignores the effectiveness of modern template protection. Methods such as homomorphic encryption, template tokenization, and multi-party computation will spread in use in the near future and enable similar privacy and security risk levels as local comparison.	Add ", unless biometric templates are stored and processed using dedicated and strong template protection methods." New Language (lines 1298-1299) Since the potential for attacks on a larger scale is greater at central verifiers, comparison SHOULD be performed locally, unless biometric templates are stored and processed using dedicated and strong template protection methods.
34	63B	3.2.3.	31	1322	Does not sufficiently take into account all use and consent cases.	Add "or after the user-consented retention period has elapsed." New language (lines 1320-1322): Biometric samples and any biometric data derived from the biometric sample SHALL be zeroized (erased) immediately after any training or research data has been derived or after the user-consented retention period has elapsed.