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

Please submit responses to dig-comments@nist.gov by October 7, 2024.

Organization:	*U.S. Department of Education*
Name of Submitter/POC:	*Michael Magrath*
Email Address of Submitter/POC:	[redacted]

Comment #	**Publication** (Base, 63A, 63B, 63C)	**Section**	**Page #**	**Line #**	**Comment** (Include rationale for comment)	**Suggested Change**
	63A	2.4.1.1	11	679	Requiring physical security features on all FAIR identity evidence, signifcantly reduces potentially acceptable evidence, which could impact equity and inclusion.. Utility bills will no longer be valid and ID cards from schools will need to have physical security features to comply.	Suggest accepting FAIR evidence without physical security features at IAL1. Physical security features shall be required for identity evidence at IAL2 and IAL3.
	63A	3.1.1.	16	845	Can NIST offer any minimum training and qualification requirements? This is very important.	
	63A	3.1.11	29	1273	Add the term Liveness Detection. This is what agencies are seeking.	
	63A	3.1.12	29	1296	Reads, "CSPs SHOULD deploy technology controls to prevent the injection of document images,..." Why is this not a SHALL?	CSPs SHALL deploy technology controls to prevent the injection of document images,..."
	63A	4.2.6.2	43	1759	If an applicant presents a passport for SUPERIOR identity evidence, what account is related to the evidence? The Department of State does not have user accounts.	
	63-Base	3	22	923	I understand this is a risk based approach and the decision trees have been removed. However, the decision trees are an excellent visual guide for agencies to complete a DIRA. It would be beneficial if a version of them were included in the Base Volume. If not in the Base Volume, then in the 800-63-4 Implementation Guidance.	
	63-Base	3.4.4	44	1648	It would be helpful to agencies if NIST were to provide a Digital Identity Acceptance Statement template. I realize that agencies differ, but having a base template to work from would be appreciated.	
	63-Base	Glossary	67	2321	Add definition of "digital evidence" to glossary in all four volumes	
	63B	2.1.2	5	522	The paragraphs from lines 523-525 and 528-529 are confusing. The former reads the implementation need not be validated under FIPS 140 while the latter that cryptography used by verifiers operated on or behalf of federal agencies at AAL1 shall be validated to meeting FIPS 140 Level 1.	Suggest rewording and providing examples.
	63B	3.2.3	30	1275	"The biometric system SHOULD implement PAD." Given the threat vector, this should be a SHALL.	"The biometric system SHALL implement PAD."
	63B	3.2.3	30	1284	Reads, "an overall limit of 50 consecutive failed authentication attempts or 100 if PAD is implemented…" This seems excessively high.	"an overall limit of 20 consecutive failed authentication attempts or 30 if PAD is implemented…"
	63B	3.2.9	35	1446	Provide examples of restricted authenticators. SMS-OTP is restricted. It would be good to list it here and also include any other restricted authenticators. Agencies shouldn't have to guess.	
	63B	Appendix B. Syncable Authenticators	88	2919	General Comment. The Syncable Authenticators section needs to be re-written so a CSP can be audited.	
	63C	3.15.1	39	1614	This describes PIV and CAC. If so, suggest naming them as examples.	
	63C	4.11.1	66	2427	In Fig. 11, suggest adding the word "Subscriber" where applicabe for clarity	
	63C	5.2	70	2527	In Fig. 13, suggest numbering the steps to coincide with the steps detailed in Lines 2525 to 2537, for clarity and readability.	