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:	*Invitae Corporation*
Name of Submitter/POC:	*Deven McGraw, Lead Data Stewardship and Data Sharing*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
	63-Base	Risk Mgmt, Genera	iii-iv	206-208	We are pleased that this draft v. 4 of 800-63-4 elevates equity as a key consideration in establishing assurance levels, but in our experience of several years at remote identity proofing of individuals to facilitate their access to electronic medical records, we are confident more needs to be done to address the limitations that current requirements have for underserved populations. This is particularly the case for remote ID proofing, where the option in this draft for underserved populations seems to be to default to an in-person, assisted "trusted referee" process, but without adequate consideration of the lack of widespread, well understood, easily accessible, and affordable ways to access in-person proofing or the burden in-person proofing can place on individuals. For example, by allowing the Relying Party (RP) complete discretion to determine the assurance levels and acceptable ID proofing processes, it guarantees the bar will be set high, as RPs are more likely to value minimization of risks w/r/t to potential for breach/data exposure or fraud higher than the impact on accessibility by hard-to-reach populations. This tendency is exacerbated by some ID proofing vendors seeking to sell particular solutions that primarily address fraud and security needs, with less consideration of impacts to equity and burden on individuals. To truly advance equity would be to incorporate into remote ID proofing requirements, with a greater degree of specificity than is currently in the guidance, more flexibility into what is required to meet assurance levels (for example, not just flexibility as to biometrics but also flexibility on types of identification required to be submitted to meet particular assurance levels); require RPs to place equity on an equivalent plane to privacy and security in setting assurance levels; working with other agencies to assure RPs are not penalized for setting assurance levels/ID proofing requirements that prioritize equity but may introduce more risk; and requiring that assisted, in-person options to be readily available (easy for underserved populations to find, adopt, and afford) before they are permitted to be utilized in lieu of remote proofing.	To truly advance equity would be to incorporate more flexibility into what is required to meet assurance levels (not just flexibility as to biometrics but also flexibility on types of identification required to be submitted to meet particular assurance levels); require RPs to place equity on an equivalent plane to privacy and security in setting assurance levels; working with other agencies to assure RPs are not penalized for setting assurance levels/ID proofing requirements that prioritize equity but may introduce more risk; and requiring that assisted, in-person options to be readily available (easy for underserved populations to find, adopt, and afford) before they are permitted to be utilized in lieu of remote proofing.
	63-Base	General (questions	iv	230	Unless we missed something in the documents, it does not appear that NIST re-assessed or revised the different types of evidence, and what combination of superior, strong, and fair need to be presented for each assurance level — and we think this is unfortunate. The penetration of REAL IDs in the U.S. is still lower than it should be due in part to COVID-19 extensions of deadlines and natural expiration cycles of driver's licenses. This requires individuals with driver's licenses to potentially have to submit even more evidence, which enhances privacy risks and is more burdensome — and these requirements are likely to be most burdensome for underserved, hard-to-reach populations. In addition, the AAMVA process for checking driver's licenses is not permitted in at least 15 states. The only adjustment that appeared to have been made was to ease the biometric requirements for LoA 1 - which is helpful, but not sufficient. We believe accommodating the needs of underserved populations requires a reassessment and recalibration of the framework for identity documents and the combinations required to meet levels of assurance, or some greater flexibility on the part of RPs seeking to adopt credentialing processes that provide greater accommodations for remote ID proofing of underserved populations.	We believe accommodating the needs of underserved populations requires a reassessment and recalibration of the framework for identity documents and the combinations required to meet levels of assurance, or some greater flexibility on the part of RPs seeking to adopt credentialing processes that provide greater accommodations for remote ID proofing of underserved populations.
	63-Base	5.3.2	37	1421	Consistent with our comments above, and our concerns that the guidance doesn't sufficiently address the remote ID proofing needs of underserved populations, we are pleased to see that this guidance allows for "compensating controls." However, it would be more helpful if the guidance could expand on how these could be effectively implemented (such as with a range of specific examples). In addition, compensating controls should preceed a shifting in tailored assurance level if properly implemented.	The guidance should expand on (such as through examples) how compensating controls can be deployed to address equity and other lack of access/individual burden issues.
	63-Base	5.3.3.	38	1449	Same comments as above w/r/t supplemental controls.	See comments above - same for supplemental controls.
	63-Base	5.4	39	1476	We agree that risk assessments and identify solutions need to be flexible and able to adapt with additional evidence and changing circumstances. With the rapid development of technology and continual change in the collective view of privacy calculations, stagnant policies quickly become antiquities. Frequent and continuous solicitation of feedback from patients, patient advocates, providers, technology companies, and other interested stakeholders should be a goal to maintain the contemporary value of additional guidance.	None
	63A	4	6	437-444	As noted above in comments to the base document, we agree with the need for flexibility in implementing this guidance, which is further supported by this text. However, it is unclear how RPs can successfully implement this flexibility, and the usability and efficacy of the guidance would be greatly enhanced by a broad array of examples.	Provide more examples of how RPs can implement the flexibility recommend in this guidance.
	63A	4.1.1	8	464	We appreciate this illustration of the basic credentialing flow. We urge NIST to offer additional examples (along with diagrams) to illustrate ways that RPs can deploy flexibility, as well as supplemental and/or compensating controls, to assure that underserved individuals can take advantage of remote identity proofing options across different assurance levels.	The guidance should offer additional examples (along with diagrams) to illustrate ways that RPs can deploy flexibility, as well as supplemental and/or compensating controls, to assure that underserved individuals can take advantage of remote identity proofing options across different assurance levels.
	63A	4.1.1	8	467-488	This diagram assumes a situation where an individual seeks out and "hires" a CSP in order to gain further access to information or services. This guidance also needs to accommodate situations where an individual doesn't choose the CSP but instead the CSP is chosen by an agency or a vendor (for example, if an individual is using an app or a platform as a mechanism to connect to information or services, and that vendor/app hires a CSP to conduct ID proofing). This guidance needs to address the division of roles and responsibilities in circumstances where the CSP is a vendor to another entity (which could be a government agency or a vendor hired by the individual or government) that enables the individual access to information or services.	We urge NIST to revise this guidance to clarify roles and responsibilities of CSPs and other entities when the CSP is not "hired"/chosen by the individual.

	63A	4.3.3	10-12	542+, 56	Please see comment above (row 10) regarding the burdens imposed on individuals by the current classifications of ID documentation. While the Real ID requirement takes effect May 7, 2025, there exists currently — and will likely persist — the lack of universal Real IDs, which is an issue that is not adequately addressed by the distinction in this guidance. An additional barrier would be the lack of universal adoption of the American Association of Motor Vehicle Administrators (AAMVA) identify proofing policies. We believe this section needs further consideration in order to address burden to individuals imposed by requiring the submission of additional proof points when an individual is attempting to ID proof with an unexpired (but not REAL) driver's license, even when that licensed is matched by the CSP to the individual through biometrics. At a minimum, the guidance should illustrate how RPs can deploy flexibility in considering these pieces of evidence, and how that flexibility impacts assurance levels.	The guidance should include information on ID proofing individuals who may not possess a REAL ID, but otherwise can meet ID proofing needs without the need to submit other confidential information that raises privacy risks. This guidance, at a minimum, should illustrate how RPs can deploy flexibility in considering these pieces of evidence, and how that flexibility impacts assurance levels.
	63A	5.1.2.2	18	782-788	Per our comment above (row 16), this section presumes a model where the individual directly hires/engages a CSP, vs. situations where the individual is interfacing with a CSP hired by an app or platform (or even a government agency), where the CSP provides a credentialing service (on behalf of the app, platform or government agency) but does not directly engage with the individual.	See suggested change regarding lines 467-488 of 63A document above (row 16).
	63A	5.1.7	22	888-904	See comments above (row 16) regarding the need for the guidance to accommodate circumstances where the CSP does not have a direct relationship with the individual but is a vendor to an agency or a private business (app or platform, for example) hired by the individual to access government information or services), and where the vendor or private business is the one with the relationship with the individual.	See suggested change regarding lines 467-488 of 63A document above (row 16).
	63A	5.1.9	24	959+	Trusted referees should be treated as only one option of increasing access to remote ID proofing for individuals, and should not be considered the sole answer to the access, burden, and equity issues described in the guidance. It's not clear how widely available and actually trusted these "trusted referees" are, particularly to underserved populations. This guidance should focus on enabling remote ID proofing experiences for individuals across a broad spectrum of the population, and for underserved and/or disadvantaged populations in particular.	We urge NIST to consider strengthening and focusing this guidance on remote ID proofing experiences for individuals across a broad spectrum of the population, with particular focus on underserved and/or disadvantaged populations.
	63A	5.1.9	24	979	Applicant references can serve as a mechanism for verifying the individual; however, it is not clear who would qualify as a reference. In theory, this person would also need to be identify proofed to ensure that they are a reliable reference; for underserved populations, the references known to the individual may face some of the same challenges to being ID proofed. We recognize applicant references would be required as part the ID proofing of children and ask for clarity of the scope of the AR's role. For purposes of advancing equity, the guidance would greatly benefit from increased information on how applicant references could work, and some further study on whether or not they increase access by underserved populations or serve to further deepen access disparities.	With respect to Applicant References, we request clarification on who they could be, the scope of their role, how they would function, and their impact on health inequities.
	63A	5.3	26	1035	We appreciate the efforts to create an assurance level — new IAL1 — that is intended to reduce the burden on individuals by removing the requirement for biometrics. Essentially, IAL1 and IAL2 now look equivalent, with the sole exception of the biometric requirements in IAL1. The new IAL0 category is now the category with few — if any — ID proofing requirements (comparable to level 1 in version 3). Because individuals needing to be remote identity proofed struggle with more than just biometrics, the lack of intermediate assurance options between 1 and 2 is problematic. NIST should consider intermediate levels of assurance, or provide greater guidance on how RPs can use flexibility, as well as compensating and supplemental controls, to draft an ID proofing process consistent with the risk level but that also does more to reduce the burden on individuals.	The guidance should outline intermediate levels of assurance between IAL1 and IAL2, or we request that NIST provide greater guidance on how RPs can use flexibility, compensating controls, and supplemental controls appropriate for the risk level.
	63A	5.3.2.1	26	1052	See comments above (row 10) expressing concern about the impact on equity of lack of changes to the categorization of superior, strong, & fair evidence, and the thresholds needed for particular assurance levels.	Please see suggested change relating to line 230 of the 63-Base document (row 10).
			26	1058-10	We appreciate that the guidance has left room for the submission of self-asserted attributes — but it is unlikely CSPs will feel empowered to take advantage of this flexibility without further guidance and/or examples on how this could be deployed at different levels of assurance and consistent with real or perceived legal obligations.	The guidance should include examples and further information on how CSPs can use the flexibility at different assurance levels.
	63A	5.4.3	28	1111	The guidance would benefit significantly from further information on how RPs are expected to validate core (or even self-asserted) attributes at the different levels of assurance.	This guidance should include additional information on how RPs are expected to validate core or self-asserted attributes at different levels of assurance.
	63A	5.5.7	31	1198	We appreciate that some individuals will need — or even want — an in-person ID proofing experience. However, the choice between in-person, supervised interaction, and a remote interaction serves as a huge barrier for patients/users who can neither be in-person nor access high quality real time video capabilities. We fear this is in conflict with the goals of the guidance to enable access and equity.	Within the process/experience of ID proofing, we urge NIST to consider the equity implications of requiring interactions that may necessitate travel, the procurement of high quality technology, or other expenditures that are prohibitive for many persons.
	63A	5.5.8	31	1209	Usability is a factor that contributes to access and equity, but usability is not taken into account when it comes to the requirements for IAL3 Supervised Remote Identity Proofing. The current process does not address some of the barriers to usability inherent within the tips outlined in this section.	We urge NIST to consider, account for, and address the barriers to usability within the tips outlined in the section on IAL3 Supervised Remote Identity Proofing.
	63A	6.1	34	1243	Consistent with our comments above (see row 16), in some models of credentialing, it will be the CSP who assigns unique identifiers to each subscriber account, but this does not address the roles of CSP if the entity interacting directly with the individual and facilitating the individual's access to government information or services is not the CSP.	We appreciate the efforts to create an assurance level — that is intended to reduce the burden on individuals by removing the requirement for biometrics. Essentially, IAL1 and IAL2 now look equivalent, with the sole exception of the biometric requirements in IAL1. The new IAL0 category is now the category with few — if any — ID proofing requirements (comparable to level 1 in version 3). Because individuals needing to be remote identity proofed struggle with more than just biometrics, the lack of intermediate assurance options between 1 and 2 is problematic. NIST should consider intermediate levels of assurance, or provide greater guidance on how RPs can use flexibility, as well as compensating and supplemental controls, to draft an ID proofing process consistent with the risk level but that also does more to reduce the burden on individuals.