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

*Please submit responses to dig-comments@nist.gov by March 24 April 14, 2023*

| | |
|---|---|
| ***Organization:*** | *Experian* |
| ***Name of Submitter/POC:*** | *Eric Thompson* |
| ***Email Address of Submitter/POC:*** | [REMOVED] |

| Comment # | Publication (Base, 63A, 63B, 63C) | Section | Page # | Line # | Comment (Include rationale for comment) | Suggested Change |
|---|---|---|---|---|---|---|
| 1 | 63-Base | 5.1 -5.3 | 24 - 39 | 965 - 1475 | The consideration of impact to mission delivery in addition to cybersecurity risk was only accounted for under 'compensating controls' in the previous version. This consideration is critical for organizations to effectively manage risk of both error types that could impact their agency: Type I error (rejecting a good subject) and Type II error (accepting an incorrect subject).<br><br>To effectively manage these combined risks, it requires a fairly mature identity proofing measurement system that tracks the outcomes of the process. These measurement systems require processes and data environments that are not common across all organizations. | Recommend providing a supplement specific to Identity Risk Measurement Systems will be key to effective implementation and management of a risk-based approach to identity management. |
| 2 | 63A | 4.3.3.1 | 11 | 557 - 559 | Given the potential for a newly issued accounts to have been established by a bad actor as part of identity theft scheme, we recognize there should be concern related to recency of issuance. However, automatically excluding any evidence that has been established in the past six months seems relatively arbitrary and lacking justification. | Revise the statement to read:<br>"The evidence has not expired or it expired within the previous six (6) months. If it does not contain an expiration date, it SHOULD be reviewed for recency of issuance prior to acceptance." |
| 3 | 63A | 4.3.4.3 | 14 | 647 - 654 | The ability for use of either authoritative or credible sources to validate identity evidence and attributes is critical to modernize any digital identity proofing process. While it was not specifically addressed in the previous version, it was the de facto method of automated validation of fair evidence.<br><br>The addition of credible sources in addition to authoritative sources better reflects the reality of what constitutes effective validation. However, the current draft (§4.3.4.4) lacks any requirement related to a credible source's reputation or credibility. The definition of credible source should include some measure of credibility, e.g., governmental regulatory oversight. Without an independent recognition of credibility included in the definition of a credible source, this runs the risk of rogue entities acting in this capacity. | Include a measure of credibility in the for a 'credible source', e.g., subject to governmental regulatory oversight. |
| 4 | 63A | 5.1.3 | 19 | 793 - 821 | As written, this section suggests the need for CSPs to collect demographic data to assess for equity. Given the requirement to minimize collection of data (800-63-4ipd §5.5), there should be no expectation to collect demographic characteristics to measure equitable impact as it relates to race, religion or other similar demographics (even if optional for the subject to enter). | Recommend clarifying this section to reflect any equity assessment may partner with federal statistical agencies and does not require additional data collection, as outlined in the "Recommendations from the Equitable Data Working Group" report resulting from EO13985.(https://www.whitehouse.gov/wp-content/uploads/2022/04/eo13985-vision-for-equitable-data.pdf) |
| 5 | 63A | 5.1.9.1 | 24 | 994 - 995 | The use of trusted referees should be an alternative available to increase equity and access to services for some, but should not be required where the system alone can suffice. | Revise first sentence of §5.1.9.1 to read:<br>"CSPs SHOULD provide the option for the use of trusted referees for remote identity proofing at IALs 1 and 2." This resolves the inconsistency with following sentence, which suggest that this is not mandatory by stating, "Where trusted referees are offered…" |
| 6 | 63A | 5.3 | 26 - 29 | 1035 - 1141 | In the current draft, IAL1 and IAL2 are not positioned to achieve balance between equitable treatment, meeting mission delivery requirements and mitigating cybersecurity threats. The concept of relying on documentary evidence at the STRONG or SUPERIOR level needs to be rethought to achieve success across these multiple criteria of success laid out in the new draft guidance. | Recommend including an option to incorporate advanced analytics as an additional option for validation and verification at the STRONG level.<br><br>At IAL1 or IAL2, identity risks can be effectively managed without mandating use of existing STRONG evidence for ALL subjects. By combining multiple pieces of evidence in conjunction with risk signals related to identity theft or synthetic identity fraud, organizations can meet their mission delivery needs, manage cybersecurity risk and ensure equity in managing Digital Identity more effectively than with what is currently rated as STRONG evidence.<br><br>Examples of fraud risk signals include, but are not limited to, PII data recent activity, Phone account and activity attributes, email data/attributes from ISPs, device and IP address review for high-risk indicators, anomalous credit bureau data, and behavioral characteristics. The use of these signals within advanced analytics to create an Identity Confidence model has proven extremely powerful in effectively reducing cybersecurity risk while simultaneously minimizing impact to good subjects within the private sector for years. Including an Identity Confidence model validation option better enables organizations to meet both their mission delivery and cybersecurity risk needs.<br><br>It is critical to ensure any use of fraud risk signals in coordination with identity proofing include empirical evidence of its effectiveness in addressing the cybersecurity risk (false negative errors) as well as mission delivery risk (false positive errors). This can generally be shown using a variety of model performance and validation analytic techniques (e.g., Receiver Operator Characteristic Curve, Area Under the Curve, KS test, GeNIe). These techniques inherently require effective measurement systems to determine subjects' disposition as either good or bad. An alternative method of measuring model performance where there is limited performance data can be random sampling to get a high level of confidence related to the model's performance.<br><br>With this approach, an Identity Confidence Score could be applied to subjects as an initial, passive option to risk rank the population. Where the confidence score renders the Identity Confidence risk LOW, then the CSP can require the current STRONG evidence to complete identity proofing. |