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

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

Organization: Better Identity Coalition	
Name of Submitter/POC:	*Jeremy Grant*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
	63-Base	5.1-5.3	23-39		The consideration of impact to mission delivery in addition to cybersecurity risk was only accounted for under 'compensating controls' in the previous version. This consideration is critical for organizations to effectively manage risk of both error types that could impact their agency: Type I error (rejecting a good subject) and Type II error (accepting an incorrect subject). To effectively manage these combined risks, it requires a fairly mature identity proofing measurement system that tracks the outcomes of the process. These measurement systems require processes and data environments that are not common across all organizations.While not expected directly in these sets of guidance, providing a supplement specific to identity risk measurement systems will be key to effective implementation and management of a risk-based approach to identity management.	Included 'mission needs' in conjunction with risk (previously only risk considered)
	63-Base	Note to Reviewers	ii	160-161	In discussing how this revision opens the door to new technologies such as mDLs and VCs - it would be helpful here or in 63A to specifically define what these means, including with reference to standards.	As stated
	63A	5.3	26	1035-1056	If a key goal of creating a revised IAL1 is to promote access "for those with different means, capabilities, and technology access," the guideline for IAL1 requiring one strong piece of evidence and one fair piece of evidence will likely exclude many underserved individuals. For all purposes Strong means a Photo ID, which many people do not have - and cannot easily obtain. To that point - members have note that the evidence requirements for IAL1 and IAL2 are the same. Some members have noted that there are ways to combining multiple pieces of fair evidence in conjunction with risk signals related to identity theft or synthetic identity fraud in a way that may deliver outcomes that are equal or better to what can be delivered solely with what is currently rated as STRONG evidence. Much as NIST is exploring whether there are ways to achieve IAL2 wihtout biometrics, NIST should also consider how alternatives to STRONG evidence can still achieve similar security outcomes.	Consider whether IAL1 can still be meaningful with evidence requirements that are not identical to IAL2.
	63A	4.3.2	10	526-541	Consider noting that mDLs and VCs (or certain types of them that comply with certain standards) may be considered acceptable digital evidence	As stated. In addition, it may be worth referencing how to handle mDLs and VCs as part of 5.5.2 and 5.5.3, dealing with Evidence and Core Attribute Collection Requirements and Validation Requirements
	63A	4.3.3.2	11	560-578	Can NIST opine on the evidence strength when an attribute and biometric match is made with an authoritative source's system of record, using the method in Sec. 4.3.4.3, pg. 13, line 625, but the underlying evidence document is not present at the time of verification? E.g. self-asserted biographic attributes and a captured portrait image are positively matched to a State's DL/ID record through a matching service?	Consider allowing system of record check against face and biographic data as Strong evidence.
	63A	4.3.3.2	11	576	Focus on physical security features implies that digital evidence cannot be Strong	Change to clarify - and align with 4.3.2 Digital evidence requirements. Same for Superior in 4.3.3.3
	63A	4.3.3.1	11	553-554	With regard to "reasonably assumed," the current language is subject-to-interpretation. This requirement can be difficult to document during the assurance certification process.	Clarification and specified definition and/or guidance on the term "reasonably assumed".
	63A	4.3.4..4	14	647-654	The ability for use of either authoritative or credible sources to validate identity evidence and attributes is critical to modernize any digital identity proofing process. While it was not specifically addressed in the previous version, it was the de facto method of automated validation of fair evidence. The addition of credible sources in addition to authoritative sources better reflects the reality of what constitutes effective validation. However, the current draft (§4.3.4.4) lacks any requirement related to a credible source's reputation or credibility. The definition of credible source should include some measure of credibility, e.g., governmental regulatory oversight. Without an independent recognition of credibility included in the definition of a credible source, this runs the risk of rogue entities acting in this capacity.	The definition of credible source should include some measure of credibility, e.g., governmental regulatory oversight.
	63A	5.1.3	19	794-821	As written, this section suggests the need for CSPs to collect demographic data to assess for equity. Given the requirement to minimize collection of data (800-63-4ipd §5.5), there should be no expectation that would include demographic characteristics to effectively measure equitable impact as it relates to race, religion or other similar demographics (even if optional for the subject to enter).	Recommend clarifying this section to reflect any equity assessment use disaggregated data and does not require additional data collection, as outlined in the "Recommendations from the Equitable Data Working Group" report resulting from EO13985.
	63A	5.1.8	23	935-956	While NIST specified FMR for biometric algorithms, it does not set performance requirements for Presentation Attack Detection. There are existing performance standards defined by independent third parties such as FIDO Alliance or ISO 30107.	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	A number of members have noted that a requirement that every CSP SHALL offer a Trusted Referree service may inadvertently exclude many potential solution providers, given the cost and complexity of providing these services. For example, if a state mDL can be considered as an IAL2 solution for purely remote and unattended ID proofing, this requirement would essentially preclude a state DMV from being considered as an IAL2 CSP if they did not also offer trusted referee services - for all purposes excluding the use of most mDLs. While the requirement for agenices to offer Trusted Referee services is sound, NIST should clarify that agencies can choose to provide those services through a channel that does not require they be bundled with other CSP services. For example, if a mDL does not work or someone does not have one, then triggering a flow where a trusted referee is invoked.	Clarify that agencies can choose to provide Trusted Referee services through a channel that does not require they be bundled with other CSP services.
	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.	Consider adding language on 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.
	63B	5.2.5		539	Since phishing resistant authenticators are now required by OMB for all government use, the sentence “While phishing resistance in Sec. 5.2.5 is not generally required for authentication at AAL2” should be removed. Additionally “SHOULD encourage the use of phishing resistant authenticators at AAL2” should be changed to “SHOULD require phishing resistant authenticators at AAL2” These changes would align NIST guidance with the guidance from OMB M-22-09.	“OMB Memorandum [M-22-09] requires federal government agencies to offer at least one phishing-resistant authenticator option to public users at AAL2. Verifiers SHOULD require the use of phishing-resistant authenticators at AAL2 whenever practical since phishing is a significant threat vector”
	63B	4.1		443	In today's envirnoment, AAL1 should encouarge the use of MFA as many options are readily available and will drive home the point that MFA should be an option for authenticaiton levels	Add sentence at 444 that states, "Multi-factor authentication options should be made available and encourage to be used."
	63B	4		434	Even though FIPS 140-3 certifications were introduced in 2019, vendors were still able to start the FIPS 140-2 certification process until mid 2021 and active modules will not be moved to the historical list until September 2026. Devices that were certified at FIPS 140-2 should still be able to be used up to 5 years post certification, due to the time and cost of the certification process.	Add the following sentence, "exising FIPS validated devices certified under FIPS 140-2 that are in good standing, meet the requirements. " after the sentence, "[FIPS140] requirements are satisfied by FIPS 140-3 or newer revisions."