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

Please submit responses to dig-comments@nist.gov by October 7, 2024.

Organization:	*Socure, LLC*
Name of Submitter/POC:	*Matt King*
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
	63A	2.5.1	14	809	**THEME**: Fraud Mitigation Measures **RECOMMENDATIONS**: Clarify "(unattended) using a captured video or photograph and the uploaded copy" means the video is captured by the CSP, not the applicant. Photograph should be removed as all comparisons should be via video or multiframe capture. Also clarify consent conditions. **RATIONALe**: All capture for comparison should be video or multiframe; single frame captures are too easy to spoof. All capture must be done live within the session and not allowing upload (other than of the evidence). Consent must be conducted in the same session as the capture.	Automated (Unattended) biometric comparison. Automated biometric comparison, such as facial recognition or other fully automated algorithm-driven biometric comparison, MAY be performed for onsite or remote identity proofing events. The facial image or other biometric characteristic (e.g., fingerprints, palm prints, iris and retina patterns, voiceprints, or vein patterns) on the identity evidence, or stored in authoritative records, is compared to the facial image in a video or other multiframe capture of the live applicant or other biometric live sample collected by the CSP from the applicant during the identity proofing event.
	63A	3.1.4	22	1078	**THEME**: Equity and fraud mitigation measures **RECOMMENDATION**: The draft places the burden of assessing whether "the elements of [an] identity service" are either inequitable or not, without clearly defined standards or definitions of key words such as "equity", "groups," "access," "treatment," and "outcomes." CSPs should be held accountable to the same, objective, measureable standards so that agencies may have assurance in their assessments. In comparison, the well-established fair lending and fair housing legal frameworks both define protected classes and types of overt and inadvertent discrimination. There are expectations that businesses subject to these laws not only pro-actively design their products and processes for fairness, but also retrospectively test them for equitable results across the defined classes. Also, the draft does not distinguish between inequities that stem from agency actions, meaning how they may use the identity service. Agencies will still control aspects of identity proofing that may impact effectiveness of an identity service. For example, the digital user experience may be more difficult for certain types of users, from inaccessible language for less educated persons to prejudicial or unfriendly language to visual designs that are harder for the elderly to comprehend. If a CSP is to assess the outcomes of the use of its service, it may need to reflect upon the context in which its services are deployed. This requires a feedback loop from the agency. Finally, the expectation of mitigation measures could be narrowly construed to mean singular, post hoc measures. In comparison, the financial services sector has a mature, *lifecycle* approach called *model risk management ("MRM")* . Entities using quantitative models to make decisions must develop governance spanning all stakeholders, processes to document and validate methodologies, control framework, and clear risk quantification. The fulsome expectations of MRM are not only useful to regulated entities, but they also minimize the possibilities of wide variance and gaps in how entities interpret the standard.	Add a new item #2 in section 3.1.4: The CSP SHALL consider equity in making determinations of fraud mitigation measures. The CSP SHOULD establish categories of users in edge populations and measure performance of those categories against established baselines to determine and monitor impacts and bias within the system and maximize inclusivity. The CSP SHOULD consider established frameworks that define protected classes and types of overt and inadvertent discrimination, such as those used in fair lending and fair housing legal frameworks and the model risk management ("MRM") lifefcycle approach used in the financial services sector.
	63A	3.1.11	27	1234	**THEME**: Biometrics **RECOMMENDATIONS**: Clarify biometric deletion request allowance **RATIONALE**: The current language states only that the CSPs allow a request, does not account for the attack vector in which an attacker can continually delete their image and immediately reuse it	CSPs SHALL allow individuals to request deletion of their biometric information at any time, except where otherwise restricted by regulation, law, or statute. The CSP MAY deny this request if the biometric information is known to have been used in attempts to commit fraud.
	63A	3.1.11	27	1268	**THEME**: Biometrics **RECOMMENDATIONS**: Narrow requirement on public availability of all biometric system testing (#13) **RATIONAL**: The current language is overbroad and risks unintended consequences. For instance, testing may occur daily for new clients or potential new model parameterization, creating a flood of testing results that do not provide additional insight into the biometric system performance.	[NIST should either remove this requirement or specify a testing program to which it applies. As written, it would apply to a developer debugging at their desk and running a test. There is no definition of what such a "performance and operational test" would be, making it a problematic requirement that gives little guidance to Agencies, CSPs, or other identity solution providers and could be misleading or lack value as each CSP produces its own non-stndard report to meet the requirement.]

	63A	3.1.11	27	1272	**THEME**: Biometrics **RECOMMENDATIONS**: Disallow single frame capture for liveness **RATIONAL**: The current language does not prohibit liveness testing with single frame comparison	Add to #1 "The following requirements apply to CSPs who collect biometric characteristics from applicants: 1270 1. CSP SHALL collect biometrics in such a way that provides reasonable assurance that the biometric is collected from the applicant, and not another subject. CSP SHALL NOT use single frame capture methods to establishing liveness detection."
	63A	3.1.11	27	1260	**THEME**: Biometrics **RECOMMENDATIONS**: Require facial matching to known fraudsters **RATIONALE**: Understanding this has been a contentious topic, comparing the captured biometric of an applicant to that of those with known fraudulent use is the single most effective fraud mitigation strategy available. NIST should require this comparison, but should put extremely tight constraints on the matching sensitivity to ensure equity and minimal false positive matches. In addition, use of automated tools will likely be more effective than a trusted agent to confirm results, so the requirement should allow for automated tools that meet a false match trheshold or a trusted agent.	Revise item #10: CSPs SHALL compare the collected biometric to a corpus of known fraudulent of attempts or biometric information connected to other personal information. The CSP SHALL either meet a performance threshold for biometric usage of 1:100,000 for false match rate or require a manual review by a trained proofing agent or trusted referee to confirm the automated matching results.