**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:*** | *Department of Veterans Affairs* |
| ***Name of Submitter/POC:*** | *John Rahaghi, Thomas Black, Porta Antiporta* |
| ***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 | 5.3.2 | 38 | 1641 | Comparable often refers to comparable in security. | Explicit call out on balancing compensating controls between security and equity / access. |
| 2 | 63-Base | 5.4, 5.5 | 39 | | These sections only focus on improvement, evolution of threat actors. It doesn't call out explicit improvements to consider for equity/access. | Add sections on improving equity and access. |
| 3 | 63A | 4.3.3.1 | 11 | 548 | In rev3 supplemental implementation guides, SSN is listed as WEAK. Yet when comparing how SSNs are issued, it meets the guidance of FAIR evidence. | Can NIST either update implementation resource to move SSN to FAIR _or_ provide detail as to why SSN would considered WEAK compared to a financial institution statement. |
| 4 | 63A | 4.3.4.4 | 13 | 630 | If we are reading this correctly, if we reasonably believe the presented evidence is not a forgery (4.3.4.1), there is no additional validation (i.e. authoritative/issuing sources) needed.<br><br>If so, this may weaken the assurance level from a security perspective, but it would also likely lower the barrier to entry for folks to complete identity proofing. | Clarify we are interpreting that passage correctly. |
| 5 | 63A | 4.3.4.4 | 13 | 630 | The other explanation is that this is a typo. It was supposed to reference 4.3.4.3 (currently references 4.3.4.1) | Correct the typo to reference 4.3.4.3 |
| 6 | 63A | 4.4.1 | 14 | 678 | This should be updated to a comparison to the facial portrait presented on the ISSUING/AUTHORITATIVE SOURCE of the identity evidence to the facial image of the applicant. If the comparison is just between the applicant and the photo on the identity evidence this will continue to be a control that can easily be defeated by fraudulent actors via photoshop while presenting an equity barrier to legitimate users. | Either specify the facial portrait comparison is to an issuing/authoritative source as opposed to the photo on the identity evidence, or remove this control completely. |
| 7 | 63A | 5.1.8 | 22 | 905 | Guidelines should call out what alternate controls can be in place when a biometric comparison fails. | |
| 8 | 63A | 5.4.2.1 | 28 | 1103 | There is no value in collecting FAIR evidence from the applicant. The lack of security features on FAIR evidence makes it impossible to detect a forgery from an authentic document. | Remove "collection" of FAIR evidence |
| 9 | | 5.4 | 28 | 1000 | Identity ASSURANCE should extend beyong a single point in time where Identity PROOFING occured. This would also provide more equity and access given controls can unduly create barriers for the historically vulnerable. For example, someone who doesn't have a reliable device that is flagged by anti-fraud device fingerprinting algorithms.<br><br>But rather than "failing" them at identity proofing, allow them to continue on to the RP, while continually assessing the risk score of that person. | |
| 10 | 63A | 5.1.9 | 24 | 959 | What is the appropriate bar for a Trusted referee and their ability to make a "risk based decision". Could help provide examples of trusted referee processes that exist since 2017. | Example of acceptable trusted referee systems. |
| 11 | 63B | 4.5 | 13 | Reauthe | Distinction between AAL2 reauthentication should be made between enterprise systems compared to direct to consumer.<br><br>From an equity and accessibility perspective, the requirement for direct to consumer applications to be 12 hours or 30 minutes of inactivity creates unnecessary burden.<br><br>A reasonable compromise would be allowing remembered devices for up to 15 days. | Allow for areauthentication of 15 days for IAL2 for public facing systems |
| 12 | | 5.31 | 49 | 1418 | Mention of considerations in this section doesn't call out the time or process needed to provide a pathway to adoption of xALs for users or agencies. Legacy access based on outdated assurance / verification protocols will need to be maintained for a period of time while change management plans are developed. This also should be reflected in the next section for compensating controls; there may not be compensating controls for a period of time | Clarify that guidance recommendations will take time to implement |
| 13 | 63-Base | Abstract | ii | 138-156 | Seeing identity guidelines highlighting both the risk of barriers to equity along with risk of fraud is encouraging as it balances trust and risk. Vulnerable populations are prone to being flagged as high risk (false positives) by anti-fraud controls, would request guidance on resources providers should look to on managing this balance. | Include resources / techniques:<br>- Risk scores / gradients rather than a pass/fail for identity assurance<br>- Quarantining / limited access |