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

Please submit responses to dig-comments@nist.gov by April 14, 2023

Organization:	*Incode Technologies, Inc*
Name of Submitter/POC:	*George Theobald*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63A	Purpose	2	360	NIST should acknowledge that remote proofing of identities of people calling into a call center/support can be of value, particularly in cases where financial or other sensitive transactions are being conducted.	While the focus of the document is outside of call centers, acknowledge that integrity for such transactions is improved by remotely proofing individuals before sensitive information is exchanged between the individual and the call center staff.
2	63A	4.1	6	459	Example attributes do not include physical attributes about the individual.	While understand that the list is not exhaustive, recommend explaining that collecting physical attributes about the individual can further bind the person to the identity. For example, if eye color is an element that appears on the evidence, that attribute can be compared against the actual eye color found in the selfie to further match the individual.
3	63A	4.3	9	505	States that photocopies of evidence are acceptable, yet many of security features on forms of Strong and Superior evidence cannot be validated from photocopies.	Recommend that photocopies of evidence be limited to fair or weak strength evidence
4	63A	4.3.4.4	14	653	Allows for attribute information from multiple sources, however there is no qualifications for said sources. Concern is that just about anybody could be a source and there could be collusion among each source	Recommend that there be qualifications for "sources" that they are in good legal standing and be creditable.
5	63a	5.1.1.2	17	736	Master Death Files are know to have numerious errors. In one State DMV, several Driver Licenses were revoked upon recieving notification that a Driver was added to the MDF. However, the deaths were incorrectly reported and drivers were penalized for the misreporting of their death.	Recommend that multiple sources along with the MDF be used to check for data correlation that ensures accuracy and consistancy.
6	63A	5.4.2.1	28	1105	Strength of evidence for Real ID Driver License	Recommend that Real ID compliant DL/ID be catagorized as SUPERIOR when the the selfie is match against the photo on record with the actual issuing DMV, should such connectivity be established in the future.
7	63A	4.1	6	454	The identity proofing process involves the presentation and validation of the minimum attributes necessary to accomplish identity proofing - this should be applicable to the RP and not the CSP	Recommend including the RP to be respponsible for notification in instances where they are using a CSP as a 3rd party service for their offering.
8	63A	5.1.7	22	888	In many cases, the Relying Party is interacting with the invividual being served with the CSP providing a 3rd party service on behalf of the Relying Party. In these cases the relying party is better positioned to satisfy Proofing Notification that the CSP.	Recommend including the RP to be respponsible for notification in instances where they are using a CSP as a 3rd party service for their offering.
9	63B	4.2.2	9	525	Software-based authenticators that operate withinthe context of an operating system MAY , where applicable, attempt to detect compromise(e.g., by malware) of the platform in which they are running	For AAL2, why just suggest attempt to detect. Recommend Shall attempt to detect, where applicable.
10	63B	4.2.2	9	526	They SHOULD NOT complete the operation when such a compromise is detected.	Should Not language suggests there is an option to not complete the operation when detected. If it's detected, recommend that it Shall Not continue.
11	63B	4.2.3	9	548	SHALL be repeated following any period of inactivity lasting 30 minutes or longer.	Recommend following any period of a minimum of 30 minutes. If a CSP or RP desire for a shorter period of inactiviy, then it should be acceptable.
12	63B	4.2.1	8	516	Second sentence is confusing, seems to contradict third sentence.	Simplify sentence