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

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

Organization:	***Idemia***
Name of Submitter/POC:	
Email Address of Submitter/POC:	

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
	63-Base	2.1	5	435-436	"Guidelines do not address the identity of subjects for physical access ....."	Suggest this be struck, physical access requires identity process and access authorization considerations, while they may not identified in the subsequent 63-* documents - excluding it as a while can crate divergence in an area that already struggles to be compliant with PIV.
	63-Base	2.3.1	7	521-532	-- No specific issue with the current language --	Consideration for physical access risks need to be added - as well and the Interagency Security Committee's Risk Management Process used to assess facility risk.
	63-Base	4.1	11	618-622	-- No specific issue with the current language --	Should the CSP description be expanded to incorporate Adjudication / Background activities associated with IAL acts.
	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.	Expand the statement to state "two factors the use of biometrics to meet the highest security requirements".
	63-Base	4.4	21	854-855	Current language does not address "downgrade" changes to an authenticator	Add "downgrade" to possible actions
	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.	
	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 do not allow the underserved population 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 for accessibility is genuine, there must be an effort to survey the reality of what the (underserved) population would find practicable whilst also guarding the need for adequate validation.	
	63A	4.3.3-4.3.4	10-12p	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.
	63A	4.3.3.1	11	551-552	The "issuing source" should be clearly defined. In real world scenario, 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 or validate or treat the issuing source for fair evidence submission.	
	63A	4.3.3.1	11	553	Clarification and specified definition and/or guidance on the term "reasonably assumed". The current language is subject-to-interpretation. This requirement can be difficult to document during the assurance certification process. Limiting to just two industries, where the evidence documents could be stemmed from, CSPs would need to determine the success of delivery from approximately 13,000 entities - which could pose a challenge.	
	63A	4.4.1.	15	684-688	Expectation and guideline is unclear, please provide a workflow with specific examples wherewhich a user is deemed to have full control of their digital account.	

	63A	4.3.4.1	12	601-607	Please kindly illustrate how can CSP "confirm" that it is indeed verify the authenticity of the edvidence as not counterfeits or CSP is indeed verifying any Security features if present? Not all Identity evidence present security features. How many security features should be deemed sufficient? And should the number of security feature verification be proportionate to the 3 IAL levels? Similar to use of biometrics, NIST should consider setting minimun performance criteria for Identity Evidence Authentication algorithm, require the algorithm be recently tested by an indenpendant third party and Federal agency/CSPs would conduct operational testings to improve and address any significant demographic variation issues.	
	63A	4.4.1.	15	684-688	Expectation and guideline is unclear, please provide a workflow with specific examples wherewhich a user is deemed to have full control of their digital account.	
	63A	5.1.1.2	17	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.	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.
	63A	5.1.5	20	850	How can organizations effectively communicate the importance of digital identity management and the role of users in protecting their identies?	More details around user education and awareness inlcuding on how to identify potential social engineering attacks (i.e. phishing), and recommendations for organizations to provide clear and concise communication to users about the importance of digital identity management and their role in protecting their identities.
	63A	5.1.8	23	935-956	While NIST specified FMR for biometric algorithm, it does not set performance requirement for Presentation Attack Detection detection. There are existing performance standards defined by independent third parties such as FIDO Alliance or ISO 30107.	NIST should include 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.
	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.
	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 making the basis of IAL1 as being more equity-based possibly if not likely moot.	
	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 ~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.	
	63A	6.1	34	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.	CSP discretion should prevail here - the SORN and data retention is in the 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. Consider adding a table would "suggested / informative" retention periods, when different proofing use cases.
	63A	9.2	45-46	1537-1542	Provide an exhaustive list of documentations that are acceptable, and then provide an acceptable validation processes.	
	63A	9.3	49	1676	How can organizations manage the risk associated with the use of biometric authentication? Biometric authentication is becoming increasingly popular as a factor for high-assurance authentication, but also introduces unique privacy and security considerations. Please emphasize/clarify this section.	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.