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

Security Industry Association
POC: Jake Parker
[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63A	General	iii	170-181	In this section, NIST seeks "an unattended, fully remote Identity Assurance Level (IAL) 2 identity proofing workflow that provide security and convenience, but does not require facial recognition." Comment: Identity Assurance establishes a 1:1 relationship between the identity documents submitted and the person who submitted the identity document. As most of identity documents include a portrait photo, 1:1 face comparison along with liveness and/or spoofing detection has been used as the most efficient, secure and least privacy intrusive method to perform identity proofing. Not leveraging 1:1 facial recognition in identity document verification would negatively impact the effectiveness of the process. There is currently no equivelant alternative to 1:1 facial recognition with liveness and presentation attack detection for fully remote identity proofing, and should remain the primary method for the IAL2 process.	
2	63A	General	iii	170-181	NIST asks: "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?" Comment: If NIST must 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. For example, government or trusted party-issued identity credentials resulting from a trusted in-person proofing event such as TSA vetted Pre-check status, State or FBI background check, or digital mobile driver license. Or it could be an alternative biometric modality enabling remote biometric identification or verification against a system of records trusted and used by other state or federal government agencies.	
3	63A	4.1	9	496-498	The goal of identity validation is to collect the most appropriate identity evidence and attribute information from the applicant and determine whether it is authentic, accurate, current and unexpired. Are these Attributes referenced in SP800-205 Attributes for Access Control?	Attributes that are collected should be referenced in SP800-205. Ad additional statement should be inserte that "Any Attribute that is considered PII should include access control policies to access, view and edit."
4	63A	4...	6	437-440	Given the emphasis on promoting access "for those with different means, capabilities, and technology access", the guideline for IAL1 requiring one strong document evidence and one fair document evidence may not allow underserved populations to pass even at IAL level 1. Mobile phone, and thus fully remote verification, is more prevalent and accessible to the underserved population than transportation (e.g. to an in-person facility for extended review) or a computer and/or computer center for technology assistance. So if the emphasis on accessibility is serious there must be an effort to survey what underserved populations would find practicable while, as well as ensurign adequate validation.	Would NIST consider making formal permanent links to sources to provide this type of information?
5	63A	4.3.3-4.3.4		542-600	Please provide clarification on evidence strength requirements, specifically the areas of Fair, Strong and Superior stipulations.	Lowering evidence collection requirements from 1 Strong and 2 Fair to 1 Strong and 1 Fair.
6	63A	4.3.3.1	11	551-552	The "issuing source" should be clearly defined. In real world scenarios, the issuing source could be any business in any industry that creates a paper trail containing core attributes resulting in thousands of potential issuing sources, and making it nearly impossible for CSPs to build capability to read, validate or treat the issuing source for fair evidence submission.	Consider amending as the stated requirements (i.e. knowing a valid issuer, creating templates etc.) are impractical in real world scenarios.
7	63A	4.3.3.1	11	557-559	Evidence documents containing fair evidence attributes do not typically contain expiration date and the fair evidence attributes typically expire. It may contain some type of date (e.g., date of issuance, print date, etc.) but there's no assigned expiration date thus imposing 6 months (or any) expiration date is impracticable.	

8	63A	4.3.4.1	12	601-607	Even if issuing sources are limited to certain industries - banking, utility and mortgage companies, for example - there are nearly 4,900 different bank "brands" registered in the US, over 3,100 utility providers registered under US Energy Information Administration, and about 4,400 financial institutions (typically also a bank but operates separately from the banking business) providing mortgage services. This equates to roughly 13,000, likely more as entities could have more than one document type, that could qualify as evidence documents wherewhich the CSPs are responsible to read and validate.	Simlar to the coment above, consider amending as the stated requirements (i.e. knowing a valid issuer, creating templates etc.) are impractical in real world scenarios.
9	63A	4.4.1	15	684-688	Expectation and guideline is unclear.	NIST could provide more detail on what is considered "full control" of a digital account, such as workflow with specific examples where a user is deemed to have full control of their digital account.
10	63A		15	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.	We suggest deleting this requirement and replacing it with an Attempt Limit that is reset by time delay of an relying party (RP) determined time period, or RP assistance.
11	63A	5.1.1.2	17	735-736	Section 5 is NORMATIVE, for example the statement "evaluating behavioral characteristics, and checking vital statistic repositories such as the Death Master File [(DMF)]". This SHOULD be a decision made by the CSP regardless.	Add a Section 5.1.1.2.1 as an INFORMATIVE add on to 5.1.1.2. Additionally, this particular example may be perceived as being invasive on the part of a CSP. Limitations may be warranted for CSP use cases when issued / managed credentials and identity information does not need to managed until the death of an applicant.
12	63A	5.1.8	23	930-932	While we support the inclusion of testing requiremetns for biometric algorithms, this requirement lacks specifiity to test that are relevant to the digital identity enrollment process. Having a tested algorithm does not guarantee that the algorithm provider has or will address demographic variation performance issues over time. Addintally, as stated in the NIST FRVT Part 7 Report for Paperless Travel and Immigration, the acceleration of algorithm development is a key goal and therefore having recently tested algorithm is equally critical for biometric enabled identity proofing solutions: "Given the pace of developments associated with the industrial migration to various convolutional neural networks, it is incumbent on end-users to establish contractual provisions for technology refreshment, factoring in such quantities as speed, scalability, stability, and cost."	NIST should consider adding other dimensions to the testing requirements such as: specification on the dataset type to be similar to the operational dataset, a "freshness of test" that results need to be from evalutation within the last 3 years or less, and a benchmarck for performance results within 20% of the leading performaner of the referenced test.
13	63A	5.1.8	23	943	This requirement is problematic for credential servie providers (CSPs) to address. Public disclosure of operational data require approval from Federal agencies. Often, there are restrictions on data sharing. Unless specified or granted permission otherwise by the agencies or end user organization, operational test results are confidential information. CSPs may not have the necessary legal authority to disclose the operational test results. The responsibility for any requreed disclosure of operational information should be for federal agencies and not CSPs.	Federal agencies must make the best effort to disclose all performance and operational test results publicly available.
14	63A	5.1.8	23	935-956	While NIST specifies a false match rate (FMR) benchmark for biometric algorithms, it does not set performance requirement for Presentation Attack Detection, despite the availablity of existing performance standards defined by independent third parties such as FIDO Alliance or ISO 30107.	NIST should add an Imposter Attack Presentation Attack Rate of PAD level 1 and Level 2 as specified by ISO or FIDO Alliance in addition to FMR in line 935.
15	63A	5.1.9	24-25	959-1002	Clarification on Trusted Referee certification requirements for Component Service IAL2 and Full Service IAL2 certification. Current and future potential identity proofing solution providers are likely unable or unwilling to provide the Trusted Referee requirement as the service is costly. As a result, there is likely to be a reduction in identity proofing solution providers, reducing choice for the consumer and increasing costs for Relying Parties, Government Agencies and the U.S. taxpayer.	Given that the Trusted Referee requirements are costly, to lower the risk of these unintended consequences while still obtaining the intended rise in identity assurance, in-person proofing solutions with large national footprints to support the affected population is suggested as Trusted Referee alternatives.
16	63A	5.3.2.1	26	1056	If the basis of IAL1 is equity by allowing "a range of acceptable techniques...", most underserved population would not have in possession what would be considered acceptable as STRONG evidence, which nullifies the idea of IAL1 as being more equity-based.	Consider risk-based approaches that would allow service providers to perform more transactions at IAL1. Risk assessments
17	63A	5.3.3	27	1068-1069	Given that two industries (financial and utility) could serve as issuing source of Fair evidence documents, and thus resulting to about 13K entities independent of each other, there would at least be around 13K possible formats representing acceptable Fair evidence documents and requiring a trained personnel to be able to visually validate the genuineness of a huge number of documents, in which there are no standard authenticity guidelines, is a challenge.	
18	63A	6.1	34	1238-1242	Regarding "identity proofing for the purposes of providing one-time access ..." - this may be a policy decision on the part of the CSP. The risk resides in data retention.	CSP discretion should prevail here - the SORN and data retention is in their control. Additionally, consideration should be given to a basic retention for "one-time" requests, as there is no guarantee the access need/request is a "one time" thing. In different proofing use cases, a table is recommended for "suggested/informative" retention periods.

20	63A	9.2.	45-46	1537-1542	Provide an exhaustive list of documentations that are acceptable, and then provide an acceptable validation processes.	
21	63A	9.3	49	1676	Identify effective approaches for managing the risks associated with biometric authentication, such as ensuring that biometric data is properly protected and that users are fully informed about the collection and use of their biometric data.	
22	63B	All	iii	101	Response to NIST question related to this section: Is there an element of this guidance that you think is missing or could be expanded?	The documents will benefit from a few additions: 1. Add a section that contains explanations of Attributes. Include examples of Attributes other than names. An example could be an attribute such as professional skills: for medical doctors, a specialty of the profession, such as Neurologist or Podiatrist. 2. Include an example of an Attribute Library (architecture) for storing, handling and distributing different attributes. 3. Provide a few use case examples of the various Authentication Assurance Levels using the various tokens and attributes.
23	63B	All	iii	102	Response to NIST question related to this section: Is any language in the guidance confusing or hard to understand?	The suite of documents would benefit from a simple re-sequencing of content. Descriptive language often makes references to sections not yet covered at that point in the document. Re-sequence so that language describing processes use content already covered.
24	63B		6	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. But this is unclear in the draft. A memorized secret is something you know. This may be used to prove possession and control of a token, or something you have, making this a 2FA.	We suggest modifiying clarification language from Section. 5.1.1 to include examples and a reference to the Memorized Secret is stored centrally by the CSP, when used as 1FA.
25	63B	9.3	60		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). The references to Section 4.4, makes further references to SP800-53 which then references on to SP800-53B are general. This is unclear. IIt needs clarifying detail in one place of how to restrict access to specific PII data objects.	Ceate a table of what data objects are to contain such PII, an example of who need to access such PII and access control policies for such PII data objects. Also add an Appendix with TABLE 3-1: ACCESS CONTROL FAMILY on page 16 SP800-53B, and the suggested Security Controls for each.
26	63B	5.2.3	32	1257-1277	This section provides no guideline value in the standard. Biometrics is a critical component of multi-factor authentication, as currently drafted it will undermine the role of biometrics.	These disclaimers should be removed.
27	63C	All			Response to NIST question related to this section: Is any language in the guidance confusing or hard to understand?	Add a description of the intended audience. Also, some sections could be simplified to enhance readability. Here is one example where this is needed: "At FAL3, the trust agreement and registration between the IdP and RP SHALL be established statically. All identifying key material and federation parameters for all parties (including the list of attributes sent to the RP) SHALL be fixed ahead of time, before the federated authentication process can take place. Runtime decisions MAY be used to further limit what is sent between parties in the federated authentication process (e.g., a runtime decision could opt to not disclose an email address even though this attribute was included in the parameters of the trust agreement)."
28	63C		8	476	Regarding this sentence: "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" - Note FIPS 201-3 deprecated use of shared Keys.	Amend langauge for consistencey with FIPS 201-3 regarding use of shared keys.
29	63-Base	4.3.1	17	740-741	"using two factors is adequate ....". To achieve high security biometrics would provide a higher level of confidence compared to other factors.	Expand the statement to state "two factors and the use of biometrics to meet the highest security requirements".
30	63-Base	4.4	21	854-855	Current language does not address "downgrade" changes to an authenticator.	Add "downgrade" to possible actions.
31		All			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. These documents should be updated to align with the new Suite of SP800-63.	We suggest adding cross references throughout the documents to show touch points with other relevant NIST and OMB documents.