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:	*HHS/PSC/RLO/ISBS*
Name of Submitter/P(	*Adam McBride*
Email Address of Subn	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Secti	age	Line #	Comment (Include rationale for comment)	Suggested Change
1	63-Base			138	Recommend to include a broader definition for equity that include other persons considered underserved: older people, pregnant, formerly incarcerated, or veterans. Promoting equity should be a shared responsibility between CSPs/IdPs and relying parties. Relying parties know their user base better than anyone else, and if needed, a combination of CSPs/IdPs should be used by the relying parties for additional coverage.	
2	63-Base			142	Remove 'who are eligible for and entitled to them" as it comes from the Relying Party. An IdP focuses on identity proofing, registration, and issuance, whereas the Replying Party / Subscribers handle entitlements.	
3	63-Base			173	How does NIST envision Identity proofing to work without Facial recognition/comparison?	
4	63-Base			196-198	Liveness detection is for facial recognition, and line 173 talks about potentially doing away with facial recognition. Please help reconcile these two.	
5	63-Base			206-208	How will this affect CSP without fraud capabilities to share fraud signals, should we not use any CSP that does not have a vetted fraud and IAL2 service?	
6	63-Base			233	Privacy notices need to explicitly educate how volunteering information has been exploited. Too much legalize and lack of simple language in privacy notice has harmed US consumers.	
7	63-Base			234	Applying security and privacy principles means collecting the least amount of information required and it's outside of scope for an IdP. While the CSPs/IdPs can test their flows using datasets available, equity conversations need to be a shared responsibility between IdPs and RPs, and RPs should look for use of multi-CSPs to provide more coverage, if needed.	
8	63-Base			554	2.3.3 EQUITY. Provide URLs that show research links from NIST that shows this disparity.	
9	63-Base			665	Does "lifetime of the subscriber account" violate data retention laws? Please clarify what lifetime means here.	
10	63-Base			712	Should specify in bullets what maintaining control means in Line 719, I sense it defining specific events, activities, and changes" . Perhaps elaborate or provide examples in appendix.	
11	63-Base			1166	This table needs to align with strategic plan and mission. And it should be communicated to relying parties.	
12	63-Base			1410	To assess equity, IdP would have to collect additional information and will be asked to provide reports outside of safety and security. If the mission requires, relying parties/subscribing systems should collect that information but it's outside the scope for an IdP.	
13	63-Base			1494	Consistent mechanisms are not realistic, perhaps "establish procedures for critical relationships".	
14	63-Base			1857	The definition presented is only a part of EO13985. The existing definition excludes other persons considered underserved: older people, pregnant, formerly incarcerated, or veterans	
15	63A			408-411	Any guidance or considerations on minimizing the operational impact of re-labeling the already IAL1s (rev 3) to IAL0 (rev 4)	
16	63A			458	Would be good to add more prescriptive recommendations on core attributes, perhaps based on industry.	
17				732	Could we add a minimum requirement around making fraud/risk signals available to the relying parties such as (but not limited to) IP address, geolocation used for any fraudulent attempt?	
18	63A			807-814	1,2,3 all basically state the same thing	
19	63A			816	Won't this change the assessment outcome? Is there an alternative?	
20	63A			834	SAOP. Shouldn't this be the CISO? The SAOP is not an official title with in our HHS Agency. Why would this term be used in this SP?	
21	63A			840-841	Add the URL for the SORN site publication	
22	63A			844-847	Why is this necessary? Agency policy would dictate this already. Why have this statement in this SP? This will only add more delay in any procurement process. Agencies already have policies in place to follow. This will only add to the list of items that will be required to complete	
23	63A			1013-102	5.1.10 Requirements for Interacting with Minors- This is too loose. More needs to be added to have a better control on how to deal with minors. I would suggest getting with DOD and use what it used for when Minor dependents are brought in for DOD ID cards are issued for those minors. They have a complete guideline for this. Why not adopt what it used by DOD?	
24	63A	General (		N/A	Develop additional guidance about how to collaborate with and identity proof international partners	
25	63A	General Comments			Additional guidance on how commerical organizations/corporations can achieve IAL3 to allow for interoperability of credentials (decentralized credentials)	

26	63B			1225	Since MFA can be achieved using various types of authenticators, a ranking of authenticators might be beneficial for risk assessment/continuous authentication type use cases	
27	63B			1252-132	In 800-63-4B (Authentication) section 5.2.3 “Use of Biometrics” Please add guidance in 800-63-4B on the AAL compliance of these newer technologies such as passkeys. Passkeys is advocated by Google, Apple, Microsoft especially for citizen identity authentication and use biometrics	
28		General Comments			NIST SP 800-53 doesn’t apply to commercial providers. Would be good to add details around how key elements of the identity workflows and ecosystem should be protected by the IdP/CSP	
29		General C		N/A	Provide formal oversight, roles, and responsibilities to certify and accept IdP and CSP solutions that meet NIST 800-63-4 IAL/AAL/FAL levels, as well as an independent auditor to uphold integrity of certification	
30	63C			340	Authenticators are not always issued by the CSP, they could be bound as well.	
31	63C			499	Does this mean that IdP-initiated flows do not comply with FAL2?	