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:	*Axiad IDS, Inc.*
Name of Submitter/POC:	*Karen Larson and Mitchell Armenta*
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	2	3	378	Human-centered is used here, but human-centric is the verbiage used through the rest of the document.	Update human-centered to be human-centric for consistency.
2	63-Base	2.1	5	435 - 436	These lines notate that these guidelines don't address physical access, but people using this documentation for guidance could be interested in physical access guidelines as well.	Link to physical access guidelines to be used by people who may be seeking this guidance along with technical security guidance.
3	63-Base	2.3.2	7	536	PII is initialized here for the first time, but hasn't been written out yet. The first time it is written out is line 2177.	Write out Personally Identifiable Information (PII) on this line since it's the first reference to this initialization.
4	63-Base	5.2.2	31	1195 - 1196	Describing IAL, AAL, and FAL as xAL was previously defined on lines 464 - 465.	This description can be removed from this area.
5	63A	7.1	38	Table 3	The "Mitigation Strategies" column for the "Automated Enrollment Attempts" row has a typo. There needs to be a space between the period after "technology." and "CSP".	Add a space between the period after "technology." and "CSP".
6	63A	4.1.1	8	480 - 482	The verification process discusses getting a photo or picture of the applicant. Since this is the first reference to picture, photo, or portrait of applicants some readers may have privacy concerns.	Link to section 5.1.2 to address that privacy concerns are addressed at a later point in the document.
7	63A	5.1.8	23	933	ISO/IEC standards are referenced here for the first time, but the definition is first linked to at line 1468.	Link to the definition of these standards at this line since it is the first reference.
8	63A	5.1.9	24	959 - 1022	Section 5.1.9 discusses accessibility referencing people with disabilities, minors, etc. Working with people who have disabilities isn't discussed again until usability considerations in section 9. Section 5.1.9.10 does discuss how to interact with minors and references the COPPA with a link to help that. There isn't a section that discusses how to interact with people with disabilities.	Consider adding a new section in 5.1.9.x to discuss how to interact with people with disabilities and link to the ADA guidelines around that. Some information from section 10.4 could be mirrored here, or linked to in order to help outline some helpful guidance for these interactions.
9	63A				Tie back to 63A for data handling of any core attributes that contain	
10	63B	6.1	41	1586	Statement is made that says that binding of a multi-factor authenticator shall require MFA or equivalent in the form of identity proofing. This seems to negate being able to offer an option for phishing-resistant authenticators for existing accounts with out having to re-do the identity proofing process. Is that the intent for agencies with existing accounts who need to provide an option for a phishing-resistant authenticator at AAL2?	
11	63B	5.1.6.1	27	1074	Single-factor cryptographic software authenticators - Seems to imply that a software backed security keys such as FIDO passkeys or authentication certificates saved to a secure element can be used. However, these implementations are not clearly called out. It will be helpful to have the intent of this section clarified if it is to allow for inclusion of FIDO passkeys	Provide examples to increase clarity of what can be used in this section
12	63B	5.1.7.1	28	1120	Requirement to require physical input for authentication is listed as "should". As this provides proof of presence, curious why this is only listed as a "should" and not a "shall". Are there accessibility issues on behalf of the user that will need this requirement to be listed as a "should"?	Provide additional explanation about what situations physical input/proof of presence shouldn't be required
13	63B	5.2.11	38		Activation secrets - I believe the intent here is to allow for a pre-set PIN to be used for access to an authenticator on first use. For example, where a certificate has been pre-provisioned on a smart card medium and is given to the user with a PIN already set for access. However, calling it "Activation Secret" seems to imply a bootstrapping use case such as logging into an account for the first time and not for account activation.	Add clarity that the activation secret is intended for authenticator first use and not for bootstrapping use cases
14	63B	General	iii		AAL levels are clear and the summary on page 13 is very helpful. It would be beneficial to call out where FIDO passkeys apply as this could be interpreted differently based on the FIDO implementation.	
15	63B	General	iii		Definition of phishing resistance makes sense and works in context with the AAL descriptions. Thank you for spelling this out.	
16	63B	General	iii		In response to the question around session management thresholds and reauthentication, it maybe beneficial to agencies to have NIST provide guidance but not exact session lengths as session lengths may need to vary depending on applications being used and the data being accessed. These recommendations may need to be adjusted due to threat landscape as well so a hard guideline from NIST might not be favorable.	
17	63C	5.4.2	27	1011	Typo - "...diverge from with each other over time."	Change to "...diverge from each other over time."
18	63C	6.1.2.2	39		Further clarification or perhaps some examples will be helpful in describing the RP-managed bound authenticators. Section was a little confusing.	Examples could be helpful here - I noticed examples are called out in the IdP-managed bound authenticator section

19	63C	5.4.1		25	Fig. 6, general in section	Identity API is called out at an implementation level while other transactions are called out at functional level.	As the identity information could be held by the RP, IdP or CSP, it might make more sense to call this out at a functional level rather than specifying an API. This drop to implementation details from functional descriptions seems out of line with other descriptions in the documents.