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:	*DoD CIO*
Name of Submitter/POC:	*Dr. Gale Pomper (1st comment); Mr. Yehudah Hampel (subsequent comments).*
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	4.3.1	19	801	Responding to question about alternate technologies to facial recognition. Based on research completed at Indiana University- in a 16-person study eye movement and mouse movement were more effective at ID uniqueness.	eye movement & mouse tracking (behavioral) Research by Indiana University -- 16 person study on eye movement uniqueness
2	63A	2.2	4	408	IAL0 appears to be roughly equivalent to IAL1 from the previous version of NIST SP 800-63 (800-63-3). This should be pointed out for those familiar with 800-63-3.	If comment is correct, recommend noting this change in document for clarity and to avoid confusion.
3	63A	5.3	26	1035	Unlike 63B and 63C, 63A doesn't delineate its three assurance levels until past halfway into the document. Readers seeking a quick understanding of the ALs in each document may find this confusing and frustrating.	As the assurance levels are arguably the core of the document, recommend putting the sections on the three IALs earlier in the document.
4	63A	5.6	33	1233	From the table, it appears that the only difference between IAL1 and IAL2 is the method of verification. Everything else is the same. This may make it less clear to readers whether much is gained from IAL2 over IAL1.	Recommend revising IAL1 and IAL2 so there are more significant differences between them, as there was in the previous version of 800-63 (800-63-3).
5	63B	4.2.2	9	539	This paragraph quotes an OMB memo which requires federal government agencies to offer at least one phishing-resistant AAL-2 authenticator to public users, than stating that phishing resistance is generally NOT required for AAL-2 authentication, and then stating that verifiers should encourage the use of phishing resistant AAL-2 authenticators. The paragraph could be read as encouraging non-compliance with the OMB memo, and could confuse the reader as to whether phishing resistance is discouraged, encouraged, or required at AAL-2.	Provide a clearer explanation of how the AAL-2 phishing resistance requirements in NIST SP 800-63-4B do or do not align with the AAL-2 requirements in OMB M-22-09. If they do not align, provide an explanation for readers so they know which policy document to follow in what use-case. Aside from that, ensure this paragraph aligns with the table on page 13, which currently states that phishing resistance is only recommended for AAL-2.
6	63C	4	7	453	The table comparing FALs appears to be far less comprehensive than the tables comparing IALs and AALs in 63A and 63B, respectively. It also does not appear to include all the requirements subsequently delineated for the FALs in the following pages.	Given how helpful the more comprehensive comparison tables are in 63A and 63B, recommend expanding this table to include more detailed requirements for each FAL.