| # | Organization/ Submitter Name | Type (General, Editorial, Technical) | Volume (-3, A, B, and C) | Section # | Line | Comment or Proposed Change |
|---|---|---|---|---|---|---|
| 1 | Deloitte | General | A | N/A | N/A | The difference in proofing requirements between IAL1 and IAL2 is substantial - which may result in challenges for agencies seeking to manage risks and cost for applications at moderate levels of threat. Looking at other guidance, the Canadian Standard on Identity and Credential Assurance include 4 levels. We recommend NIST explore the possibility of adding an intermediate assurance level (or redefine IAL1) to support more granular risk management that still aligns to a common profile. This may also support greater cross border interoperability. |
| 2 | Deloitte | General | A | 5.2.1 | Table 5-1 | For both strong and superior evidence, the document makes references to digital information being protected using approved cryptographic or proprietary methods. Within these references, we recommend NIST clarify what methods are considered acceptable for protecting this data, and to provide greater clarity on the use of the word proprietary - particularly when it is allowed as an alternative to approved cryptographic methods. |
| 3 | Deloitte | General | A | Multiple | N/A | Throughout the Special Publication, the term "authoritative" and "authoritativeness" are used, but the lack of clarity of this term may result in issues or confusion. For example, if a CSP is meant to support multiple agencies, and each agency has a different interpretation, it could damage interoperability at scale. We recommend additional text be provided in this section to for allow for more consistent understanding - perhaps a set of characteristics |
| 4 | Deloitte | Editorial | A | N/A | N/A | We recommend the removal of "weak" and "unacceptable" evidence characteristics, validation requirements, and verification requirements as they may cause confusion. Instead, we recommend including specific examples of "weak" and "unacceptable" document types that should not be used for identity proofing purposes. |
| 5 | Deloitte | Editorial | A | 4.3 | "A CSP that supports only IAL1 SHALL NOT validate and verify attributes" | We recommend the clarification of this broad statement, as it may restrict the use of external CSPs that validate and verify attributes for business purposes. For example, the validation of email addresses, phone numbers, and group affiliations could be conducted for legitimate business purposes at lower xALs. |
| 6 | Deloitte | Technical | A | 5.2.2 | Table 5-2 | The performance of validation systems are critical, as proofing now heavily relies on the ability to remotely confirm the authenticity of identity evidence. NIST providing concrete performance expectations, or further analysis of these validation systems, would be valuable. We also recommend NIST consider establishing - or working with industry to establish - a program (similar to their biometric testing programs) to provide a structured method for testing document validation systems. |
| 7 | Deloitte | Technical | B | 5.1.1.2 | "When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised." | After this statement in the Special Publication, it is followed by a list of what "may" be included on a prospective list - including "dictionary words" and "repetitive characters." If possible, please include a minimum set of required checks to enable a clear level of risk management when applying NIST's new memorized secret guidance. |
| 8 | Deloitte | Technical | A | 5.2.1 | "Applicant proves possession of an AAL2 authenticator, or equivalent, bound to an IAL2 identity, at a minimum." | This statement included in Table 5-1 under strong evidence characteristics may be misplaced. We recommend this to either be consolidated into a section on how digital credentials can be explicitly used as evidence in a derived process (perhaps adding to section 6), or in the Validation/Verification section of the document. |
| 9 | Deloitte | Technical | -3 | 4.4.2 | "The RP is the final arbiter concerning whether a specific assertion presented by a verifier meets the RP’s established criteria for system access regardless of IAL, AAL, or FAL." | NIST providing additional guidance of granular examples of how to implement the technical acceptance of an assertion of various risk levels would be helpful to provide further details this instance. |
| 10 | Deloitte | Technical | -3 | 5.5 | "Agencies SHOULD include this information in existing artifacts required to achieve a SA&A." | Agencies would likely appreciate insight on plans for revising current SA&A publications, standards, and documentation to align with an updated 800-63. Having the guidance show this as optional (using SHOULD instead of SHALL) may mean that agency systems risk management (SA&A) processes are out of sync with identity management specifics. |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| 11 | Deloitte | Technical | A | 4.2 | "The CSP SHOULD obtain additional confidence in identity proofing using fraud mitigation measures (e.g., inspecting geolocation, examining the device characteristics of the applicant, evaluating behavioral characteristics, checking vital statistic repositories such as the Death Master File [DMF], so long as any additional mitigations do not substitute for the mandatory requirements contained herein. In the event the CSP uses fraud mitigation measures, the CSP SHALL conduct a privacy risk assessment for these mitigation measures. Such assessments SHALL include any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography), and be documented per requirement 4.2(7) above." | NIST may wish to provide greater detail on how to leverage fraud mitigation capabilities specifically from financial institutions, as these institutions are often targeted and should have well-established mitigation techniques. These details could be expanded on specifically in Section 7.1. We would further recommend that guidance be provided on how to establish a risk scoring model that may incorporate some of these additional factors into decision making. This guidance could be informative material incorporated into the base document or a separate supporting document, potentially developed in collaboration with commercial partners. |
| 12 | Deloitte | Technical | C | 9.1 | N/A | We recommend that NIST provide further details for the Privacy Impact Assessments which outline specific courses of action that can be taken to achieve the predictability and manageability objectives, and that are commensurate with identified privacy risks. |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |