General Responses

#	Volume (800-63-3, a, b, c)	Current State	Suggested Change	Rationale	Reference Location (Section #.#)
1	3	AAL2 supports a wide range of technologies that offer different authentication strengths. For example, both OTP and FIDO are both AAL2.	Differentiate in AALs between authentication tools that are phishable and that are phishing resistant.	Phishing has emerged as a threat that is now making it possible to compromise authentication factors used in MFA (such as OTP and some types of push notifications) that are based on shared secrets. Given how threats have evolved, NIST should be looking to 1) help implementers understand these threats and 2) steer them toward phishing-resistant authentication. Authentication guidance should focus on resistance to common threats.	
2	3	AAL 1 , 2 and 3, the strength of authentication is measured by counting how many Multi-factor Authentication methods are used irrespective of weakness due to common vulnurabilities.	Strength of multiple authenticators should require the use of different factors with NO overlapping security vulnerabilities.	Most multi-factor authenticators are susceptible to phishing / MIM attacks. Authentication strength is improved by using factors with NO overlapping vulnerabilities. Text needs to discourage the use of factors with common vulnerabilities.	
3	3	Authentication is treated as a binary operation. No focus on dynamic risk based authentication.	Modern authentication binds a user to a device to a credential. Relying party can tell if the the user has is a connecting from a known user/device/location combination as opposed to a new unseen before access tempt. In summary, a risk engine can be pretty sure about the identity of the user even before creditails are echanged. Risk based authentication should be supported.	Modern authentication is a lot about perception. A Relying Party can deduce who is the claimed identity before credentials are exchanged. Risk-based authentication should be encouraged.	
4	3	Account Recovery/Credential Recovery is not addressed properly. Some autthentication methods (e.g. FIDO) require a robust account recovery method.	Some authentication methods can benefit from using trust frameworks where there is a trusted device that can be used to enroll or recover credentials to the user device. This step is needed for passwordless methods.	Passwordless solutions need a robust method to allow user to logon through more than a single device or to recover access when a particular device is lost or is upgraded.	
5	3	During the COVID-19 pandemic, the White House issued the memorandum M-20-19 with exceptional rules for authentication and identification for remote workers. Stated in 800-63-3 ---- 2.1 applicability. These users are expected to hold a valid government-issued credential, primarily the Personal Identity Verification (PIV) card or a derived PIV.	This expectation on PIV cards SHOULD be relaxed to allow for other types of authentication devices (for example FIDO authenticators), at least temporarily during a pandemic or similar crisis.	The eID initiative in Europe kept going with online services despite the pandemic because they had the right tools is place. NIST should clear a path for the same provisions during a crisis.	
6	3	Data Tokenization	Fully consider user consent	User consent remains a hot and evolving aspect of identiy. Consider how much the privacy landscape has changed since 800-63-3 was first published. GDPR has become mainstream, states are passing their own privacy legislation, and there has been a push for Congress to do likewise. While nobody holds a crystal ball on what the next five years will bring it's probably safe to assume that user consent will not "go away." -4 should consider consent aspects, including extension and revocation, and the auditability to be able to demonstrate compliance.	
7	3	Proofing	Differentiate between entity-managed and federated solutions. Entity-managed solutions should be leveraged across a given entity. Federated solutions should rely on open protocols such OAuth. Zero Trust should be the default posture.	Entity-managed solutions should have as wide a net as possible to be able to leverage behavior events. Despite deployment across the entity, they should be context and channel aware.	
8	3	Authentication	Authentication should consider real time channel-oriented event-level interdiction services that define: * When, with what, and how often, but also context with channel awareness needs to be deployed to manage risk * Events could be defined to describe transaction risk level and for authentication via appropriate Authentication Level as POLICY. * SMS -> TOTP / Bio need to be factored in conjunction with Identity proofing in RT.	As with above, identity systems need to move away from static indicators as much as possible, instead leveraging real-time information that is organizationally aware.	
9	3	Continued use of short message service (SMS) and public switched telephone networks (PSTN) as restricted authentication channels for out-of-band authenticators	o MNO and or device-binding must be at PKI level for carrier data where applicable. o Local authentication is needed, thus switching to Secure SMS as opposed to vulnerability-prone normal SMS o Time based tokens on local host are desired for higher transaction risk levels		
10	3	Security and performance capabilities (e.g., presentation attack detection or liveness testing) for biometric characteristic collection to support Identity Assurance Level 2 remote identity proofing in the areas of identity evidence verification (physical/biometric comparison) or binding of authenticators.	o Traceability of events from perimeter attacks to fraud systems at backend are good. o BOT & CVA should be part of risk mitigation plan with ability to fraud losses or ATO impacts o Integration with threat monitoring + feedback loop at higher layers (LI4- L7)		
11	3	Capabilities and innovative approaches for remote identity proofing to achieve equivalent assurance as in-person identity proofing	o Answered above o RT interdictions services where proofing needs to be standardized at firm and anytime digital profiles are updates cross channel, RT risk assessment with aging process needs to be defined.		
12	3	Security and privacy considerations and performance metrics for the use of behavioral characteristics as an authentication factor	o Retention of authentication o Customer defined preferences o Ability to interdict and measure challenge rate by channel & product o Performance of delivery tools on customer impact o ATO/CVA/BOT attack impacts need to be measured so profiles aren't getting damaged o Model accuracy + analytics should be getting good visibility to power all aspects of fraud decisioning including prevention + detection as volumes would need to be systematically managed in a risk based construct as opposed to conditional logic rules only (exceptions would be applicable at specific attack vectors).		
13	3	Use of dynamic knowledge-based information for identity verification	o Needs to be a contingent or secondary control o Captchas, visual authentication or voice authentication could be considered as well.		

14	3	Capabilities to meet Federation Assurance Level 3 (see SP 800-63C FAQ C03)	o It has to be in a decentralized mode preserving integrity & atomicity of transactions o Liability aspects are key ,therefore consume but verify model in anonymized mode would be recommended. o Privacy needs to be considered.		
15	3	Capabilities and security considerations for verifier impersonation resistance (see SP 800-63B FAQ B04)	o Use biometrics with behavior to address the risk. o MFA in bio context is needed o This is a key area of fraud – especially in branch and care center. o Address MITM or MITB attacks		
16	3	Address verification is an operational challenge especially when using out of band systems like mailing postcards to physical mailing addresses.	Would ask to clarify the value gained in security from these methods vs. UX and see if other methods deliver similar net gains (e.g. using address of ID Card).		
17	3	Biometric-matching focuses on tech performance "selfie-to-selfie" but does not specify performance specs around selfie-to-card image which is a different problem for IDV (vs. authentication.)	Would recommend setting minimum performance metrics for this use case in addition to authentication. In all cases, the FMR needs to measured with representative data for the use case, i.e. for doc vs selfie or vs video. Generally, FAR and FRR need always to be presented as a pair.		
18	3	Biometric data reuse for repeat attacks	It would be advantageous that malicious users who have been identified with sufficiently high confidence should have their biometric data retained (in a privacy-preserving manner) so that it may be used to filter them out on repeat attacks, which is a common attack pattern. Ideally the industry could work together to share this data to prevent these attacks cross sites? There is a big privacy canyon that needs to be navigated, but an equally big opportunity for the industry to tighten down on fraudsters/rings.	Reference: Biometrics are also used in some cases to prevent repudiation of enrollment and to verify that the same individual participates in all phases of the enrollment process as described in SP 800-63A.	
19	3	Generally in-person proofing is becoming more challenging, so prioritizing stronger remote proofing seems like a good goal, especially considering the current frame or COVID world.	Can we use more live chat/recordings of video as a stronger proxy?	There should be a mechanism to support asynchronous video based verification, where the video is authenticated. Not exactly like but similar to the consumer app Marco Polo.	
20					
21					
22					
23					
24					
25					