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:	*Biometrics Security iTC*
Name of Submitter/POC:	*Brian Wood (Chairperson)*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63B	5.2.3	N/A	N/A	There is a call for PAD testing programs. The Biometrics Security iTC has created a public repository for PAD testing for fingerprints, eye, face and vein modalities. The current target of the requirements is to test to a basic attack potential. The iTC is currently launching a process to create a second set of tests which would meet at least enhanced-basic attack potential threats. The iTC is open to subject matter experts and any interested party to collaborate and provide feedback.	
2	63B	5.2.3	32	1278-12	The document states that biometrics shall only be used as part of multi-factor authentication. A mobile device may contain keys that can only be unlocked by authenticating with a biometric (and initially some sort of password/PIN/pattern). Would such as system be considered a multi-factor authentication to enable access to another system (not to the mobile device itself). The full sequence to meet the requirements would be: The user must enter a "something you know" to initially unlock the device and enable the biometric use The user could use a biometric (such as a face or fingerprint) to unlock the device The action of unlocking the device would allow access to a key that could be used to unlock a remote service (or another function such as a key to be transmitted over UWB) As the mobile device is the "something you have" this would seem to meet the expectations of multiple separate components, but in this case they are self-contained into one device to provide access to the external (to the mobile device) system. Clarification as to whether a mobile device used in this fashion would be acceptable to meet multi-factor authentication would be good to have (either that it is allowed or that it is not). If it would be allowed, it is likely that additional requirements may need to be provided on how the keys are released and used for remote authentication.	clarify if a mobile device with biometric authentication capabilities is considered multi-factor
3	63B	5.2.3	33	1290-12	The timeout period after 10 consecutive attempts being fixed at 30 seconds seems to be limiting of alternative possible solutions that are available on different systems. For example many systems implement blocks of allowed attempts with increasing timeouts between authentication failures (such as every 5 attempts the delay grows in a geometric progression).	Instead of requiring a minimum fixed 30 second timeout after each attempt, provide more flexibility with a minimum time set initially and then some expectations for attempts over time that could be met in a variety of ways (for example 5 attempts need to take at least 2.5 minutes after the initial 10).
4	63B	5.2.3	33	1290-12	50 attempts without PAD seems very high if the system is on the low-end of acceptable FMR, even with it being part of MFA	The number of attempts allowed should be lowered or justified as to why the number of attempts and the included delays are acceptable. It seems that the number of attempts should be tied to the FAR/FMR value of the system, and not globally defined. Possibly a table showing acceptable FMR values and a range of allowed attempts.
5	63B	5.2.3	33	1290-12	How is the relation between no-PAD and PAD (the 1:2 relation) determined? Is this the correct ratio?	Provide a justification for the determination of the no-PAD to the PAD ratio, or further information about how to determine a proper ratio in different device scenarios. The ratio may vary by modality or FAR/FMR.
6	63A	5.1.8	23	933-934	The requirement that only ISO/IEC is acceptable as a standard is limiting as several industry groups are working on implementing biometric and PAD performance testing, many based on the ISO requirements. These should be accepted as valid systems for testing. Note that industry standards can include ISO/IEC, FIDO, Biometrics Security iTC or similar programs. NIST should specify minimum requirements to conduct performance testing that would then set a minimum standard for expectations of this type of testing.	Testing of all algorithms and systems SHALL be consistent with published industry standards for the given modality.
7	63B	5.2.3	33	1280-12	Biometric performance testing should be done following best practices or international standards to measure the false acceptance or rejection objectively. Such standards should also be referred correctly. ISO/IEC TS 19795-9 "Information technology — Biometric performance testing and reporting — Part 9: Testing on mobile devices" uses FAR, instead of FMR, for the performance testing for mobile biometrics. ISO/IEC 19795-1 "ISO/IEC 19795-1 "Information technology — Biometric performance testing and reporting — Part 1: Principles and framework" states that confidence level shall also be determined to estimate the FAR/FMR to show that how the estimated FAR/FMR may be accurate. [ISO/IEC30107-1] is a standard for the PAD testing and explains that zero-effort impostor attempt is an example of human PAI. [ISO/IEC30107-1] doesn't mention or explain the FMR at all. The Biometrics Security iTC has created a guidance for biometric performance testing refering ISO/IEC 19795-1, however, this guidance doesn't require full compliance with ISO/IEC 19795-1 to enable cost-effective performance testing.	The biometric system SHALL operate with a false accept rate (FAR) or false-match rate (FMR) [ISO/IEC2382-37] of 1 in 10000 or better with adequate confidence level. Testing of biometric performance SHALL be in accordance [ISO/IEC19795-1].

8	63B	5.2.3	33	1287-12	Clause 12 of [ISO/IEC30107-3:2017] mainly defines metrics (e.g., IAPAR) that should be reported for the performance testing of PAD but provides little information about how to perform “Testing of presentation attack resistance”. Clause 9 of [ISO/IEC30107-3:2017] requires reporting how the PAIs (e.g., fake fingerprints) are created, however, this standard doesn’t tell anything about how the PAIs should be created (e.g, material or tools used for the creation of PAIs). Primitive PAIs can be created easily but such PAIs are simply rejected by data capture or quality check before reaching to the PAD subsystem. That’s is the reason why the Biometrics Security iTC developed the various recipes for the creation of useful PAIs to conduct the meaningful PAD testing. [ISO/IEC30107-3] doesn’t specify who should perform the PAD testing. The Biometrics Security iTC recommends that the testing should be done by the evaluation labs to confirm that the devices have adequate presentation attack resistance because it may be difficult for non-biometric experts to judge this decision. [ISO/IEC30107-3:2017] has been revised by [ISO/IEC 30107-3:2023] and Clause 12 of [ISO/IEC 30107-3:2017] moves to Clause 13 of [ISO/IEC 30107-3:2023].	Testing of presentation attack resistance SHALL be in accordance with industry standards. Note that industry standards can include ISO/IEC 30107, FIDO, Biometrics Security iTC or similar programs. Update the reference to ISO/IEC30107-3 to the latest version.
9	63B	5.2.3	34	1326-13	Guidance created by the Biometrics Security iTC only recommends vendors to report test subject demographics (e.g., age, gender and ethnicity) in the performance test report because there is no best practice or standard (e.g., how many test subjects should be gathered for each ethnicity at minimum?) to estimate performance for different demographic types objectively. However, ISO SC37 is developing ISO/IEC 19795-10 “Information technology — Biometric performance testing and reporting — Part 10: Quantifying biometric system performance variation across demographic groups” and we may see a clear standard in this area in the future. So, SHALL (requirement) should be replaced with SHOULD until we can see such standard and have a common understanding what “similar performance” exactly means.	In lieu of published standards on how to achieve statistically-sound demographic biometric performance testing, testing reports of biometric authentication technologies SHALL provide information about the demographic breakdown of test subjects whose biometrics were used in performance analysis.
10	63A	5.1.8	22	943 & 9	These lines are duplicate	Remove one of the lines.