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:	*iProov*
Name of Submitter/POC:	*Campbell Cowie*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63A	9.1	45	1499	We welcome the focus on usability and equity. Usability is a multifaceted and complex challenge and it would help to have more granular support, in particular setting clear principles to which providers of identity services should be required to satisfy. Whilst a lot of what we would consider core facets of usability are covered, it is critical that providers accept accountability for protecting users against identity fraud threats. 101 of ERM is that risk should rest with the party best able to mitigate it. We know consumers are ill equipped to understand the complex nature of the threat landscape so they should not be required to either own the latest devices or to be required to maintain the latest device-based security. That is neither a proportionate nor a realistic proposition. At the very least providers should be transparent with users over what measures they adopt to safeguard users from sophisticated identity fraud such as depfakes and synthetic identities.	Add the key principles for a useable service - suggested: Inclusion through user choice: No imposition or requirement for special device hardware or sensors. Ability to securely authenticate on any device with a user-facing camera. Inclusion through accessibility: Device & platform agnostic to include all users; Robust performance and bias monitoring;Cloud-based delivery Robust choice pathways: Non-biometric enrolment option must be equally secure…even if convenience is sacrificed. Device risk mitigation: No reliance on users' devices for security. Mitigate risk from synthetic or compromised devices. Identity recovery: Users should not be required to re-enroll when devices are changed or replaced. Verification integrity: Use inaccessible processing to prevent reverse engineering by attackers. Mitigate the threat of adversarial attacks. Relieve users of the burden of responsibility: Implementation of new detection algorithms must not rely on or compel the user to update their personal device. Agile response: Ongoing threat intelligence should be included to evolve defenses and protect users from fraud.
2	63-Base	2.1	3	369	Serivces should be required to demonstrate compliance with availabe accessibility standards, such as those provided by WCAG	Insert " by ensuring compliance with available accessibility standards, such as those provided by WCAG."
3	63-Base	5.2.3	32	1241	Given the potential impact on consumers from identity fraud, where a non-biometric/liveness check is not included or where the provider is unable to confirm an active threat intelligence capability the impact level should default to High, with requisite assurance measures adopted.	Insert "Where there is no active threat intelligence capability or where the impact of identity fraud is uncertain, organisations shall categorise the impact as High."
4	63-Base	5.5	39	1481	Given the potential impact on consumers from identity fraud, providers must offer a robust threat intelligence service, including active monitoring of the threat landscape.	Replace "should" with "shall"
5	63-Base	5.2.2.1	31	1204	The definition of IAL 3 places users at a significant risk of fraud. It is well understood that a physical check of documents by an operator is less secure than a biometric liveness check. For example, a recent report from the Chaos Computer Club on the use of video ident by German agencies, including health authorities, has shown how simple it is for bad actors to overcome physical checks by human operators. See https://www.ccc.de/en/updates/2022/chaos-computer-club-hackt-video-ident. And for the avoidabce of doubt the work of the CCC is highly respected even by the German Government, who regularly call upon their testimony for Parliamentary hearings. Similarly, it is as a result of weaknesses in operator controlled systems that the European Banking Authority has recently revised it guidelines for remote onboarding to require a liveness test (https://www.eba.europa.eu/eba-publishes-guidelines-remote-customer-onboarding). The presumption that a human check is robust and provides assurance sadly does hold hold up to scrutiny in the real world. As it stands, compliance with the guidelines in this area would leave US consumers at risk.	For IAL 3 a liveness check using biometrics should be a required minimum, which can be complemented by a human operator check if required.
6	63A	2.2	4	419-421	As above, the use of a human, even one that is trained, is less secure than a biometric test including liveness. Respected studies have shown this and regulators in other markets, notable the EBA, has accepted this and now requires a biometric liveness check.	As above, a human check should only ever be as a complement to a biometric check incorporating liveness.
7	63A	5.1.8	23	935-937	The performance thresholds are fair for digital systems. Where the Guidelines permits the use of trained operators to conduct physical checks this should only be in cases where the performance of the operators meets the same threshold. Otherwise, customers are being put at risk.	CSPs shall meet the minimum performance thresholds for all usage (biometric and when employing in person checks).
8	63A	5.1.8	23	956-958	It needs to be recognised that operators/humans are less well equipped to identify deep fakes and synthetic identity fraud than liveness based biometric tests.	
9	63A	5.5	29	1143-1147	It needs to be recognised that in person checks are inherently less secure than biometric checks. NIST has not explained why in person checks provide the highest level of assurance when research routinely shows this not to be the case. At the very least, in person checks should meet the same performance criteria as are set for biometric checks.	

10	63A	5.5.8	31		As above, it has been shown repeatedly in tests that in person video identity checks are less secure than biometric checks incorporating liveness. The recent report from the Chaos Computer Club in Germany shows well the vulnerabilities with in person video identity checks. As a result of their recent work video identity has been withdrawn as a means of checking identity for a number of parties, including health authorities. The German cyber security authority has similarly confirmed that video identity is less secure than biometric checks in face of deep fakes, synthetic identity and even low level document fraud. At the very least operators conducting in person checks (physically or by video) must meet the same performance standards as is required of biometric checks.	
11	63A	7,1	37	1314-1219	Agencies should be required to inform end consumers what active monitoriing of the threat landscape is in place. That way, consumers are better informed as to the nature of the risks involved. The threat landscape is evolving rapidly and without active monitoring end consumers are at risk from sophisticated fraud. Failiure to be transparent around the nature of acgive threat monitoring, or even if there is no active monitoring in place, places consumers at risk.	
12	63A	10.3	53	1797	As above, it needs to be recognised that in-person or use of video indentification, rather than biometric checks incorporating liveness, is high risk as it is well understood that bad actors are easily to fool non-biometric checks. Should NIST decide to keep in-person or video identity based checks then these will need to be subject the same rigorous performance checks as those applied to biometrics.	"...with in person checks being subject to the same performance management requirements as those applied to biometric checks."
13	63A	5.1.8	23	933	Clarity which specific standards	"ISO 19795"
14	63A	5.1.8	23	953-955	Clarify specific standards	"ISO30107"
15	63A	5.18.6	23	943	Risk that requireing ALL performance testing to be published risks dissuading providers from testing. The requirement should specify a narrower set of standardised tests, rather than the guidelines being for "all" tests.	