	Publication				Comment	
Comment #	(Base, 63A, 63B, 63C)	Section	Page #	Line #	(Include rationale for comment)	Suggested Change
1	63B	Entire	1		The 800-63B authentication specification, and most mainstream MFA products, ignores use cases where users may have adverse interests to the relying party, such as a desire to alienate or share their identity, either in an attempt to commit fraud, to evade detection of aliases, for expediency, or to share an access benefit among a group of co-conspirators. Tokens and phone authentication techniques allow for unauthorized delegation through sharing devices or enrolling a proxy, even into a "biometric-protected" factor. FIDO is, at its core, a consumer technology, so the holder of a biometric FIDO token is free to enroll anyone else's fingerprint as an authorized user. PIN codes and tokens can be shared and often are. Central biometric verification has a longstanding role in preventing unauthorized delegation and account sharing, yet it is cast only as a minority use case, ignoring the relying party benefits inherent in controlling the entire authentication stack, not assigning access governance to the end user.	Recognize that centrally managed and secured biometrics have been used for decades, and plays an important role in the identity use case spectrum. Properly implemented with user choice, consent, cryptography at rest and in motion, integrity and control, biometrics serves an important role in protecting the interests of the relying party in more intimate trust scenarios, while making the subject tightly-bound to their identity, and unable to delegate it.
2	63B	5.2.3	32	1257-12	Pairing biometrics with tokens effectively eliminates the important What-you-are factor from practical implementation in a NIST-conforming solution due to excessive cost of adding unnecessary hardware to each user. The flimsy enumerated reasons for precluding biometric authentication options unless paired with a what-you-have hardware factor demonstrates that 800-63-B has been influenced to its detriment by the FIDO Alliance's anti-competitive, anti-central-biometric standard, which similarly prohibits biometrics except when attached to a hardware device. As background, it is important to observe that the FIDO Alliance's founding and earliest Board members (Infineon, Yubico, Synaptics/Validity, Lenovo, NXP, Qualcomm) all had a vested interest in dampening the market for centralized biometrics, which represents an existential threat to the what-you-have authentication market. Consequently, FIDO amplifies and exploits mistaken concerns about central biometric reliability and privacy in order to standardize a requirement for the what-you-have factors they sell. using the power of their standards-setting organization to deprive consenting users and relying parties from a full spectrum of authentication options to address all use cases. It should surprise no one that a group of what-you-have factor market players would deprecate central biometrics by creating an anti-competitive FIDO standard that arbitrarily forecloses the use of a longstanding and successful competing technology approach unless combined with the tokens and phone factors they profit from. The sleight of hand is at its peak where FIDO's Enterprise Lifecycle document accommodates the use of "remote biometrics" to re-proof a subject as part of reassociating them a new token. Likewise IAL2 and IAL3 call for a biometric verification against what could be a centrally-stored biometric. Contrary to these allowances, and ignoring decades of central biometric use cases and success, the 800-63-B adoptee is instructed that can not use that same centrally stored biometric to authenticate without having to procure, provision, and lifecycle replace multiple FIDO tokens per user for everyday authentication. Biometrics is a well-tested, proven technology, whose value is significantly diminished when forced to pair up on a dance card with costly tokens, especially for roving users and asymmetrical deployments involving more people than access points. A person being their own credential without something to carry represents an existential threat to the what-you-have manufacturers' continuing revenue, but that should not influence this standard.	Commercial-grade centralized Biometrics should be allowed as a factor without sandbagging it by mandating it only be allowed in combination with a hardware token. Every reason listed is either a misrepresentation of the current state of the art in biometrics, or is subsequently mitigated in the SHOULD and SHALL recommendations that follow on the page that follows. If the mitigation measures on p. 33 are implemented to ensure a quality matching algorithm, PAD mitigation, integrity evaluation, and data protection (not revocation), the red herring reasons in 1259-1262 relating to vague, outdated and misleading statements about biometric shortcomings are a neutralized. The statement that biometrics are somehow vulnerable because "they are not secrets" has long been a trope of the anti-biometric triad of fraudsters, competing technology companies, and well-intentioned privacy advocates. Biometrics is not based on secrecy. Biometrics is based on integrity, because biometrics are unchanging facts about the subscriber. The competing interests try to impose the requirements of a secrecy-based authentication model on an integrity-based one, and have had great success in FUDing the marketplace. When viewed as an integrity-based, not secrecy-based system, concepts of revocable biometric data become superfluous, in favor of proper encryption of data at rest and in motion, and use of indirection to separate identity from biometric records. Review those claimed reasons in light of modern biometric deployments, where accuracy and PAD resistance biometric FMR doesn't provide "confidence of the authentication" and that algorithms are "probabalistic vs. deterministic", when these authentications are being performed in a 1 to 1 matching manner, and the accuracy of the modern fingerprint algorithm is better than 1 in 100's of thousands.
3	63B	5.2.3	33	1306	This statement - that matching should be performed locally, not centrally, places a perceived user privacy concern ahead of the relying party's interest in being certain who they are dealing with. WIth consent, encryption at rest and secure communications to protect biometric data from manipulation, central biometrics serves an important role in providing long-lasting, device independent identity services. Biometric data is not a secret, but rather is factual datum, derived by measuring publicly-observable individuals. Biometrics relies on integrity of processes and storage, not secrecy. Revocation is a red herring, because biometric facts remain the same and can be obtained by measuring the individual at any point. Treating biometric data like it must be kept secret instead of what it is - factual measurements derived from a public person - perpetuates the misconception that biometrics require secrecy to operate effectively.	Rather than putting preference on user-governed biometric processes, recognize that for high-trust scenarios, or to prevent unauthorized delegation, biometrics can be managed and matched centrally. Biometric data - whether locally or centrally stored and matched - should be secured and encrypted at rest and in motion in a manner sufficient to ensure that the data is valueless to any attacker or insider who attempts to exfiltrate the data.
4	63B	5.2.3	33	1314	Revocation can be substituted with encryption and data isolation techniques. Revocation is a red-herring designed to mitigate a belief that enrollment data could be used to assume an identity if stolen. Encryption and data isolation achieves the same end without imposing a specific scheme	Require that data at rest be encrypted such that a compromise to the data store will yield only useless data.
5	63B	5.2.3	33	1310	This secures FIDO and its board members with the market dominance that they desire, but at the detriment of the market economics and user experience. Biometrics should be allowed where a secure channel protects the biometric data from interception, tampering and manipulation, and is not reliant on a "main authenticator" being unlocked first.	Allow a properly-implemented biometric system without the encumberance of a hardware token required.
6	63B	5.2.3	34	1326	This requirement relating to avoiding demographic bias goes to accuracy, and should be stated up with the bullets on FMR and PAD.	
7	63B	5.2.3	34	1307, 13	The term "verifier" is confusing because many interpret it to mean "matcher", implying that encryption must be atomic between the sensor and the matcher. This imposes unnecesary centralized processing burdens on the system. "Verifier" is defined in the definitions as an entity doing the identity verification, which would then imply that the requirement is for authenticated protected channel from a USB-connected fingerprint scanner to a process that is under the custody and control of the verifier entity, even if that process is running on an end-user device. That process might perform some pre-processing such as quality analysis or template extraction, and then prepare an encrypted data package to send to its server, but the authenticated channel is at that point between it and the server, not the sensor and the server.	Specify that the goal is to protect against biometric spoofing by way of USB replay, and against tampering, manipulation or injection in transport. State that the operator of a biometric system should ensure that biometric data is secure at all points during its movement, including capture from remote systems with biometric capture devices conected, as to ensure high confidence in the integrity of the entire custodial pipeline.