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

Please submit responses to dig-comments@nist.gov by March 24, 2023 April 14, 2023

Organization:	***Secure Technology Alliance - Identity & Access Forum***
Name of Submitter/POC:	[REMOVED]
Name of Participants	[REMOVED]

2	Commenter	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)
	Michael Harris	63-Base	Identity Proofing & Enrollment	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 basis.
	Michael Harris	63-Base	Identity Proofing & Enrollment	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.
	Michael Harris	63-Base	Identity Proofing & Enrollment	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.
	Michael Harris	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).
	Michael Harris	63-Base	Call for Patent Claims	vi	277	NextgenID will submit applicable assurance and response to dig-comments@nist.gov
	Bill Windsor	63-Base	2.1	5	435-436	"Guidelines do not address the identity of subjects for physical access ....."
	Bill Windsor	63-Base	2.3.1	7	521-532	-- No specific issue with the current language --
	Michael Harris	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 have transportation challenged.
	Michael Harris	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.
	Bill Windsor	63-Base	4.1	11	618-622	-- No specific issue with the current language --
	Michael Harris	63-Base	4.2	15	721	Implies that CSP boundary doesn't stop at just identiity-proofing and must maintain ongoing "accounts".
	Michael Harris	63-Base	4.3.1	17	735	Need to evolve the standard to make a "something you are" authentication requirement for morre than just the "highest security requirements" (line 740-741).
	Bill Windsor John Jacob	63-Base	4.3.1	17	740-741	"using two factors is adequate ....". To achieve high security biometrics would provide a high level of confidence compared to other factors.
		63-Base	4.3.1	17	735	Need to evolve the standard to make a "something you are" authentication requirement for morre than just the "highest security requirements" (line 740-741).
	Bill Windsor John Jacob	63-Base	4.4	21	854-855	Current language does not address "downgrade" changes to an authenticator
		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+
	Michael Harris	63-Base	5	23	945-952	CD/CI methodology can best be applied when using controlled systems and aggregating metrics.
	Michael Harris	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
	Michael Harris	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.
	Michael Harris	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.

	Michael Harris	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.
	T. Lockwood	63-Base	Definations		1615-1616	Defination for Applicant - Needed additional information/Clarification to Bridge to Equity Discussion. 2.3.3 provides guiding principle/the EO - but there is not provide policy, framework for normative defination for measuring and assessing equity. See: IEC CD 19795-10 - Information technology — Biometric performance testing and reporting — Part 10: Quantifying biometric system performance variation across demographic groups. https://www.iso.org/standard/81223.html
	Teresa Wu	63A	General	iii	204-218	Identity Proofing and Enrollment - NIST sees a need for inclusion of an unattended, fully remote Identity Assurance Level (IAL) 2 identity proofing workflow that provide security and convenience, but does not require facial recognition. Accordingly, NIST seeks input on the following questions:
						What technologies or methods can be applied to develop a remote, unattended IAL2 identity proofing process that demonstrably mitigates the same risks as the current IAL2 process?
						Identity Assurance establishes a 1:1 relationship between the identity documents submitted and the person who submitted the identity document. As most of the identity documents include a portrait photo, 1:1 face comparison along with liveness and/or spoofing detection has been used as the most efficient and least privacy intrusive method to perform identity proofing. As not many identity document issuers provide online system of record checking in real time, not leveraging 1:1 facial recognition in identity document verification would negatively impact the effectiveness of the process. 1:1 facial recognition is a critical tool in identity proofing process. Must NIST consider another identity proofing method without requiring the use of 1:1 facial recognition (and liveness check), NIST should consider enabling the CSP to recognize prior identity proofing events such as leveraging the method of digitally verifying. -- In-person proofing event taken place as part of a State or Federal background check process. -- A government or trusted party issued identity credentials resulted from a trusted in-person proofing event such as TSA vetted Pre-check status, State or FBI background check, digital mobile driver license and capturing alternative biometric modality that enable remote biometric identification or verification against a system of records that is trusted and used by other state or federal government agencies.
	Lars Sunborn	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.
	Lars Sunborn	63A	4.1	8	496 - 498	The goal of identity validation is to collect the most appropriate identity evidence and attribute information from the applicant and determine it is authentic, accurate, current, and unexpired. Are these Attributes referenced in SP800-205 Attributes for Access Control?
	Michael Harris	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?
	Michael Harris	63A	4.1.1	9	469	The difference between "Resolution" "Validation" and "Verification" are vague.
	Michael Harris	63A	4.1.1	9	485	Typo in page 9: “verifying they the”
	Michael Harris	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?
	Michael Harris	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?
	Michael Harris	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
	Teresa Wu	63A	4.3.3.1		553	We would prefer to see more definition or guidance on "reasonably assumed". This requirement can be difficult to document during assurance certification process. Additionlly, there should be harmonization between this section and SP 800-157 that relies upon 800-63, "Home Agency" for non-PKI authenticators.
	Michael Harris					
	Michael Harris	63A	4.3.3.2	11	574	facial portrait or other biometric characteristic of the person?
	Bill Windsor John Jacob	63A	5.1.1.2	11	735-736	"evaluating behavioral characteristics, and checking vital statistic repositories such as the Death Master File [(DMF)]". Section 5 is NORMATIVE, this statement is provided as an example. This SHOULD be a decision made by the CSP regardless.
	Michael Harris	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.
	Michael Harris	63A	4.3.4.3	13	622-623	trained personnel is not adequate

	Michael Harris	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.
	Michael Harris	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.
	Michael Harris	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.'
	Michael Harris	63A	5.1.9	17	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.)?
	Michael Harris	63A	5.1.9.1	24	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.
	Michael Harris	63A	5.1.9.2	25	1003-1012	When allowing and using an applicant reference chain-of-custody rules should apply
	Michael Harris	63A	5.5.8	25	1215	what should occur if an applicant leaves the identity proofing session? E.g., 1 second, 30 seconds, longer?
	Michael Harris	63A	5.5.8	31	1217	What is meant by 'participate' and for the 'entirety of the identity proofing session'?
	Michael Harris	63A	5.5.8	32	1221	Further definition of integrated is required.
	Michael Harris	63A	5.5.8	32	1221	Collection of fingerprint biometrics should mandate the use of FBI approved fingerprint capture devices and algorithms.
	Bill Windsor	63A	6.1	32	1238-1242	"With the exception of identity proofing for the purposes of providing one-time access .....". This maybe a policy decision on the part of the CSP, the risk resides in data retention.
	Michael Harris	63A	9.3	34	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.
	Michael Harris	63A	9.3	47	1643	Session-End confirmation can prompt subject to select a method (email, text message, etc.) to deliver narrative/instructions on the next step.
	Michael Harris	63A	10.3	48	1783	Addition of augmented lighting may assist in capturing a broader range of persons
	Lars Sunborn	63B		53	443	AAL1 requires either single-factor or multi-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.This is unclear. A Memorized Secret is Something you know. This may be used to prove posession and control of a token, or Something you have, making this a 2FA
	Lars Sunborn	63B		6	713	When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a blocklist that contains values known to be commonly used, expected, or compromised. For example, the list MAY include, but is not limited to: • Passwords obtained from previous breach corpuses. • Dictionary words. • Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd').The list of repetitive or Sequential characters may be extensive.
	Lars Sunborn	63B		15	722 - 724	Excessively large blocklists SHOULD NOT be used because they frustrate subscribers' attempts to establish an acceptable memorized secret and do not provide significantly improved security. Comment: Agree with this statement as justification for comment above. What is the demarkation in the eight character secret for sequential, or repeated charachters that are allowed, vs blocked?
	Lars Sunborn	63B	9.3			Other processing of attributes may carry different privacy risks that call for obtaining consent or allowing subscribers more control over the use or disclosure of specific attributes (manageability) Comment: The references to Section 4.4, makes further references to SP800-53 which then references on to SP800-53B are general. This is unclear, reads similar to a chapter from Dan Brown's novel The Da Vinci Code. Need clarifying detail in one place of how to restrict access to specific PII dataobjects..
	Lars Sunborn	63B	Generally in all sections	60	101	Is there an element of this guidance that you think is missing or could be expanded?
	Lars Sunborn	63B	Generally in all sections	iii	102	Is any language in the guidance confusing or hard to understand?

	Michael Harris	63B	5.2.2	iii	1235	The limit of consecutive fails of 100 is too high.
	Lars Sunborn	63C	General	31		Is any language in the guidance confusing or hard to understand? Suggestion: Add a description of intended audience. Some sections could be simplified.
	Lars Sunborn	63C			476	" If the assertion is protected by a keyed message authentication code (MAC) using a shared key, the IdP SHALL use a different shared key for each RP" Comment: FIPS 201 3 deprecated use of Shared Keys,
	Lars Sunborn	63C		8		See comment on Line 19: The federation authority conducts some level of vetting on each party in the federation to verify compliance with predetermined standards that define the trust agreement. The level of vetting is unique to the use cases and models employed within the federation. This vetting is depicted in theo left side of Figure 2
	Lars Sunborn		All			Gemera; comment: There are several NIST and OMB documents that should be aligned with common terms and definitions. Old terms such as LoA are now being repllaced with IAL 1-3, AAL 1-3 and FAL 1-3 Attributes described in SP 800 -205 ,SP 800-157, SP800 - 171, OMB 19-17 are a few examples. Will these be updated to align with the Suite of SP800-63?