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:	*LexisNexis Risk Solutions, Inc.*
Name of Submitter/POC:	*Justin Hyde*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63A	2.2	4	412-415	While identity verification is not actually stated here, all three sentences describing / defining IAL1 are essentially inferring 'identity verification' as defined in lines 400-401 above.	The last sentence should read "All core attributes are validated against authoritative AND credible sources and steps are taken to link the attributes to the person undergoing the identity proofing process, resulting in indentity verification."
2	63A	2.2	4	417	The phrase "Stronger types of evidence" is not comprehensive enough	Expand the IAL2 definition to include "additional" types of evidence in order to combine more identity verification tools (ie two weak for one strong) to achieve IAL2. The sentence should read "IALS adds additional rigor to the identity proofing process by requiring the collections of stronger and/or additional types of evidence..."
3	63A	2.2	4	419	IAL3 should include language around a government representative as an alternative to a trained CSP representative to interact directly with the applicant	"IAL3 adds the requirement for a trained CSP representativeor designated government agency representative..."
4	63A	4	6	427	Typo	Replace "and" with "an" Typo - "This section provides an overview..."
5	63A	4	6	438	"organizations should enable optionality..." phrase is too loose, should be more stringent	"organizations must enable optionality..." - This change ensures true equitable access
6	63A	4	6	440	Section states that this "should" include accepting multiple types and combinations of identity evidence , supporting mutiple data validation sources, enabling multiple mentiods for verifying identity... however, the latter part is very prescriptive, not necessarily offering multiple options as stated in this section.	Include examples of "multiple types of and combinations of identity evidence" and examples of "multiple data validation sources." In addition, only the use of trusted referees is mentioned as an example of "multiple methods for verifying identity." Suggestion is to add another example, leaving this section less prescriptive and less dependent/focused on trusted referees.
7	63A	4.1.1	8	472-477	Evidence as described (driver's license or passport) should not be required to do a IAL1 workflow; see simiar comment for section 5.3.4. Subsequently, the removal of said evidence documentation would relieve the CSP of the onus to validate the authenticity, accuracy, currency of said presented evidence.	Remove drivers license and passport as evidence
8	63A	4.1.1	8	480-482	This prescriptive verification step does not accommodate the minimization of biometrics. Verification does not need to be only through comparison of a document photo to a selfie.	Suggest removing biometric requirement from the process OR revisit document references to the minimization of biometrics from the process. If a biometric component remains in the process, suggest adding an alternative/additional means of verification to be less prescriptive in approach to accommodate the desired level of identity assurance by each individual agency.
9	63A	4.2	9	490	We agree with data minimization, however with this section written as-is someone could resolve John Smith with DOB 1/1/1980 to any John Smith with DOB 1/1/1980 if only those two attributes were utilzed and the agency was using probablistic or deterministic matching. NIST should include language around accuracy of identity resolution.	"The goal of identity resolution is to use the smallest set of core attributes to uniquely and accurately distinguish an individual within a given population or context." Suggest NIST qualify the identity resolution goals by defining accurate identity resolution.
10	63A	4.2	9	490-494	Resolution to a synthetic identitiy can open a door for perpetrators of synthetic identity fraud.	Suggest adding language to address the detection of synthetic identities in this section.
11	63A	4.3	9	495	How is self-asserted evidence (as noted in line 413) handled with no supporting evidence? Possession of evidence should not be required in order to resolve, validate, and verify an identity. Most successful non-Federal agency use cases do not require the submission of the evidence prescribed by NIST to verify an identity.	We suggest that NIST includes a standard, particularly applicable to IAL1 for other ways to successfully, securily, and equitaby verify an identity rather than just using a document, image, compared to the applicants biometrics. Also of note: This section should also indicate the identity evidence should belong to the person supplying it.
12	63A	4.3	9	504-506	Evidence is highly focused on existing 'records' whether it be physical or digital. There are other pieces of evidence sufficient to resolve, validate, verify an identity.	Additional verification methods should include utilizing credible source-supplied linkage/association information between the idntity presented and the device envoking the transaction. Digital birth certificate credentials are another option. Additionally, knowledge-based verification, used in conjunction with data validation outcomes should be considered an option, particularly for IAL-1 workflows. KBV technology continues to evolve and is a widely accepted step-up verifcation tool utilzied across finanical service and goverpent programs
13	63A	4.3.1	10	513-525	There is not a way for a CSP to ever confirm whether identity proofing occurred prior to document issuance or that the document was delivered to the intended person. These are assumptions that have to be made by the CSP based on the guidelines and reputation of the issuer, it does not take fraudulent document creation or the use of synthetic identities into consideration. Also, this does not account for alterations or falsified versions of physical documentation.	Suggest adding language to Items 4 & 5 (line 522-525) that state the issuer of the document is presumed to have performed identity proofing prior to issuance. The onus of identity proofing prior to issuance is not with the CSP.
14	63A	4.3.2	10	526-541	Digital evidence seems to be a digital form of the tradtionally physical identity evidence documents; represented as a verifiable credential. Additionally, there is no required indicator that verifies the validity of digital documentation mentioned in this section, or of the use of synthetic identities, and requires the assumption that the credentialing agency/company/entity performed adequate validation prior to issuance. Similar to commentary for physical identity evidence, there are other pieces of evidence sufficient to resolve, validate, verify an identity.	Additional verification methods should include utilizing credible source-supplied linkage/association information between the idntity presented and the device envoking the transaction. Digital birth certificate credentials are another option. Additionally, knowledge-based verification, used in conjunction with data validation outcomes should be considered an option, particularly for IAL-1 workflows. KBV technology continues to evolve and is a widely accepted step-up verifcation tool utilzied across finanical service and goverpent programs.
15	63A	4.3.3.1	11	548-559	To be 'FAIR', still need to have gone through an identity proofing process	Suggest revisiting FAIR requirements and change from meet "all" requirements to meet "three of four."
16	63A	4.3.4.1	12	601-615	All requirements in this section still tie to the evidence being very limited to documents or verifiable credentials.	If progress is made to allow for other types of evidence, this section should inherently change accordingly. For example, consideration of mobile drivers licenses, digital birth certificates, or the use of a quiz to verify identity.
17	63A	4.3.4.2	13	617	How is self-asserted attribute collection governed if not collected from the prescribed sufficient evidence?	Suggest defining applicant self-assertion and providing an example of how this differs from prescribe sufficient evidence. See Comment #16 above.
18	63A	4.3.4.4		625-626	Needs to address synthetic identities and counterfeit documents.	Recommend additional validation as a further measure of protection from counterfit documentations and synthetic identities. See Comment #16 above.
19	63A	4.4.1	14	659	The identity verification methods prescribed are high-friction and rely on biometric capture for remote identity proofing. There are other ways to verify the 'linkage of the claimed identity to the applicant engaged in the identity proofing process.	Additional verification methods should include utilizing credible source-supplied linkage/association information between the idntity presented and the device envoking the transaction. Digital birth certificate credentials are another option. Additionally, knowledge-based verification, used in conjunction with data validation outcomes should be considered an option, particularly for IAL-1 workflows. KBV technology continues to evolve and is a widely accepted step-up verifcation tool utilzied across finanical service and goverpent programs.
20	63A	5.1.1	16	706	This references 5.1.9 for alternative means to verify an identity, but none are stated in 5.1.9 and rely heavily on trusted referee assistance.	Suggest NIST considers alternative identity verification processes that will be inclusive of more individuals; allowing for more automation and less reliance on the inherently subjective trusted referee decisioning. This reduces friction for the applicant and allows for more equitable access. Also suggest removing "if applicable."
21	63A	5.1.1	16	708	Core attributes shouldn't be determined by the CSP	Suggest a required minimum set of core attributes to ensure equal consideration regardless of CSP's strengths or attributes of focus
22	63A	5.1.1	17	723	Typo - there should either be no "and" without another line item	Remove "and"

23	63A	5.1.1.2	17	733	Examining device characteristics has been proven in not only fraud mitigation, but also in frictionless positive verification.	Suggest removing SHOULD and replacing with SHALL
24	63A	5.1.2.1	17	746-771	There is no mention of documenting or safeguarding the transmission of PII when CSPs receive/send information	If this is covered in other NIST documents, we suggest adding a reference to said publications
25	63A	5.1.4	20	825	There are CSP's that require users to 'OPT OUT' of other services when engaging their commercially-based federated platform. This is worrysome when it comes to public trust when transacting with Government agencies.	NIST should mandate that any commercial third party full service CSP provider shall not utilize any of the collected PII data for purposes other than identity verification.
26	63A	5.1.7	22	895	In our experience, credible referential/corroborative data provides the most accurate up to date address of individuals. Also, when does the notification occur? What happens if there is an account takeover after validation/verification? What address is used?	NIST should define best practice approaches when verifying or validating an address when tying it to the true owner of the identity.
27	63A	5.1.8	22	905-958	There is no clause about whether someone can opt out of biometrics, what can be substituted, what happens to the application if someone opts out.	Suggest adding language regarding whether an applicant can opt out of biometrics and include alternatives. Alternatives should not be trusted referee.
28	63A	5.1.9	24	963-972	Individuals and demographics groups included in the document are limited	Suggest stating it is not limited to the list of examples included in the guidelines.
29	63A	5.1.9	24	959-992	How will trusted referees make objective decisions meeting the assurance levels without the proper evidence that is prescribed in Section 4?	Suggest adding language that includes proper evidence that is referenced in Section 4.
30	63A	5.1.9.1	24	994-995	Is the use of trusted referee for IAL1 needed?	Based on all preceding comments regarding the differentiation of IAL1 from IAL2, the challenges with trusted referees vs automation, we do not believe trusted referees should be a primary option for IAL1. While trusted referees create efficiencies for the government agency, they do so at the expense of the applicant - the applicant is forced to spend more time in the process and, when considered a special circumstance that is referred to a trusted referee, it can leave the applicant with the impression he or she has been singled out.
31	63A	5.1.9.1	25	999-1000	If trusted referees are an option for identity proofing, NIST must ensure that the applicant is protected on all fronts as they would be for a fully automated remote transaction. Training can be subjective and insufficient training can cause errors and additional friction. Additinally there are significant risks particulaly with supervised remote transactions wherby there is little abitiy to protect the leakage of sensitive data that an applicant is required to provide, leading to identity embezzlement.	Suggest adding specific training requirements to this section in order to ensure that trusted referrees meet the highest standard of integrity, as well as objective and secure decisioning; reducing potential errors and additional friction for applicants.
32	63A	5.3.2.1	26	055-105	The IAL1 requirements are similar to IAL2 listed in 5.4.2.1, lines 1105-1106.	As written throughout the document, there should be greater differentation between the two levels, along with different approaches. The IAL1 process, by design, should be less rigorous than IAL2. Further, IAL1 should remove some of the verification-associated friction found in IAL2 (such as trusted referee) and replace with a less stringent process. See our comment 19.
33	63A	5.3.4	27	078-108	In this section's opening paragraph, NIST states that the use of biometric matching is optional, however 5.3.4 seems to effectively make it a requirement to verify one's identity who doesn't currently have an established digital account or receives a valid enrollment code; the enrollment code being the only alternative identity verification from IAL2. There are proven ways to do an automated, strong, secure identity verification for net-new clients without requiring the biometric. As NIST has stated, alternatives to biometrics is important in this revision. As written, this seems much too strict and complicated for IAL1. Biometrics are one option but without them, an applicant is left with only an AAL process OR a one-time passcode. If the applicant does not have a drivers license/passport or text capabilities, that leaves very few options for IAL1, which seems prohibitively difficult.	We suggest that NIST includes a standard, particularly applicable to IAL1 for other ways to successfully, securily, and equitaby verify an identity rather than relying on a document, image, compared to the applicants biometrics. Suggest loosening the requirements or creating alternative options to accommodate for applicants with technology challenges. In its current state, this section can generate potential issues with equitable access. We recommended the use of a quiz, or KBA/KYC approach to decrease dependence on more restrictive requirements for IAL1. There have been significant improvements with quiz technology use in conjunction with other verification points. The totality of the transaction should account for the overall success of IAL1, not its individual components.
34	63A	7	34	1296	This section should be normative. Since this section "...focuses on impersonation and false or fraudulent representation threats..." which is a very important component to all levels of assurance, having this section entirely informaitve leaves agencies with little direction in a very important area.	Suggest this section be fleshed out in order to identify proper/tested threat mitigation strategies (that may differ from the reference sections) and make them normative. An ageny must have some type of threat mitigation strategy. The challenge with a prescriptive standard is that fraudsters then know the defense plan and can easily adapt. We suggest the requirment of a strategy, but leave it up to the agency to build the defenses to fulfill the requirments.
35	63A	7.1	38	Table 3	The Mitigation Strategies listed for Synthetic Identity Fraud would not necessarily detect/prevent this type of fraud - this approach may simply validate and verify the synthetic identity. A proper synthetic identity should be easlily passable by the prescribed proofing processes set forth as they are created and goomed by the fraudsters.	To mitigate synthetic identity fraud, assessing digital/device attributes and behavior will be very important, thus we recommend NIST make it required as stated in our comments for section 5.1.1.2 Social engineering is a huge risk when it comes to human interatction. The mitigation to social engineering is to ensure more accomodating robust automated processes with less focus on 'trusted referees' because someone had difficulties presenting/proving the identity verifiaction evidence prescribed in this draft.
36	63A	7.1	38	Table 3	The 'Fraudulent Use of Identity' mitigation strategies may be overly comprehensive in its current state.	Suggest adding ORs or some other means of explaining, otherwise IAL1 appears to be too exhaustive.
37	63A	9	44	483-148	This section needs better definition and clarification of what comprises a usability evaluation.	If a usability evaluation is going to be referenced here, this section should contain an example of what that evaluation should measure and what success looks like. It is also referenced on p. 45 lines 1530-1531.
38	63A	10	51	703-172	The section Equity Considerations relies heavily on the use of a trusted referee - this could present friction for some applicants due to the sensitive nature of the considerations themselves. For example, requiring a trans individual to work with a trusted referee causes additional friction because of technology limitations and potential social stigma due to the singling out of certain individuals. A non-English speaker or an individual who is not able to use technology would also be singled out for perceived additional scrutiny.	Suggest a re-working of this and other sections as noted to allow for social considerations.
39	63A	10.3	53	1778	NIST states that identity verification most often involved collecting a picture... and comparing it to a photogrpah contained on a validated piece of identity evidence. That said, NIST agrees that there are other ways to resolve, validate, and verify identities and thier attributes, but focuses only on the document capture and picture comparison for verification purposes in this document.	We suggest that NIST includes a standard, particularly applicable to IAL1 for other ways to successfully, securily, and equitaby verify an identity rather than just using a document, image, compared to the applicants biometrics. For example, use KBV in place of documentation or biometrics for IAL1.