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:	*National Institute of Health (NIH)*
Name of Submitter/POC:	*Rachel Leffler*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63-Base	Section 4.1	Page 11		The SP 800-63 guidelines use digital identity models that reflect technologies and architectures currently available in the market. What about some SSI technologies? – are the guidelines intended to also cover SSI technologies? Self-sovereign identities (SSI) are digital identities that are managed in a decentralized manner	
2	63-Base	Section 4.4	Page 20,	3rd bullet	sharing identity assertions (e.g., a federation protocol like OpenID Connect or SAML), Should Kerberos tickets be included?	
3	63-Base	Section 5.2.2.3	Page 32	FAL1	FAL1 allows for the subscriber to log into the RP using an assertion from the IdP that can be verified by the RP as coming from the IdP and targeted for a specific RP. Can a digital wallet be the IdP in this context?	
4	63-Base	General			What about information on self-sovereign? Add a section for Self-Sovereign Identity: Users can enter an app on their phone where their identity data is stored, then use an identification number and identity information to verify who they are. Self-sovereign identity adds security and flexibility to users and enables them the ability to share data only when they choose.	
5	63-Base	General			Additional clarification and use cases on IAL Level 0 would be helpful in understanding when should this apply.	
6	63-Base	General			Recommend that NIST provide a template to evaluate impact and risk as part of the guidance or provide a clear mapping for the assurance level recommendation based on system FIPS impact levels.	
7	63B	NIST SP 800-63B-4 ipd 396-403			Phishing resistant authenticators are only required for AAL 3 (High Baseline (or equivalent) per the guidance, while OMB Memo M-22-09 requires use of Phishing resistant authenticators and strong authentication for agency staff, contractors, and partners, phishing-resistant MFA is required. For public users, phishing-resistant MFA must be an option. There seems to be a disconnect between the OMB meemo requirment and the NIST guidance	
8	63B	NIST SP 800-63B-4 ipd			The guidance states that "Memorized secrets SHALL be at least 8 characters in length." please clarify if this would apply to a PIN as well (usually these are 4-6 digits).	
9	63B	NIST SP 800-63B-4 ipd			The IAL and FAL categories are not shown to map to system FIPS rating; but AAL is. Can these others be mapped similarly to AAL in the summary tables of the respective documents	
10	63-Base	General			It would be helpful to have the documents combined as one document rather than 4. Having to open 4 is highly cumbersome.	
11	63B	NIST SP 800-63B-4 ipd			How do reauthentication times provided in the AAL NIST SP 800-63B-4 ipd align with continuous authorization requirments from OMB Memo 22-09	