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

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

Organization:	***Transunion and Neustar (a Transunion company)***
Name of Submitter/POC:	*Stuart Levy, Vice President, Public Sector Identity*
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	Note to Reviewers	iii	175	If identity binding to photo ID via Selfie Match is to be replaced by other strategies at IAL 2 going forward, NIST could publish a quantifiable scoring system within the identity proofing process incorporating values to allow for value-based replacements for elements such as Selfie Match. Rationale: 1. We believe that the innovative strengths of the solutions marketplace would be unleashed with more freedom to combine technologies/practices to deliver the intended outcomes of all proofing and authentication levels. A well-constructed valuation methodology would empower the development of a robust marketplace of solution options to meet the identity assurance goals of the rule. 2. In order to offer alternatives to the use of biometrics at the highest levels of proofing and authentication, the market needs a means of quantifying the value they currently bring to a model. With a methodology clearly communicated within guidance, solutions can be assembled to offset the value only biometrics could deliver under prior rule releases. 3. Improving equity and accessibility requires solutions to be extended to meet the capabilities available to lesser served populations. With a methodology that offers room for solutions providers to assert new evidence/approaches (and to propose what values they should hold) we can collectively broaden support to wider demographics across more channels. 4. Specific risk-based value categories can be created to allow for multi-vendor support such as: a) Device fingerprint risk; b) Device Reputation risk; c) Real-time user behavior risk; d) identity attribute risks; e) identity resolution risks; f) Photo ID risks; g) KBV risks	
2	63-Base	Note to Reviewers	iii	187	NIST asks, "Are there existing fraud checks (e.g., date of death) or fraud prevention techniques (e.g., device fingerprinting) that should be incorporated as baseline normative requirements? If so, at what assurance levels could these be applied?" SP800-63 has always been more of a binary identity check. We believe that fraud checks should not be normative requirements, and should instead be considered as risk mitigations. This is because industry provides risk insights differently across vendors, making specificity difficult to document within guidance (except at the highest level – see (3) above). Also, as technology changes, prior fraud checks may be replaced with new ones making conformance difficult on CSP's going forward. That being said, guidance that references known and accepted high level fraud checks (see (3) above) can be referenced	
3	63-Base	Note to Reviewers	iii	206	NIST asks, "How might risk analytics and fraud mitigation techniques be integrated into the selection of different identity assurance levels? How can we qualify or quantify their ability to mitigate overall identity risk?" The required use of risk-based controls (but not normative/specific requirements) to allow for KBV's at IAL1 and the non-selfie matched Photo ID at IAL2. This would allow CSPs to document and employ risk mitigations that match their preferences across a range. We encourage NIST to create room within the 800-63-4 for CSPs and solution providers to assess all risks with the goal of minimizing the need for individuals to be proofed with a facial comparison. IAL1 evidence, combined with a lack of risk-based telemetry, should allow for transactions that previously required IAL2 proofing to be performed with expanded options. Not only would this adjustment allow for individuals to opt-out of biometric technologies, it would also support broader capabilities aimed at addressing equity and accessibility	
4	63-Base	Note to Reviewers	iv	230	NIST asks, "Is there an element of this guidance that you think is missing or could be expanded?" 1. As digital channel access controls have improved, impersonation attack risks have shifted to call centers. 63-4 should therefore provide guidance for Agencies and CSP's to protect telephony or the audio channel with the definition of "omnichannel authentication". 2. STIR/SHAKEN is a caller ID authentication methodology designed for this purpose and will protect against Spoofed Calls (fraud) and Robocalls (waste & abuse). This service is provided by telephone carriers and is analogous to digital channel encryption. 3. This recommendation is also supportive of equity as not all users are able to use the digital or in-person channels.	
5	63-Base	2.3.3	8	554	**If Trusted Referees can support users in a Remote Supervised fashion within a call center, proofing would require security protections analogous to encryption within the digital channel. 63B-4 makes multiple references to encryption that shall be implemented to protect the digital channel. Therefore, we recommend the inclusion of Secure Telephone Identity Revisited (STIR), sometimes referred to as STIR/SHAKEN, to protect the audio channel and therefore securing relying party trust. There is also the potential to use STIR for IAL's. The STIR capability is supported by the FCC here: https://www.fcc.gov/call-authentication** **Rationale:** **1. As digital channel access controls have improved, impersonation attack risks have shifted to call centers. 63-4 should therefore provide guidance for Agencies and CSP's to protect telephony or the audio channel with the definition of "omnichannel authentication".** **2. STIR/SHAKEN is a caller ID authentication methodology designed for this purpose and will protect against Spoofed Calls (fraud) and Robocalls (waste & abuse). This service is provided by telephone carriers and is analogous to digital channel encryption.** **3. This recommendation is also supportive of equity as not all users are able to use the digital or in-person channels.**	

6	63-Base	2.3.3. Equity	8	554	Rationale: Providing equitable accessibility to programs for all populations requires 800-63-4 to have the ability to welcome the use of “Pay-as-you-go” mobile phones. Comment: NIST is looking for pathways to better extend access to important programs/systems for populations that have been historically underserved by identity proofing/auth solutions. Certain demographics leverage pay-as-you-go mobile phones for a variety of legitimate reasons. We believe those devices should be more welcome within omni-channel identity services and therefore encourage NIST to make accommodations for them in the next draft via specific reference. This simple update would provide support to CSPs in the use of such devices which is supportive of equity and	
7	63A	10.4	54	1818	**Comment: If Remote Supervised is acceptable across assurance levels using Trusted Referees and potentially involving Vouching Parties, then non-digital guidance should be provided within 63A and 63B.** **Rationale:** **1. Call center-based proofing using Trusted Referee in a Remote Supervised format is technically feasible using hybrid digital/audio technologies.** **2. This channel is required to support large populations in an equitable manner as desired by CSPs for the benefit of the customer facing federal agencies including SSA, IRS, VA, CMS and users** **3. Equity and inclusion is promoted in a cost efficient manner by supporting the telephony channel.** **4. The use of call center-based proofing will allow for the use of an agent/Trusted Referee at non-IAL3 assurance levels.**	
8	63A	5.1.9.1	24	993	Rational - Question regarding Trusted Referees With the expansion of the role Trusted Referees will play in 800-63-4, can you please add specifics regarding their ability to make “risk-based decisions”. Is it the intent of NIST to allow individuals to make risk-based decisions by relying on published CSP policies? Or, are risk-based decisions purely made by systems/software? What ability can/should the referees have to override or make individual decisions. This is especially important in the areas of advancing equity and accessibility as the requirement for unique actions will be dramatically increased. In order to cater to the diverse needs of specific (perhaps traditionally under-served) populations, Trusted Referees should be well empowered to make decisions. Please offer guidance within the next draft regarding this aspect of the rule.	
9	63A	5.3	26	1035	Given sensitivities regarding the use of biometric comparisons, NIST could simply adjust the definition of Strong evidence to exclude the requirement for identity binding to a photo ID when risk-based controls are present thereby allowing for a more equitable IAL 2 with fewer failures. Increase support for the use of knowledge-based questions at IAL 1 when risk-based controls are present including required velocity controls to prevent scaled attacks. Reserve Selfie Match-based identity binding as required for Superior at IAL 3. Adjust impact assessment and assurance level selection to incorporate use cases that are applicable: i.e. IAL 1 = CSP interactions supporting government benefits or call center-based interactions (see (1) above); IAL 2 = CSP interactions involving the release of digital data such as tax or health information	NIST clearly is looking to allow for more business to be conducted without the need of the biometric elements prevalent in IAL2 proofing. Our goal here is to encourage NIST to create room within the 800-63-4 for CSPs and solution providers to assess all risks with the goal of minimizing the need for individuals to be proofed with a facial comparison. IAL1 evidence, combined with a lack of risk-based telemetry, should allow for transactions that previously required IAL2 proofing to be performed with expanded options. Not only would this adjustment allow for individuals to opt-out of biometric technologies, it would also support broader capabilities aimed at addressing equity and accessibility.
10	63A	Note to Reviewers	iii	182	Mobile Driver License (mDL) ISO standards appear to be on its own development path. The underlying identity verification approach for mDL credential provisioning is the REAL ID Act of 2005. However, synthetic fraud risks are still realized (https://www.justice.gov/usao-md/pr/former-maryland-motor-vehicle-employee-facing-federal-indictment-illegal-production) at the DMV level. Therefore, guidance should be referenced within SP800-63 to employ real-time identity verification standards when using mDL as a digital credential. References to the use of real-time identity resolution and risk mitigation methods including synthetic and identity fraud checks, plus the use of device-based fraud checks, would appear to be appropriate.	
11	63B	4.2.2	9	532	**If Trusted Referees can support users in a Remote Supervised fashion within a call center, proofing would require security protections analogous to encryption within the digital channel. 63B-4 makes multiple references to encryption that shall be implemented to protect the digital channel. Therefore, we recommend the inclusion of Secure Telephone Identity Revisited (STIR), sometimes referred to as STIR/SHAKEN, to protect the audio channel and therefore securing relying party trust. There is also the potential to use STIR for IAL’s. The STIR capability is supported by the FCC here: https://www.fcc.gov/call-authentication** **Rationale:** **1. As digital channel access controls have improved, impersonation attack risks have shifted to call centers. 63-4 should therefore provide guidance for Agencies and CSP’s to protect telephony or the audio channel with the definition of “omnichannel authentication”.** **2. STIR/SHAKEN is a caller ID authentication methodology designed for this purpose and will protect against Spoofed Calls (fraud) and Robocalls (waste & abuse). This service is provided by telephone carriers and is analogous to digital channel encryption.**	
12	63A				**Increase equity and access across diverse populations by clarifying and expanding Remote Supervised for use at IAL 1 and IAL 2 vs specifically referencing at only IAL 3.** **Rationale:** **1. The 63-4 draft only references Supervised Remote at IAL 3 as an in-person experience is expected, though references to the use of a Trusted Referee is included within other assurance levels.** **2. Since the use of a Trusted Referee can be remote or in-person, clarification that Supervised Remote is acceptable at IAL1 and IAL2 is advised as a means to expand equity and access to underserved populations, and challenging cases**	