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:	*NextgenId, Inc.*
Name of Submitter/POC:	*Michael Harris*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
NGID001	63-Base	y Proofing and Enro	iii	175-177	Measurable, standardized, and quantifiable inclusive biometric modalities should be added to verified, trusted identity stores, that are together validated against known knowledge bases	Using standardized biometrics with baseline validation requirements together with a weighted matrix for assurance, e.g., bio1+bio2+KYC1+doc1+doc2 where data sets are layered by IAL level and cross-referenced could provide an unattended, or ML model for fully remote identity assurance.
NGID002	63-Base	y Proofing and Enro	iii	194-195	For maximum adoption, integrity, ethical, and religious reasons privacy must remain a paramount consideration. For equity it is well-known that availability to services, devices, and even fair and equitable use of biometrics are not inclusive or fairly distributed.	Just as documentation proofs can be substituted, no one proofing mechanism shall depend upon a single biometric modality. E.g., if an elderly person cannot for motility or other reasons use a fingerprint biometric, they must be availed the ability to use alternate methods, such as face, iris, etc.
NGID003	63-Base	y Proofing and Enro	iii	196-198	Liveness and PAD performance testing will ALWAYS lag behind new subversion techniques. Both sides may eventually escalate in an AI arms race.	A proposed methodology would be to continue testing liveness and PAD for each modality but to layer multiple modalities in randomized challenges to limit risk from deep fakes and linear presentation attacks
NGID004	63-Base	General	iv	230	The implications and affects related to AI/ML should be further defined. Similarly, the guidance related to continuity of operations with maintained assurance in times of disaster (e.g., pandemic).	Alternative process guidance should be defined for continuing operations without limiting or reducing authentication and assurance regardless of extraneous changes in environment or operational parameters. What checks/balances can be built in to ensure baseline integrity confirmation.
NGID005	63-Base	all for Patent Claim	vi	277	NextgenID will submit applicable assurance and response to dig-comments@nist.gov	
NGID006	63-Base	2.3.3	8	554-586	The standard guidance should be strengthened such that CSP can operate in a mobile/transportable context to serve those who are transportation challenged.	Allow for alternative form-factors within the context of in-person and remote identity proofing such that they can be located across broader demographics and/or enabling the kiosks or proofing devices to be securely transported to the individual (e.g., portable units that could go to a hospital, elderly home, etc)
NGID007	63-Base	2.3.4	9	597	Standard usability metrics can automatically ensure baseline compliance and system integrity for usability, inclusivity, and customer experience validation.	Add relevant standardized usability metrics for baseline compliance testing. This can be readily added to self-service, remote, and SRIP sessions to measure, maintain, and ensure the continuous integrity and usability of the system.
NGID008	63-Base	4.2	15	721	Implies that CSP boundary doesn't stop at just identiity-proofing and must maintain ongoing "accounts".	
NGID009	63-Base	4.3.1	17	735	Need to evolve the standard to make a "something you are" authentication requirement for more than just the "highest security requirements" (line 740-741).	To adequately identify an entity it MUST require the use of "something you are." Relying on something known + something held only binds to the item not the individual entity. For e.g., many phones employ TSM's that may/may not use something you are for authentication but there is no correlation with the have. The identity relies simply on the item held.
NGID010	63-Base	5	23	929	Need to evolve the guidance to prompt agencies that are now lower than IAL-3 to move towards the new standard baseline and controls if IAL-2+	The introduction of readily available tools (e.g., NLMs), increased phishing and fraud, it is necessary to eliminate IAL-1 and elevate minimum xALs to apply stronger Ial-2 and IAL-3 controls
NGID011	63-Base	5	23	945-952	CD/CI methodology can best be applied when using controlled systems and aggregating metrics.	Require components to report and collect standardized telemetry metrics for a set period of performance to report, manage, and measure performance and impacts of change/improvements over time. Suggest a 3-year rolling cycle for YoY performance monitoring. This works best for systems that rely on algorithms and objective data versus subjective human assessment. For e.g., during an endpoint capture of enrollment data the system can aggregate and measure time to enroll, failure to enroll, etc.
NGID012	63-Base	5.1.2	25	999-1004	Need to advise on the less-obvious harms that could occur in this and the following bullets	Further delineate potential, less obvious impacts and harms. Not to be exhaustive but the provided 6 bullets are broad and generalized.
NGID013	63-Base	5.2.2.1	31	1200	IAL1 should be obviated given the preclusion of antifraud measures at this IAL level. IAL2 should require automated comparison and validation using authoritative sources and IAL3 should perform all IAL2 checks/validation plus provide human supervision, authentication, and confirmation.	Could elevate the 'supported validation' by implementing an AI/ML model that could compare supporting evidence against authoritative sources for validation and verification of claimed identity. In this way we improve IAL2 and this same method could be used to assist or support the physical examination of supplied evidence for IAL3. Collect, authenticate, validate, verify, supervise, and review.
NGID014	63-Base	5.2.3	32	1240	SHALL develop and document based on selection of assurance levels determined by digital identity failure impacts. This is entirely SELF-GOVERNED by the organization and does not enforce minimum safeguards to the constituents.	The definition of required xAL's MUST be defined by the guidance based on impact assessment. How does the guidance protect the entity or constituent if they can in effect self-govern? Suggest that reference xAL associations be made based on intended use (e.g., banking, benefits, healthcare, etc>0
NGID015	63-Base	5.2.3.1	44	1245	To implement risk-based approach, other attributes should be collected during identity proofing. There should be weighted risks associated with the subject, service, transaction, access and other possible attributes/parameters to facilitate CSP provide a more accurate risk-based decision.	
NGID016	63A	2.2	4	416	Minimum rigor for IAL2 should be the person to person interaction necessary to validate a live subject during the application process.	Suggest that IAL2 introduce language such as, "adds the requirement for a trained CSP representative to interact directly with the applicant during x (not entire but some period to have human confirmation of the subject) at some point within the identity proofing session"
NGID017	63A	4.1.1	8	479-482	Two forms of evidence with photos may not be presented for all xALs. No direction is provided for objective picture comparison. Is facial 'picture' verification the only approved method for step 3?	Using the evidenciary documents provided, and depending on the xAL forms required, a minimum number of valid document photos will be compared for match with the live subject AND applicant's photo. The comparison match should not be subjective for IAL2 or IAL3, instead the comparison match should be done through the use of a standard facial algorithm with sufficient PAD, liveness, and minimum accuracy setting FMR/FNMR. Ideally, the face photos extracted from the documents would be matched against each other and submitted photos and/or live video captures.
NGID018	63A	4.1.1	9	469	The difference between "Resolution" "Validation" and "Verification" are vague.	
NGID019	63A	4.1.1	9	485	Typo in page 9: “verifying they the”	...Verifying that the...
NGID020	63A	4.3.1	10	522	Should it be considered that the document issuer performed an equal or greater xAL proofing session prior to document issuance?	The issuer of the document performed an equal or greater level of assurance identity proofing of the applicant prior to issuing the document that is now being presented as acceptable physical evidence.
NGID021	63A	4.3.2	10	536	Should it be considered that the digital evidence issuer performed an equal or greater xAL proofing session prior to digital evidence issuance?	The issuer of the digital evidence performed an equal or greater level of assurance identity proofing of the applicant prior to issuing the digital evidence that is now being presented as acceptable physical evidence.
NGID022	63A	4.3.2	10	538	Digital evidence can be altered and should be required to have an associated digital signature to ensure it is valid and untampered	
NGID023	63A	4.3.3.2	11	574	facial portrait or other biometric characteristic of the person?	...contains a biometric attribute uniquely associated with the evidence holder

NGID024	63A	4.3.4.1	12	608	For inclusivity and equity, SRIP could be mandated when using an expired ID. The CSP could require the expired ID to be validated by external validating authority and to match the invidivual in real time to the expired id with approviate PAD/liveness checks.	
NGID025	63A	4.3.4.3	13	622-623	trained personnel is not adequate	suggest harmonization of terms to reflect 'Supervisors', 'Trusted Agent', or the like to better reflect that they must be credentialed, trained, assessed, and competent
NGID026	63A	4.4.1	14	663	Add the details of "Enrollment code verification" here and switch bullets for numbers. Confusing that all other bullets here have the details for the bolded information but the reader must jump down to another section to undertand this.	Provide all methods here so reader can compare them without jumping from one section of the document to the other. If there are other mentions of this method, they can refer to this section (4.4.1.a, etc.).
NGID027	63A	4.4.1	14	673	Storage of captured video & the evidence introduces a whole set of security/PII concerns. Users may exploit this to playback a recording via a user's home web cam - effectively spoofing or injecting video that without a LIVE operator cannot be validated for authenticity. There is no check/balance to ensure that an operator would later return to the video for review.	Removal of the option to record/review is strongly encouraged to prevent risk of subversion, injection, circumvention, missed requirement steps, or leaked PII.
NGID028	63A	4.4.1	14	668	facial image comparison is subjective and non equitable or inclusive. Racial bias exists in substantiated double blind tests proving 'facial blindness.'	While a live operator SHALL be available to observe and ensure the integrity of a session they should NOT be relied upon for facial comparison. Neural dissonance, facial blindness, and racial bias preclude this from a valid verification method. Instead ever-improving, baselined, and measured biometric matching can score the likelihood of facial match and the resultant score can be substantiated by the operator along with supervision of the session to ensure integrity, liveness.
NGID029	63A	5.1.9	24	964	How can we address individuals who do not possess and cannot obtain required identity evidence, homlessness, little to no access to computing devices, etc.)?	This calls for a Trusted Referee or applicant reference that could be remote or local. Providing SRIP services could assist in several of these persona cases. Line 982 says that trusted referees ARE NOT agents of the CSP. We do not see a reason they could not be CSP employees if they could, e.g., help assist the active user in performing the enrollment or proofing process. In either case, when using a trusted refere and/or applicant reference, it is our strong contention that all parties must be adequately identified to the same or higher xAL level and the adjudication package should maintain a digitally signed record of all parties to the transaction.
NGID030	63A	5.1.9.1	25	999	For CSP referees and/or agents to make risk-based decisions, training as well as a systematic risk-based approach classification should be deployed to facilitate and support risk-based decisions.	Training, classification or risk/s, reporting, decision processing, reporting, and retention should be addressed to mitigate potential claims of exclusivity or inequity.
NGID031	63A	5.1.9.2	25	003-101	When allowing and using an applicant reference chain-of-custody rules should apply	Include the same xAL process and data record used for the applicant along with the applicant reference within the session, retention, and submission package so that there is a chain-of-custody binding the enrollment/proofing source to the adjudication and issuance. I.e., there must be a means for someone to review and identify that an applicant reference was validated and they in effect become one of the strong forms of evidence for that identity session
NGID032	63A	5.5.8	31	1215	what should occur if an applicant leaves the identity proofing session? E.g., 1 second, 30 seconds, longer?	Suggest that a mitigation or guidance path be prescribed such that if an applicant leaves the view of the SRIP agent during an identity proofing session e.g., the session must be terminated with immediate effect along with a note indicating the causative factor. The CSP may prescribe the method of handling should the applicant leave the session for X period of time.
NGID033	63A	5.5.8	32	1217	What is meant by 'participate' and for the 'entirety of the identity proofing session'?	What is the definition of participation in this context? What is the defintion of an entire identity proofing session? Is it necessary for the operator to verbally engage with the user? Should the operator actively participate and monitor the placement of paper documents for scanning or typing of data?
NGID034	63A	5.5.8	32	1221	Further definition of integrated is required.	Integrated directly with the compute platform performing the verification (so as to avoid man-in-the-middle attacks or other subversion), employing anti-tampering, no exposed cabling/wires, built in to a secured enclosure.
NGID035	63A	5.5.8	32	1221	Collection of fingerprint biometrics should mandate the use of FBI approved fingerprint capture devices and algorithms.	Collection of fingerprints SHALL use FBI approved for NGI and IQS as defined on the FBI APL in accordance with https://fbibiospecs.fbi.gov/certifications-1/faq
NGID036	63A	9.3	47	1593	Where applicable, provide a parallel run of the process on self-help step-by-step auxiliary screen or video recording to guide subjects during enrollment.	
NGID037	63A	9.3	48	1643	Session-End confirmation can prompt subject to select a method (email, text message, etc.) to deliver narrative/instructions on the next step.	
NGID038	63A	10.3	53	1783	Addition of augmented lighting may assist in capturing a broader range of persons	
NGID039	63B	5.2.2	31	1235	The limit of consecutive fails of 100 is too high.	We think up to 5 consecutive fails with a count-down prompting subject of the number of attempts remaining before locking the session or prompting other methods for verification.