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:	Kantara Initiative, Inc.
Name of Submitter/POC:	Identity Assurance Work Group
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
Kantara-1	63-Base	General Comment	0	0	In support of NIST's desire to increase one-time and ongoing device risk assessment and trust, 800-63-4 should specifically call for demonstrated techniques/technologies that are being leveraged with all devices that are involved in a proofing or authentication workflow. Device risk should include device reputation.	Assess Real-Time Device Risk on all inbound channels regardless of modality. For Identity Proofing, CSPs should be able to assess the riskiness of all devices invoked by individuals during entire process. Individuals may interact with the CSP through a series of channels/devices during the proofing process including personal computers, tablets, mobile devices and even phone calls with a call center representative. 800-63-4 should include requirements for CSPs to demonstrate their ability to assess risk with regard to all of these devices at proofing time… and on a regular basis thereafter as the individual returns to authenticate themselves and via normal business transactions to ensure the identity continues to operate within reasonable risk thresholds. For Authentication, CSPs should be required to have one-time and ongoing risk assessment capabilities in place specific to the devices that hold authenticators. When an authenticator is aligned with a proofed identity, the CSP must be able to demonstrate their ability to re-assess risk whenever the authenticator is presented at a minimum. For adding new Authenticators or changing identity attributes, CSPs should be able to demonstrate their ability to assess the risk of any device used during the request and provision of new authenticators acter the proofing event has been completed. The new authenticator should adhere to the requirements above in that they are able to assess the device and device reputation risk every time the individual presents it for authentication. Ongoing use of Authoritative Attribute Providers should also be specifical required for CSPs to have in place regarding their proofed identities as a means mitigating risk long-term. CSPs should be able to demonstrate a dynamic ability to leverage their relationship with the authoritative sources they leveraged during identity proofing to be alerted to changes that may indicate an identity may no longer be trustworthy.
Kantara-2	63-Base	General Comment	0	0	Fraud mitigation must be an omnichannel approach in order to be effective. 800-63-4 should reference and leverage the FCC's requirement for phone networks to have implemented the STIR/SHAKEN Standard and a corresponding mitigation plan.	STIR/SHAKEN is required as a means of restoring trust to the phone systems we all depend on to ensure people can "trust" incoming calls with specific reference to illegal robo-calling. Caller IDs are "signed" as legitimate by originating carriers under the standard. This activity will offer important new means of risk assessment and trust when phone channels are involved in identity specific solutions. We believe NIST should specifically reference STIR/SHAKEN as an important part of assessing risk/improving assurance during both proofing and authentication events. Innovators will be able to innovate around this capability by introducing STIR/SHAKEN, and derived solutions, into their proofing and authentication approaches. Further, solutions will be offered that will create new levels of value from the baseline requirements of STIR/SHAKEN in the form of "Complementary Solutions".
Kantara-3	63-Base	Whole doc / set	0	0	Language is causing market confusion. To the providers it is confusing if it is guidance or a requirement. All volumes of this text are presented in contradictory ways ("These guidelines provide technical requirements ...") and in §1 ("This publication [provides] technical guidelines ...", "This document provides requirements ..."). The terminology is inconsistent. Requirements define something that one has to do, whereas guidance is purely informational, to be taken or ignored at will and without consequence. It is noted that the main body of the work contains a mix of informative material and presumably normative material which uses the specific capitalized key words 'SHALL', 'SHOULD' and 'MAY' in a very specific style of presentation. The intent of which is assumed to take on the meanings imparted to these words by RFC 2119, a practice widely adopted amongst SDOs (see also ISO Directives Part 2 App.H). This dichotomy should be resolved.	Determine if these are requirements or guidelines and make the necessary changes to each volume to reflect this change to state clearly that the document defines [normative] requirements [using key words as defined in RFC 2119] whilst providing supporting, explanatory and informative guidance. Implicit in this suggested change is that all references throughout the document to 'guidance' need to be reviewed to determine whether they are truly informative as opposed to being actual normative requirements.
Kantara-4	63-Base	Whole doc / set	0	0	The structure of the document does not lend itself to easy determination of: a) which clauses are actually expressing normative requirements; and b) what are discrete normative requirements. This is evidenced by no consistency in style regarding whether informative discussion precedes normative requirements and by single paragraphs which bear both normative and informative text. This weakens the utility of the document [set] in either its use as an educational/informative source or as a set of formal requirements.	1 - Express each normative requirement as a distinct clause; 2 - Give each such clause a unique reference; 3 - Give the user a very clear means to determine the status of a passage of text - i.e. exclusively normative or informative. It is noted that adopting a presentational distinction would be an easier solution to achieving much greater presentational clarity than trying to extract and regroup all passages of one type or another.
Kantara-5	63-Base	Note to Reviewers	ii	139-144	Advancing equity is a fantastic goal, but practically speaking, how will this mandate be implemented? Will gathering demographics be required during identity proofing? If so, what will be the required set? Rural (where broadband and cell service may be inadequate) vs city, race/national origin/ethnicity (which ones?), income (which income bands should be grouped together?), sex, disability (receiving disability payments?, has a specific disabilities, if so which ones?), English fluency?, technology the users have access to? which technologies? (scanners, mobile phone with a camera, webcams, printers, etc.), what about proficiency with technology? (having the tech is necessary but insufficient). For maximum impact, these metrics will need to be consistent across agencies. Each agency will then have to gather additional data on identity proofing pass/fail rates, at what point in the process failure occurs, usage, etc. Will this be required? How frequently must the analysis be done? How will inequities, if discovered be addressed? Will reporting be required? To who?	Consider questions; further explain and clarify section

Kantara-6	63-Base	Note to Reviewers	ii	148-155	NIST stands to unlock the true innovative capabilities of the solutions market by clearly stating quantifiable details for all proofing and authentication levels. With the freedom to creatively develop solutions that achieve the desired outcomes for each proofing/authentication level, the choices available to CSPs across public and private sectors will flourish. These options will drastically improve the overall ability to make the advancements in equity and accessibility described in the draft.	We suggest NIST publish a "quantifiable" set of measures and requirements for proofing and authentication levels, including a set of technologies/elements with their corresponding values. With such a framework in place, the technology community can build innovative approaches to satisfy the desired proofing/authentication value outcomes with being limited by a small set of acceptable methods. This is especially critical with regard to NIST's request for alternatives for solutions such as Face Biometrics. Please find the areas of focus regarding this topic below: - Establish a scoring/measurement system for all proofing and authentication levels. 800-63-4 should include a scale that allows all CSPs to understand the value of proofing and authentication. For example, an IAL2 Proofing event must equal a value of "10 points". - Rather than a short list of "strong" and "fair" pieces of evidence, please offer a list of evidence categories with point values. From there the technology community can innovate to achieve the desired outcomes in ways that will address all populations better by combining them to better fit the realities of each audience. - In lieu of publishing a list of acceptable evidence "categories" and point values, NIST may also allow for solution providers to present their own assessments of proofing/authentication values when the are certifying their solutions. Further, they may also be allowed to present their case for alternatives and unique combinations of evidence that meet the spirit/desire of 800-63-4 for approval.
Kantara-7	63-Base	2	3	355	word change --> 'the unique' should be changed to 'a unique'.	the unique --> a unique
Kantara-8	63-Base	2.1	5	435-436	"Guidelines do not address the identity of subjects for physical access ....."	Suggest this be struck, physical access requires identity process and access authorization considerations, while they may not identified in the subsequent 63-* documents - excluding it as a while can crate divergence in an area that already struggles to be compliant with PIV.
Kantara-9	63-Base	2.3	6	490	edit for clarity	consider rewording the sentence to something like: "Enterprise risk management is most effective when it is designed to be multidisciplinary and to consider a diverse set of factors and equities. "
Kantara-10	63-Base	2.3	7	501	consider adding reasons for why this a good idea to the end of the sentence	such as "...at a lower level of assurance in order to improve equity and access without compromising security or to balance access with security concerns."
Kantara-11	63-Base	2.3.1	7	521-532	Addition to section for physical access risks	Consideration for physical access risks need to be added - as well and the Interagency Security Committee's Risk Management Process used to assess facility risk.
Kantara-12	63-Base	2.3.3	8	554	Broaden the landscape of technologies included in omni-channel identity by introducing more telephony-based capabilities within the scope of the rule for both proofing and authentication. Specific reference to the FCC required implementation of "STIR/SHAKEN" for phone networks to ensure people can trust incoming calls. Caller IDs are "signed" as legitimate by originating carriers under the standard. 1. As digital channels of accessibility become harder to penetrate, risk shifts to call centers. 800-63-4 should include telephony with the definition of "omni-channel" and drive solutions to protect it. 2. STIR/SHAKEN offers the opportunity to add safety to phone-based interactions analogous to the rigor encryption provides to digital channels. The ability to leverage a digital signature within the SIP header of a call offers innovative vendors new pathways to explore in creating proofing/auth capabilities. STIR/SHAKEN expands the art of the possible for all solution providers. 3. This comment lends itself to addressing NIST's desire for alternatives to offset the use of biometrics. Telephony oriented solutions (likely combined with others) may address the desire for non-biometric alternatives. 4. Increasing equity and accessibility means meeting users with capabilities they have available to them. STIR/SHAKEN, and complementary solutions, may reduce the risk profile for under-proofed populations. When advanced technologies are not accessible or feasible, individuals resort to telephone-based interactions. 800-63-4 should be inclusive of this channel to address fraud and identity assurance.	Our legacy standards and approaches have been focused on purely digital interactions (websites, apps, authenticators, biometric technologies, etc.), but the phone channel continues to be a channel that requires attention. Without specific methods and safeguards in place for phone-based channels, CSPs are at risk of either (1) being compromised by sophisticated phishing attacks targeting call center agents or (2) are not able to support the needs of individuals that are not able to be cared for by other channels. When systems and technologies in the digital channel fail, aren't usable or aren't accessible to populations of individuals… the call center becomes to default. To support citizen-facing agencies, 800-63-4 should include means of securely empowering call centers and telephone-based technologies to add-value to the proofing and authentication workflows of the future.
Kantara-13	63-Base	2.3.3	8	554	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.	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" or "burner phones". Build in accommodations for the safe use of "pay-as-you-go" mobile phones given their prominence with some demographics.
Kantara-14	63-Base	2.3.3	8	554-586	The standard guidance should be strengthened such that CSP can operate in a mobile/transportable context to serve those who have transportation challenged.	Allow for alternative form-factors within the context of in-person and remote identity proofing such that they can be located across broader demographics and/or enabling the kiosks or proofing devices to be securely transported to the individual (e.g., portable units that could go to a hospital, elderly home, etc)
Kantara-15	63-Base	2.3.3	8	561	LGBTQ+, much like the term 'LatinX', is a term that while it has been embraced by the media can be offensive to many in the community it purports to describe.	Recommend removing this term. It doesn't add clarity to the sentence.
Kantara-16	63-Base	2.3.4	9	597	Without a qualifier it's too easy to design a study around a 'typical' or 'average' user who has good internet connectivity and an up to date smart phone and exclude the users who may be more challenging to support. In fact, if we want to reduce inequity I would skew the demographics of samples towards those who have the greatest challenges with technology.	add 'demographically', so it reads 'with demographically representative users'.
Kantara-17	63-Base	2.3.4	9	597	Standard usability metrics can automatically ensure baseline compliance and system integrity for usability, inclusivity, and customer experience validation.	Add relevant standardized usability metrics for baseline compliance testing. This can be readily added to self-service, remote, and Supervised Remote In Person sessions to measure, maintain, and ensure the continuous integrity and usability of the system.
Kantara-18	63-Base	4.1	11	613	"Subject" roles are inconsistent with the defined term "Subject: A person, organization, device, hardware, network, software, or service" in Appendix A.	Replace the defined term "Subject" with something like: Subject: an entity, usually a person, that applies to, or subscribes to, a digital identity management system
Kantara-19	63-Base	4.1	11	613	The "Attacker" entity is missing from the digital identity model section. The Attacker motivates a large part of the Digital Identity Guidelines, and should be represented as an Entity related to the system.	Add "Attacker" as one of the entities described in the digital identity model.
Kantara-20	63-Base	4.1	11	614	account for IAL0/AALx credentials	recommend changing to: "Applicant - the subject applying for a credential; for IAL1 and above, the subject to be identity proofed"
Kantara-21	63-Base	4.1	11	618-622	Definition of CSP could be expanded.	Should the CSP description be expanded to incorporate Adjudication / Background activities associated with IAL acts.
Kantara-22	63-Base	4.1	11	636	edit for wording	Recommendation: Change 'The usual' to "One possible" or similar.
Kantara-23	63-Base	4.2	15	721	Implies that CSP boundary doesn't stop at just identiity-proofing and must maintain ongoing "accounts".	

Kantara-24	63-Base	4.3.1	17	733	proposed edit for clarity	Recommend changing to 'memorized password or PIN' to account for the fact that passwords are often now closer to 'something you have' for individuals using password managers.
Kantara-25	63-Base	4.3.1	17	735	Need to evolve the standard to make a "something you are" authentication requirement for more than just the "highest security requirements" (referenced in lines 740-741).	To adequately identify an entity it MUST require the use of "something you are." Relying on something known + something held only binds to the item not the individual entity. For e.g., many phones employ TSM's that may/may not use something you are for authentication but there is no correlation with the have. The identity relies simply on the item held. E.g. a child may enroll in a parents phone - with services then applying the identity of the parent.
Kantara-26	63-Base	4.3.1	17	740-741	"using two factors is adequate ….". To achieve high security biometrics would provide a high level of confidence compared to other factors.	Expand the statement to state "two factors the use of biometrics to meet the highest security requirements".
Kantara-27	63-Base	4.4	21	854-855	Current language does not address "downgrade" changes to an authenticator.	Add "downgrade" to possible actions
Kantara-28	63-Base	5	23	922	In Section 5, NIST calls for "Continuously Evaluate and Improve" as part of the Digital Identity Risk Managment, but does not provide specific guidance on how to do this. We have suggested an approach and metrics that NIST can require CSPs to report. NIST can also use an independent body, like Kantara Initiative, to audit collection and reporting of these metrics in a standardized way across industry. Measuring the system level performance of solutions yields some benefits: 1. Improved Procurement: Enables agencies to evaluate and select the highest performing identity solutions. 2. Standards Feedback: Enables NIST with empirical data that can be used to develop operational guidance and to shape the next version of SP 800-63. 3. Increased Trust: Transparency will further public trust and will hold digital identity solutions providers accountable for actual performance data. We are also concerned that focusing on any one component – and removing or including it – is too narrow a view. Digital identity solutions providers are responsible for including equity and access “safety valves” to mitigate the risk of bias for ALL potential component failures tied to identity resolution, identity validation, and identity verification. Additionally, digital identity solutions providers should account for populations like international users, who may not be present in an issuing or credible source, Americans without credit history or an accurate presence in records, unhoused populations, etc. Controlling for the exogenous impact of user incentives on performance should also be normalized. The incentives of a user to undergo identity proofing can significantly impact metrics like Abandon Rate outside of the digital identity solution providers control. For example, a doctor who needs to meet the NIST 800-63 requirements to electronically prescribe according to state law will have a much lower abandonment rate than an American who might have a mild curiosity to learn a little bit more about their retirement benefits data.	Specifically, we recommend NIST implement the following normative requirements, supplemented by regular audits, to ensure consistent and accurate measurement of performance. Digital identity solution providers should be required to report the following metrics: 1. Pass Rate: Overall percentage of unique users who complete proofing 2. Fail Rate: Overall percentage of unique users who try but fail a given step e.g. unable to pass document authentication despite two attempts 3. Abandon Rate: Overall percentage of unique users who abandon at a step in the flow without attempting that step 4. Fraud Rate: Overall percentage of estimated fraudulent users Independent audits conducted by a reliable third party, such as the Kantara Initiative, should validate or invalidate the digital solution’s providers estimates. For example, an auditor should look into users marked as fraudulent to determine if those individuals are in fact fraudulent actors or if the vendor had a false positive. This independent check would force reconciliation of vendor reported data to ensure accurate measurement. Digital identity providers should be required to monitor the following KPIs: 1. True Pass Rate: Overall Pass Rate minus the Fraud Rate - If attempted fraud blocked is 3% one month and 20% the next month, it doesn’t make sense to show a 17% drop in performance when the solutions provider is actually effectively preventing identity theft and fraud. Rather, the key metric for accessibility should focus on the experience of non-fraudulent users. 2. Customer Experience: Time spent identity proofing. This time should be the unique user average of new identity proofing events at each agency: - Federated Users who arrived at the agency with an IAL2 credential, logged in at AAL2 and provided consent to verify at a different agency. - Unsupervised Remote users who proofed via self-serve flows. - Supervised Remote users who proofed via video chat. - In-Person users who verified at an in-person location. Agencies should be able to filter metrics through the lens of Equity to understand the impact of a solutions provider on a given community: - Zip Code Level Performance - Demographic Performance, including but not limited to: + International Users + Unhoused Populations + Age Bands + Race/Ethnicity Measurement will ensure a fair and impartial scoreboard for access, equity, reliability, security and privacy-protection. Once there is transparency around solution
Kantara-29	63-Base	5	23	923	clarity	Due to the complexity of this process, consider relabeling this as informative.
Kantara-30	63-Base	5	23	930	clarity	function seems to refer to 'digital identity function'. Perhaps 'digital identity function' would be more clear than 'function in the identity system'?
Kantara-31	63-Base	5	23	932	The first step for agencies needs to be fully defining and tailoring impact categories to provide concrete thresholds and examples for 'Limited/Low', 'Moderate', and 'High' for each category. This is non-trivial and should be an organized effort that includes business owners, cybersecurity & fraud experts, and enterprise risk management executives. Once clearly defined impact thresholds are established then an agency can conduct assessments that are meaningful, repeatable, and fully reflect that risk appetite of the agency. Ideally, this should precede conducting impact assessments. Otherwise, assessments will vary widely depending on the way an individual analyst interprets the term 'limited' or 'serious' on a particular day. Furthermore, this should be an iterative process - when confronted with an application-specific impact not initially considered the decision made should be documented in the impact criteria used as an assessment reference. Team composition is also important - and agencies need guidance on the skill sets and knowledge required to do thorough assessments	expand on the process of defined set of impact categories
Kantara-32	63-Base	5	23	939	For equity, usability - Will detailed guidance be provided on how to conduct 'detailed equity and usability assessments' and how to measure 'equity'? These are wonderful goals, but it will be difficult to achieve meaningful results. Will agencies decide individually which equity parameters they will measure for their performance metrics, then decide on individual targets for improvement? There are many potential equity parameters - as partially enumerated in section 2.3.3 .	consider providing guidance
Kantara-33	63-Base	5	23	939	Further on equity/usability, it will be challenging to balance privacy principals such as data minimization with efforts to improve equity and usability. It is not possible to measure all the equity impacts of a system without capturing information about users that some may see as overly intrusive, so we may need an 'opt out' or 'opt in' requirement so individuals being identity proofed can provide demographics voluntarily.	for consideration
Kantara-34	63-Base	5	23	939	Further on equity/usability, additional funding will likely be required. These are complex and expensive endeavors that may require applications to be updated so they can provide the necessary data for these assessments to occur.	for consideration
Kantara-35	63-Base	5	23	939	Will guidance be provided on how to conduct threat assessments? With the shortage of cyber and DI expertise in the government, explicit guidance will be needed for this to be implemented well at many agencies.	consider providing guidance
Kantara-36	63-Base	5	23	945	Continuously Evaluate & Improve: This is definitely needed, however agencies will need concrete guidance on how to do this. If that guidance is provided in a subsequent section in this document, it should be referenced here.	consider providing guidance and referencing
Kantara-37	63-Base	5	23	945	Agencies will need guidance on what information to collect and how to evaluate/analyze it. This is non-trivial. Many applications are not designed in a way to make the right information easy to collect, and it may need to be supplemented with demographic or other information for analysis.	consider providing guidance

Kantara-38	63-Base	5	23	945-952	CD/CI methodology can best be applied when using controlled systems and aggregating metrics.	Require components to report and collect standardized telemetry metrics for a set period of performance to report, manage, and measure performance and impacts of change/improvements over time. Suggest a 3-year rolling cycle for YoY performance monitoring. This works best for systems that rely on algorithms and objective data versus subjective human assessment. For e.g., during an endpoint capture of enrollment data the system can aggregate and measure time to enroll, failure to enroll, etc.
Kantara-39	63-Base	5	23	949	Monitoring for unintended harms is something to aspire to, but is complex. It is challenging to distinguish bad actors from legitimate users in an operational environment.	Explicit guidance will need to be provided.
Kantara-40	63-Base	5	23	958	How will the typical analyst conducting risk assessments know about the changes to the threat environment that are relevant to them? We're not aware of any government resources that can give analysts the information they need to do this well. CISA's current resources are not a good match for this need.	consider how it will occur or remove
Kantara-41	63-Base	5	24	962	clarity - SHALL's should only be placed before clearly defined requirements. This type of displaced SHALL could lead to compliance challenges for agencies.	revise
Kantara-42	63-Base	5.1-5.3	24	965	Change in Rev 4 - included 'mission needs' in conjunction with risk (previously only risk considered) The consideration of impact to mission delivery in addition to cybersecurity risk was only accounted for under 'compensating controls' in the previous version. This consideration is critical for organizations to effectively manage risk of both error types that could impact their agency: Type I error (rejecting a good subject) and Type II error (accepting an incorrect subject). To effectively manage these combined risks, it requires a fairly mature identity proofing measurement system that tracks the outcomes of the process. These measurement systems require processes and data environments that are not common across all organizations.	While not expected directly in these sets of guidance, providing a supplement specific to identity risk measurement systems will be key to effective implementation and management of a risk-based approach to identity management.
Kantara-43	63-Base	5.1	24	971	An additional step is required - bad actors need to be explicitly and carefully considered. Who may be motivated to gain access to a particular transaction? What may they gain by obtaining information they shouldn't have access to or by providing false information? What are their incentives/motivations? Different categories of bad actor should be considered separately - primarily politically vs economically motivated & bad actors who know the individual whose identity they are attempting to fraudulently utilize vs bad actors who do not know their victims. (This is not a comprehensive list.)	Include the additional step.
Kantara-44	63-Base	5.1	24	979	add clarity	Add the option to use a more granular scoring system, especially for agencies with a wide variety of user types and applications. SSA is using a 0-9 scheme where 0 is N/A, 1-3 is Limited, 4-6 is Moderate, and 7-9 is high. Given the inherent subjectivity in making impact assessments, as well as the equity and operational considerations that must be taken into consideration when implementation decisions are made, it is useful to understand whether an impact is assessed as a 'very low Low' (1) or a 'Low, but borderline Moderate' (3), and whether a Moderate is closer to Low/Limited (4) or High (6).
Kantara-45	63-Base	5.1.2	25	998	edit for clarity	Recommend changing to 'expected potential' or similar. Otherwise, some risk assessors may take a 'butterfly flapping their wings sets off a hurricane' approach to risk assessment, conjuring highly unlikely worst-case scenarios.
Kantara-46	63-Base	5.1.2	25	999-1004	Need to advise on the less-obvious harms that could occur in this and the following bullets	Further delineate potential, less obvious impacts and harms. Not to be exhaustive but the provided 6 bullets are broad and generalized.
Kantara-47	63-Base	5.1.2	25	1001	Why was 'unauthorized release of' replaced by 'loss of'? 'Loss' implies that the information may have been destroyed.	Perhaps rename this category 'Loss or unauthorized release of information', which would clearly cover both cases of inappropriately shared information and information that is deleted or destroyed by a bad actor, which is a risk with an authenticator error to a service where the legitimate user has previously provided information. Further suggest expanding the title to "Unauthorized release, verification, or loss of information". When information such as someone's SSN is verified by a bad actor it becomes more likely to be used for identity theft. Verified information is more valuable on the black market than unverified information, so government verification services pose a risk as well.
Kantara-48	63-Base	5.1.2	25	1002	Did NIST intentionally remove agency liability from consideration entirely? Also, organizations and wealthier individuals can sustain sometimes very large economic losses without losing 'economic stability'. Was the intent to only consider losses that have truly dire impacts? Isn't that the purpose of the 'Low', 'Moderate', and 'High' thresholds?	If that was not the intent revert back to the prior language which is clear and comprehensive "Financial Loss/Agency Liability".
Kantara-49	63-Base	5.1.2	25	1003	edit for word choice	Recommend using the term 'physical safety and health'. Without the 'physical' qualifier this may be interpreted in too broad a fashion to include mental health. 'Reputation' sufficiently encompasses impacts that would commonly be expected to infringe upon mental health.
Kantara-50	63-Base	5.1.2	25	1003	Consideration for the environment is a welcome inclusion in this DRAFT, however environmental damage that can lead to safety and health issues is not necessarily the same as environmental 'stability'.	Recommend removing 'environmental stability' from the title of this category and instead provide an example in the explanation that reminds readers that environmental damage may lead to health or safety impacts. If the intent is to address other impacts on the environment that may not directly impact human health or safety, a separate category could be created for those agencies where that category is relevant.
Kantara-51	63-Base	5.1.2	25	1006 -1007	Agencies will need more guidance on this: Each impact category SHALL be documented and consistently applied across different applications assessed by the organization.	Provide guidance
Kantara-52	63-Base	5.1.2	25	1014	Include additional examples.	It would be helpful to provide examples of harms to businesses or external organizations for those agencies that provide services to other organizations, such as SSA, IRS, FDA, USDA, etc.
Kantara-53	63-Base	5.1.2	25	1027, 1033	The unauthorized verification of PII can also lead to harms. The value of stolen PII increases when it has been verified by an authoritative source, and increases the likelihood that the PII will be used for identity theft.	change 'loss of PII' to 'unauthorized release or verification of PII'
Kantara-54	63-Base	5.1.2	25	1034	When these impacts are the results of impacts in other categories it is recommend only accounting for them in the primary impact category. This category should then be scoped so that it deals with direct financial loss only, such as when a check is rerouted from a beneficiary to a bad actor.	consider rescoping

Kantara-55	63-Base	5.1.2	26	1037	If these arise from loss of sensitive information, damage to trust/reputation, or other impact categories, they can be addressed there.	consider scoping this to only direct financial loses.
Kantara-56	63-Base	5.1.2	26	1039	editing category of environmental stability and corresponding bullet points	recommend removing this from the health/safety category title and consider creating an Environmental Stability/Damage category to be used by agencies whose services or programs could have direct environmental impacts.
Kantara-57	63-Base	5.1.2	26	1040	Suggest removing 'mental and emotional well-being' from this category and instead keep it focused on clear physical harm. Impacts to mental and emotional well-being are secondary rather than primary impacts and can therefore be fully accounted for in the appropriate primary impact category. For example, financial loss or unauthorized release of sensitive information can both result in distress. That distress is best accounted for within the precipitating category. It's important to not dilute this category which can paradoxically result in it being given less weight than it deserves.	remove mental, or emotional well-being from category
Kantara-58	63-Base	5.1.2	26	1041	edit for clarity	Recommend changing this to 'damage to the environment that is expected to lead to death or loss of physical health'. If other results of damage to the environment are to be accounted for, that is best done in a separate impact category. This category should be focused on clear and immediate physical harm to individuals so the risk associated with a high rating is immediately and clearly understandable.
Kantara-59	63-Base	5.1.2	26	1041	This impact should be covered within the financial harms category. Counting the same impact in multiple categories could reduce the readability (and therefore the import) of a risk assessment.	move category
Kantara-60	63-Base	5.1.2	26	1043	Is this a realistic primary consequence of a DI error in a service provided to the public? What is an example of this? And wouldn't the organization's inability to operate fall more appropriately in the damage to mission delivery category?	consider feasibility
Kantara-61	63-Base	5.1.2	26	1047	These are all secondary impacts that are covered by the other impact categories. The only primary impact for this category is to the agency/organization providing a service. SSA is rating the impact to the public for this category as N/A. The other categories such as damage to mission delivery already cover these impacts to the public.	Recommendation: Do not repeat impacts across categories without careful consideration. Instead, try to make them as focused and atomic as possible. In this case, the recommendation is to focus on the impact to the agency/organization if they violate laws/regulations/contractual obligations.
Kantara-62	63-Base	5.1.3	26	1055	Agencies need to be aware that they MUST concretely and unambiguously define what 'limited vs serious vs severe' looks like for their agency for each category, which is a non-trivial effort. Otherwise, assessments will be based on what 'feels' limited or serious to the individual tasked with doing the analysis that day (an individual who may very likely not have a strong risk assessment or DI or cyber background).	consider adding language about requirement
Kantara-63	63-Base	5.1.3	26	1066	While IAL, AAL, & FAL need to be considered separately, formally evaluating them separately typically leads to a repetitive copy-paste effort in DIRAs. In the vast majority of cases the impact will be the same regardless of the source of the error whenever there is identity proofing.	Change 'evaluated' to 'considered'.
Kantara-64	63-Base	5.1.3	27	1071	edit for alignment	Recommend removing the word 'slight' to align this explanation better with the FIPS 199 definition of 'Low'.
Kantara-65	63-Base	5.1.3	27	1071	Disparities in access are independent of the impact categories and instead correlate with the implemented controls (which are chosen based on the impact category ratings.) So, the higher the rating in an impact category due to inappropriate access being granted, the higher the controls will be, and the greater the disparities. Impacts from disparities in appropriate access that arise from the implementation of controls simply can't be considered at the same time as impacts that arise from granting inappropriate access.	Recommendation: As part of the DIRA process, separately document the expected disparities in pass/success rates for legitimate users that may arise from the differentIAL, AAL, & FAL implementations. (And remove it from this section.) For example, at IAL1 x% of legitimate individuals below the poverty line are expected to pass remote identity proofing, and at IAL2 only x-20%, etc. (Although this will be challenging to measure and implement. See previous comments).
Kantara-66	63-Base	5.1.3	27	1085 - 1088	Outcome disparities due to DI errors can be eliminated by removing all controls. The impacts arising from inappropriately granting access cannot be assessed in the same category as the impacts that arise from inappropriately denying someone access (due to the controls intended to prevent the first type of impact).	Recommendation: As part of the DIRA process, separately document the expected disparities in pass/success rates for legitimate users that may arise from the differentIAL, AAL, & FAL implementations. (And remove it from this section.) For example, at IAL1 x% of legitimate individuals below the poverty line are expected to pass remote identity proofing, and at IAL2 only x-20%, etc. (Although this will be challenging to measure and implement. See previous comments).
Kantara-67	63-Base	5.1.3	27	1093	Inconvenience' is both a secondary effect and categorically different from damage to trust or reputation. It will often arise naturally from other impacts such as damage to mission delivery and financial loss, so should usually be accounted for in those primary categories. For cases where it is the primary impact a separate	Recommendation: Remove 'inconvenience' from this category. 'Inconvenience" category makes more sense.
Kantara-68	63-Base	5.1.3	28	1100	The title is missing: 'Unauthorized Release of Sensitive Information'	correct.
Kantara-69	63-Base	5.1.3	28	1110	Recommend that this category only be used for direct financial loss (for example, payments are redirected to the wrong account). Indirect losses that occur as a result of impacts in other categories can be accounted for in those primary categories.	rescope category
Kantara-70	63-Base	5.1.3	28	1111	edit for alignment	Recommend changing to 'a limited' to align with FIPS 199
Kantara-71	63-Base	5.1.3	28	1116	Mental health impacts are secondary to other impact categories so can be handled in the primary category, such as damage to reputation, loss/exposure of sensitive information, and financial loss. Also, mental health is far too subjective and variable to assess on its own. An event that traumatizes one individual may not even be noticed or remembered by another individual, and that is especially true across cultures. Agencies would need both social anthropologists and psychologists on staff to assess this separately.	consider removing
Kantara-72	63-Base	5.1.3	28	1116 - 1117	Remove from this category and create a separate category, or clarify to indicate that this is environmental impact that is expected to have impacts on the health of individuals (such as increased lead levels in water).	adjust structure according to comment (remove or clarify)
Kantara-73	63-Base	5.1.3	28	1127	edit wording	an insignificant or inconsequential --> limited
Kantara-74	63-Base	5.1.4	29	1133	This section is where the tension between strength of controls and demographic disparities that may arise from the implementation of those controls could be discussed. For example, IAL2 may cause an in increase in legitimate users being denied access to a service, which may lead to economic harm, whereas IAL1 may lower the access disparities but increase the risk of fraud (which may also lead to economic harm).	consider adding context to section
Kantara-75	63-Base	5.1.4	29	1139	Risk combines impact and likelihood.	Since we aren't discussing likelihood, recommend changing to 'impact'
Kantara-76	63-Base	5.1.4	29	1140	Strongly recommend changing this from 'assess' to 'consider'. The word 'consider' leads to readable risk assessments where the risks are easy to discern, and any differences in identity and authentication errors can be made clear. The word 'assess' results in unreadable copy-paste exercises where the same impact is typically repeated three times for each of the seven categories which drowns out the actual impacts in a lot of noise.	changing this from 'assess' to 'consider'.

Kantara-77	63-Base	5.1.4	29	1140	consider rewording - replacing risk or adding guidance. see suggestion.	either change 'risk' to 'impact' or add guidance on assessing likelihood and determining risk based on both likelihood and impact. If likelihood is used, consider discussing confidence in the likelihood, which can be challenging to determine and many (most?) agencies may not be doing the analysis required to determine likelihood accurately.
Kantara-78	63-Base	5.1.4	29	1150	We can't assess barriers that arise due to identity proofing controls until after we've decided on what those controls will be (based on the impact of granting inappropriate access).	remove or reconsider clarity
Kantara-79	63-Base	Table1	30	n/a	L/M/H does not provide sufficient granularity when DEI and other operational impacts will be taken into consideration	Recommend 1-3 L, 4-6 M, 7-9 H
Kantara-80	63-Base	5.2.2.1	31	1197	A reference to IAL0 should be included. Some agencies will have IAL0 for some of their credentials, and its absence here may lead to over-use of identity proofing when it's not required or, at the very least, inconsistent terminology (which has impacts in a federated environment).	reference IAL0
Kantara-81	63-Base	5.2.2.2	31	1212, 1216	edit grammar	change to the plural - authenticators
Kantara-82	63-Base	5.2.3	32	1238	edit - reword for clarity/accuracy	Change 'primarily based on cybersecurity risk' to 'primarily based on the impacts arising from digital identity errors'.
Kantara-83	63-Base	5.2.3	32	1240	Organizations may select an assurance level for marketing reasons (i.e., they wish to offer an IAL2 service); and would therefore not need a documented process for selecting an assurance level.	The document should note this.
Kantara-84	63-Base	5.2.3	32	1240	SHALL develop and document based on selection of assurance levels determined by digital identity failure impacts. This is entirely self-governed by the organization and does not enforce minimum safeguards to the constituents.	The definition of required xAL's must be defined by the guidance based on impact assessment. How does the guidance protect the entity or constituent if they can in effect self-govern? Suggest that reference xAL associations be made based on intended use (e.g., banking, benefits, healthcare, etc>0
Kantara-85	63-Base	5.2.3	32	1241	edit - clarify A 'failure' to identity proof someone or to authenticate someone could mean that it is working as designed - such as when an impersonator/ bad actor is prevented from gaining access to a system. Errors may be a better word choice.	Change to 'errors'.
Kantara-86	63-Base	5.2.3.1	44	1245	To implement risk-based approach, other attributes should be collected during identity proofing. There should be weighted risks associated with the subject, service, transaction, access and other possible attributes/parameters to facilitate CSP provide a more accurate risk-based decision.	
Kantara-87	63-Base	5.2.3.1; 5.2.3.2	33; 34	1267, 1308	edit - reword suggestion	Strongly recommend replacing 'worst-case' with 'highest assessed impact'.
Kantara-88	63-Base	5.2.3.2	34	1315 - 1318	Rather than taking this approach, it's recommended to assess the impact to mission delivery caused by false positive DI errors along with the other categories. Do not wait and evaluate it and then try to combine the impacts of errors caused by false positives with the impacts of the controls. Instead, evaluate the potential impacts of false negatives separately.	consider recommendation
Kantara-89	63-Base	5.2.3.2	34	1322	Many low impact applications will be AAL2 because they contain some PII, such as a name.	Update Moderate to Low
Kantara-90	63-Base	5.2.3.3	35	1351	edit - word choice	change worst-case --> to highest impact
Kantara-91	63-Base	5.3.1	37	1406	Is this the same as a Privacy Impact Assessment? If it is different, how is it different?	add clarity to answer questions
Kantara-92	63-Base	5.3.1	37	1411	Will there be guidance on which demographics and groups should, at a minimum be considered? Will it be left up to each agency? Will agencies also independently establish their on metrics and evaluation techniques?	add clarity to answer questions
Kantara-93	63-Base	5.3.1	37	1414 - 1416	This can't be left up to each individual agency. They don't have the expertise or resources, and doing this right is a significant effort.	consider how to provide support, or remove expectation
Kantara-94	63-Base	5.3.2	38	1438	edit - word choice	Change "due to availability" to: "due to the lack of availability of required evidence"
Kantara-95	63-Base	5.3.4	38	1463	The Digital Identity Acceptance Statement appears to be an SSP for the 800-63 process?	
Kantara-96	63-Base	5.5	39	1493	Recommend changing this to a SHALL. It's critical that this occur and should be relatively easy to implement.	increase requirement to SHALL
Kantara-97	63-Base	Appendix A	43	1590	Increase formality of introduction paragraph.	Suggested replacement: The terms and definitions used in SP 800-63 (all volumes) are defined in this Appendix. Terms have been updated for this version of SP 800-63. Note that terms used in other publications may differ from these definitions.
Kantara-98	63-Base	Appendix A	43	1590	Suggest to structure the terms to enable alphabetic grouping of variations of a term. For example instead of "Active Attack" and "Passive Attack" use "Attack, Active" and "Attack, Passive" Alternatively, one could use sub-headings to group the variants.	Restructure terms to enable alphabetic grouping of variants of a term.
Kantara-99	63-Base	Appendix A	43	1595	Definition of Access rewording for simplicity.	Suggested replacement: To make contact with one or more functions of a digital service.
Kantara-100	63-Base	Appendix A	43	1607	"address of record" definition is very complex as written	Consider enhancing the definition to cover the "identity attribute" aspect of addresses (the place of residence); the "communication channel" aspect; and include some information about "whose record" is referenced in the term (i.e. if the CSP obtains the 'address of record' from a trusted 'authority' does that mean that the address of record has the properties of being valid and verified? or is the address of record the address recorded by the CSP that has also been actively validated and verified by the CSP?
Kantara-101	63-Base	Appendix A	44	1631	Rethink how the term "attack" is used throughout the volumes. As defined here, "an unauthorized entity's attempt to fool a verifier or RP into believing that the unauthorized individual in question is the subscriber", "attack" is a very specific kind of impersonation. However, the other terms in 800-63 that build on the base definition do not universally fit into that way of describing "attack". Consider re-using models (from NCCoE or NIST or other Federal sources) of threat-threatvector-vulnerability-adversary or risk-impact-likelihood or other well-established ways of describing adversaries and their impacts on the system goals. In the absence of a well-understood structure for risk evaluation and attacker identification/mitigation, solution designers have difficulty designing appropriate countermeastures throughout the 800-63 volumes.	Examine every definition that builds on the definition of "attack" (e.g. 'offline attack', 'phishing', 'presentation attack', 'passive attack', etc) and consider whether these other definitions are actually "attacks" in the context of the current 800-63 definition of attack. Consider restructuring the underlying model of attack-countermeasure vs threat-risk in a way that is better suited for analysis and design of controls in the other volumes of 800-63.
Kantara-102	63-Base	Appendix A	45	1679	Use of the term "subject" in the definition of "authentication" may be inconsistent in the context of 800-63. In 800-63 "Subject" is defined as "A person, organization, device, hardware, network, software, or service." While not technically incorrect, when compared to other Terms in 800-63 it seems to be inconsistent. For example, "Authenticator: something the claimant possesses and controls..." specifies a different actor for the same activity. For consistency with e.g. "Verifier: an entity that verifies the claimant's identity...", one could use "claimant" as the term for the actor.	Replace "subject" with the word "claimant"

Kantara-103	63-Base	Appendix A	45	1679	"authentication" term is missing the aspect that 800-63 relies on. Authentication in the context of 800-63 is about checking authenticator validity for the purpose of substantiating the claim of a particular "digital identity" - but the actual facts that authentication substantiates is that the claimant is able to demonstrate that they are associated or linked to a subscriber account, and from that subscriber account, the identifiers which are relied on by the RP. The missing bit in the current defintion is the piece about verifying the linkages or bindings - it's implied in the definition but should be made explicit.	Modify the definition of "authentication" and related terms in a way that describes how authentication, authenticators and subscriber accounts are linked/associated/bound together at enrolment time, then subsequently proven at transaction time. And the established bindings at transaction time are what the RP relies on.
Kantara-104	63-Base	Appendix A	46	1698	Definition of 'authentication secret' is incorrect	Should be something like "Authentication Secret: An authenticator that embodies a knowledge-based authentication factor"
Kantara-105	63-Base	Appendix A	47	1742	Definition of 'bearer assertion' is strange if 'bearer assertion' is a sub-category of the defined term 'assertion'.	Clarify whether the term 'bearer assertion' is actually as sub-category of the term 'assertion' or in fact something different (for example, 'bearer assertion' is possibly an information token that contains information about an entity, but has no binding information to the entity that is presenting the 'bearer assertion')
Kantara-106	63-Base	Appendix A	49	1786	"core attributes" as defined breaks easy interoperability - if every CSP is able to make their own definition of "core" then RPs will be unable to predict what information each CSP offers, without performing mapping between all the different CSPs that an RP wants to use.	Reconsider the term "core attributes" - perhaps this term should be defined by a federation or trust framework, for use by all federation participants. And, if a CSP is a "federation of one" it can define core attributes as it wishes - at the risk of being unacceptable to any particular RP.
Kantara-107	63-Base	Appendix A	49	1815	Definition of "cryptographic authenticator" mentions "the endpoint" - which endpoint?	Clarify what's referred to as "the endpoint"
Kantara-108	63-Base	Appendix A	50	1835	What's the difference between the terms "Digital Authentication" and "Authentication"? Are they supposed to be the same underlying term, with the only difference being that "digital" is simply "authentication" using digital or electronic means?	Re-consider the relationship between "authentication" and "digital authentication"
Kantara-109	63-Base	Appendix A	56	2043	Term "Processing" is a synonym and duplicate of term "PII Processing" on p55 line 2018	Merge the definitions
Kantara-110	63-Base	Appendix A	60	2152	Heading "software statement" is duplicated	Delete line 2152
Kantara-111	63-Base	Appendix A	60	2154	Ambiguous grammar (what is signed - the list of attributes? or the software?)	Clarify by altering the sentence structure

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:	Kantara Initiative, Inc.
Name of Submitter/POC:	Identity Assurance Work Group
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
Kantara-112	63A	Whole doc / set	0	0	Language is causing market confusion. To the providers it is confusing if it is guidance or a requirement. All volumes of this text are presented in contradictory ways ("These guidelines provide technical requirements ...") and in §1 ("This publication [provides] technical guidelines ...", "This document provides requirements ..."). The terminology is inconsistent. Requirements define something that one has to do, whereas guidance is purely informational, to be taken or ignored at will and without consequence. It is noted that the main body of the work contains a mix of informative material and presumably normative material which uses the specific capitalized key words 'SHALL', 'SHOULD' and 'MAY' in a very specific style of presentation. The intent of which is assumed to take on the meanings imparted to these words by RFC 2119, a practice widely adopted amongst SDOs (see also ISO Directives Part 2 App.H). This dichotomy should be resolved.	Determine if these are requirements or guidelines and make the necessary changes to each volume to reflect this change to state clearly that the document defines [normative] requirements [using key words as defined in RFC 2119] whilst providing supporting, explanatory and informative guidance. Implicit in this suggested change is that all references throughout the document to 'guidance' need to be reviewed to determine whether they are truly informative as opposed to being actual normative requirements.
Kantara-113	63A	Whole doc	0	0	The terminology used to refer to various types of proofing is inconsistent and does not readily describe actual practice. Though it is appreciated that there is good reason to allow developers and service providers scope for innovation, increased clarity in categorization would be appreciated.	A proposed taxonomy and associated definitions are provided in tab 'Proofing Type Taxonomy'. The content of this tab (including making use of the Notes provided) should be inserted as a new §2.2 'Identity Proofing Types'. Adopt the proposed taxonomy and use the defined terms or their abbreviations very deliberately and specifically for each normative clause. This will serve to remove from the start a considerable scope for confusion in implementation and in assessment/audit/evaluation. EACH reference to a proofing type needs to be reviewed and in almost all cases replaced with the appropriate term from the taxonomy.
Kantara-114	63A	Whole doc / set	0	0	The structure of the document does not lend itself to easy determination of: a) which clauses are actually expressing normative requirements; and b) what are discrete normative requirements. This is evidenced by no consistency in style regarding whether informative discussion precedes normative requirements and by single paragraphs which bear both normative and informative text (e.g. para commencing line 611). This weakens the utility of the document [set] in either its use as an educational/informative source or as a set of formal requirements.	1 - Express each normative requirement as a distinct clause; 2 - Give each such clause a unique reference; 3 - Give the user a very clear means to determine the status of a passage of text - i.e. exclusively normative or informative. It is noted that adopting a presentational distinction would be an easier solution to achieving much greater presentational clarity than trying to extract and regroup all passages of one type or another.
Kantara-115	63A	Whole doc / set	0	0	With relevance to comment above (Kantara-114) it is difficult to make a discrete reference to any part of these documents when they either: 1 - use bulleted lists, not those indexed (e.g.); or 2 - within any given clause, the numbering of indexed lists within different paragraphs is reset for each list, rather than continuing the numbering within the specific clause (e.g. §5.1.8)	Refrain from bulleted lists; indexed lists are easier to comprehend. Continue numbering of indexed list elements within a distinct parent clause, rather than restart each list where multiple paragraphs within the same parent clause have such lists. Furthermore, consider the choice of indexing sequences: taking 5.1.2.1 as an example, which has two levels of indexation, consider lower-case alphabetic indexing for the first level, numbers for the second. Thus, rather than §5.1.2.1 1) a), one would refer to 5.1.2.1 a) 1). The benefit of this is that it avoids confusion / error when referring to (e.g.) 3.2.1 and 3.2.1)
Kantara-116	63A	Whole doc / set	0	0	What is actually different between each xAL? As presented, this is not readily determined from reading the text. (E.g. §5.3.1 (IAL1), §5.4.1 (IAL2), §5.5.1 (IAL3) have identical text.) Why need this be repeated, rather than stated once in a section which addresses common proofing requirements? Table 1 gives a summary, but is not comprehensive (e.g., does not address the example given earlier). The detail is in the text and it is that to which anyone with a serious interest is going to have to refer.	Remove the duplicative text that appears from level to level. Help implementers, operators, agencies, consumers (Subjects and RPs), certification bodies, assessors/auditors, etc. get an easy read into what are the incremental changes between xALs by stating these clearly and distinctly.
Kantara-117	63A	Whole doc / set	0	0	Notwithstanding suggestions to replace 'subject' with 'subscriber', in order to ensure internal consistency and also in keeping with the usage of the drafts as presented, where a single entity appears to be uniquely intended (as opposed to the word being interpreted with the broad definition which is offered) it is noted that whereas the NIST set of documents refers to a 'Subscriber' seemingly as a sole person, other standards (e.g. ISO?, EN, Kantara) differentiate between a Subscriber and a Subject, as follows: Subscriber: a party that has entered into an agreement to use a «Proofing / Credential / other trusted» Service; Subject: an Applicant which has had its Identity proven [and potentially bound to a credential]. The notion here is that a Subscriber could be an organization which subscribes to a service provider for the provision of proofing / authentication / verifier services for the organizations specific community of (potential) subjects. The NIST definitions reverse the relationship between the two terms, which creates conflict when 'subject' alone is used.	NIST needs to do a review for every entity they talk about. Amend the definitions as now given and replace all instances of 'subscriber' with 'subject' (taking care not to eliminate the frequent instances of 'subject' in its natural sense). This will resolve to a consistent usage. As a recommendation in this specific instance but recommended across the whole suite of documents is that defined terms should be set in a capitalized form. This makes clear the intention that the word or term is being applied with the specific context of its definition. This also delineates between words (such as subject/Subject) which may be used in their natural language sense(s).
Kantara-118	63A	Acknowledgments	1	343 - 346	There has been notable interaction with Kantara pre-publication of -63 rev.4 DRAFT and since, and it is noted that concepts developed by Kantara in creating its own criteria against which to have assessments performed have now been adopted in rev.4. Recognition of this would be appropriate.	Add Kantara Initiative to line 346
Kantara-119	63A	2.2	4	416	Minimum rigor for IAL2 should be the person to person interaction necessary to validate a live subject during the application process.	Suggestion that IAL2 introduce language, based up specific use cases or based on risk level a trained CSP representative interact directly with the applicant during x (not entire but some period to have human confirmation of the subject) at some point within the identity proofing session. Guidance should contain information with recommended risk levels and triggers as examples.
Kantara-120	63A	4	6	426	This (and all other such instances) is not an accurate statement - the section is not entirely normative	Amend to "This section includes normative clauses"
Kantara-121	63A	4	6	427	typo	this section provides an overview ...

Kantara-122	63A	4	6	434	Value of the data to whom?	better to state "value which a successful attacker might gain" ?
Kantara-123	63A	4	6	437-440	Given the emphasis on promoting access "for those with different means, capabilities, and technology access", the guideline for IAL1 requiring one strong document evidence and one fair document evidence do not allow the underserved population to pass even at IAL level 1. Mobile phone, and thus fully remote verification, is more prevalent and accessible to the underserved population than transportation (e.g. to an in-person facility for extended review) or a computer and/or computer center for technology assistance. So if the emphasis for accessibility is genuine, there must be an effort to survey the reality of what the (underserved) population would find practicable whilst also guarding the need for adequate validation.	Would NIST consider making formal permanent links to sources to provide this type of information?
Kantara-124	63A	4	6	438	What does it mean to 'enable optionality', and is that the same as 'providing options'? Enabling and providing are not the same.	Please explain this phrase or amend the text to be more explicative.
Kantara-125	63A	4	6	443	"Multiple channels for engagement" lacks clarity - the exemplars being proofing types is confusing given the definition of 'multiple channels'	"multiple means of access for the Applicant" would be a clearer term to use
Kantara-126	63A	4.1	6	451	grammar	"certainty, that the applicant"
Kantara-127	63A	4.1.1	9	469	The difference between "Resolution" "Validation" and "Verification" is vague.	please clarify in terms and definitions
Kantara-128	63A	4.1.1	8	479-482	Subjective face matching is unreliable	Comparison match should be done through the use of a standard facial algorithm with sufficient PAD, liveness, and minimum accuracy setting FMR/FNMR.
Kantara-129	63A	4.1.1	8	479-482	Two forms of evidence with photos may not be presented for all xALs. No direction is provided for objective picture comparison. Is facial 'picture' verification the only approved method for step 3?	Using the evidenciary documents provided, and depending on the xAL forms required, a minimum number of valid document photos will be compared for match with the live subject AND applicant's photo. The comparison match should not be subjective for IAL2 or IAL3, instead the Ideally, the face photos extracted from the documents would be matched against each other and submitted photos and/or live video captures.
Kantara-130	63A	4.1.1	9	485	Typo: “verifying they the”	…Verifying that the…
Kantara-131	63A	4.2	9	494	word choice	Better to say "identity proofing process", not transaction
Kantara-132	63A	4.3	9	495	Multiple types and combinations of identity evidence are referenced.	NIST should publish and maintain a list of acceptable identity evidence. This should not be a document, but a live website that can be continuously updated for agencies to reference.
Kantara-133	63A	4.3	9	497	word choice	Better to say "determine whether it is …", not transaction
Kantara-134	63A	4.3.1	10	522	Should it be considered that the document issuer performed an equal or greater xAL proofing session prior to document issuance?	The issuer of the document performed an equal or greater level of assurance identity proofing of the applicant prior to issuing the document that is now being presented as physical evidence.
Kantara-135	63A	4.3.2	10	536	Should it be considered that the digital evidence issuer performed an equal or greater xAL proofing session prior to digital evidence issuance?	The issuer of the digital evidence performed an equal or greater level of assurance identity proofing of the applicant prior to issuing the digital evidence that is now being presented as additional digital evidence.
Kantara-136	63A	4.3.2	10	538	Digital evidence can be altered and should be required to have an associated digital signature to ensure it is valid and untampered.	Digital evidence can be altered and should be required to have an associated digital signature to ensure it is valid and untampered
Kantara-137	63A	4.3.2	10	539	typo	"accessible to the intended person"
Kantara-138	63A	4.3.3	10	542	63A should identify the strength of evidence requirements for typical identification; like those found in the I9. These items are currently identified in the "Digital Identity Guidelines: Implementation Resources" (Table A-3-2. Notional Strength of Evidence). Common IDs (e.g., US Passport and Cards, PIV Cards, REAL ID Cards, non-Real Driver’s License, Social Security Cards) should have identified specific strengths, rather than "notional" strengths identified.	Provide a strength of evidence table (perhaps as an appendix or in 4.3.3) for typical well-known IDs. Most likely a subset of "Digital Identity Guidelines: Implementation Resources" Table A-3-2. Notional Strength of Evidence. Additionally, the live website mentioned in Kantara-132 is preferred.
Kantara-139	63A	4.3.3-4.3.4	10-12	542-600	Please provide clarification on evidence strength requirements, specifically the areas of Fair, Strong and Superior stipulations.	Reference Kantara-132 for live website and Kantara-140.
Kantara-140	63A	4.3.3.1	11	548	Fair evidence is more of a barrier than a security feature.	Remove the need for Fair evidence at IAL2 & IAL3
Kantara-141	63A	4.3.3.1	11	551-552	The "issuing source" should be clearly defined. In real world scenario, issuing source could be any business in any industry that creates a paper trail containing core attributes resulting in thousands of potential issuing sources, and making it nearly impossible for CSPs to build capability to read or validate or treat the issuing source for fair evidence submission.	The stated requirements are impractical in real world scenarios. i.e. knowing a valid issuer, creating templates etc. may be difficult to manage etc.
Kantara-142	63A	4.3.3.1	11	553-554	Clarification and specified definition and/or guidance on the term "reasonably assumed". The current language is subject-to-interpretation. This requirement can be difficult to document during the assurance certification process. Limiting to just two industries, where the evidence documents could be stemmed from, CSPs would need to determine the success of delivery from approximately 13,000 entities - which could pose a challenge.	The stated requirements are impractical in real world scenarios. i.e. knowing a valid issuer, creating templates etc. may be difficult to manage etc.
Kantara-143	63A	4.3.3.1	11	557 - 559	Change in rev-4 - The evidence has not expired or it expired within the previous six (6) months, or it was issued within the previous six (6) months if it does not contain an expiration date. Given the potential for a newly issued account to have been established by a bad actor as part of an identity theft scheme, we recognize there should be concern related to recency of issuance. However, automatically excluding any evidence that has been established in the past six months seems relatively arbitrary and lacking justification.	Recommend revising the statement to read: “The evidence has not expired or it expired within the previous six (6) months. If it does not contain an expiration date, it SHOULD be reviewed for recency of issuance prior to acceptance.”
Kantara-144	63A	4.3.3.2	11	570	"high likelihood" is difficult to determine even without the 'high'.	Stick to the current term 'reasonable belief'
Kantara-145	63A	4.3.3.2	11	574	"a facial portrait or other biometric characteristic" seems to be slightly weird wording: could it be a painting, or must it be a photographic/digital image? Why make a case of the facial representation at all?	Simply require "a biometric characteristic" or explain whatever subtle difference there is in the mind of the author(s) between a facial image and any other bio characteristic. Alternatively, harmonize text between #3 and #4…contains a biometric attribute uniquely associated with the evidence holder
Kantara-146	63A	4.3.3.2	11	576; 595	5) presumes a physical form of evidence	Use instead "The evidence includes physical or cryptographic security features that make it difficult to copy, or reproduce or otherwise misuse." This is repeated for line 595.

Kantara-147	63A	4.3.4.1	12	601-607	Even if issuing sources are limited to certain industries - banking, utility and mortgage companies, for example - there are nearly 4,900 different bank "brands" registered in the US, over 3,100 utility providers registered under US Energy Information Administration, and about 4,400 financial institutions (typically also a bank but operates separately from the banking business) providing mortgage services. This equates to roughly 13,000, likely more as entities could have more than one document type, that could qualify as evidence documents wherewhich the CSPs are responsible to read and validate.	The stated requirements are impractical in real world scenarios. i.e. knowing a valid issuer, creating templates etc. may be difficult to manage etc. Numerous scenarios would need to be addressed.
Kantara-148	63A	4.3.4.1	12	603	text structure	State "by confirming" and remove 'confirming' from each of the three following points (see also Kantara-115)
Kantara-149	63A	4.3.4.1	12	608	For inclusivity and equity, Supervised Remote In Person Proofing could be mandated when using an expired ID. The CSP could require the expired ID to be validated by external validating authority and to match the invidivual in real time to the expired id with approviate PAD/liveness checks.	For individuals unable to access non-expired ID evidence, consider permitting the usage of expired ID evidence with supervised remote in person or in person proofing. Update terms if updated proofing taxonomy is adopted.
Kantara-150	63A	4.3.4.3	13	620	Change in Rev-4 - Included validation of evidence provided with a credible source. The ability for use of either authoritative or credible sources to validate identity evidence and attributes is critical to modernize any digital identity proofing process. While it was not specifically addressed in the previous version, it was the de facto method of automated validation of fair evidence. The addition of credible sources in addition to authoritative sources better reflects the reality of what constitutes effective validation. However, the current draft (§4.3.4.4) lacks any requirement related to a credible source's reputation or credibility.	The definition of credible source should include some measure of credibility, e.g., governmental regulatory oversight. Without an independent recognition of credibility included in the definition of a credible source, this runs the risk of rogue entities acting in this capacity. Which regulations denote credibility should be identified.
Kantara-151	63A	4.3.4.3	13	620-628	The text mixes manners of validation with proofing types.	After embedding a proofing taxonomy this can hopefully be made clearer
Kantara-152	63A	4.3.4.3	13	622, 623	This line uses 'trained personnel' The definition of IAL3 uses ' trained CSP representative ' In 4.4.1 we have 'CSP operator'. If these are essentially the same role then a single label would be much clearer - if they are not the same role then something needs to be done to describe the differences between them, use differential terms, and when one might apply vs. any other(s).	For the sake of consistency and therefore reducing potential confusion amongst implementers and possibly auditors/assessors, a single phrase would be helpful. The term 'Supervisor' (as used in 63 rev.3) would seem sufficient, if defined in a manner which imparts the need that they be trained, competent and efficient.
Kantara-153	63A	4.3.4.4	13	633 - 646	It is unclear whether this is informative or trying to set limitations, i.e. it is pseudo-normative. Better to be clear, if this is essentially trying to place limitations on how a CSP may consider an entity to be authoritative.	Modify line 634/635 to state: "A CSP SHALL only consider a source to be authoritative if it:" Modify line 642 to commence "Has collected ..." (for grammatical correctness)
Kantara-154	63A	4.3.4.4	14	647	Credible sources is a useful addition; however, there is no criterion that distinguishes between authoritative and credible sources (either is acceptable) .	considering using one term
Kantara-155	63A	4.3.4.4	14	647 - 654	It is unclear whether this is informative or trying to set limitations, i.e. it is pseudo-normative. Better to be clear, if this is essentially trying to place limitations on how a CSP may consider an entity to be authoritative.	Modify to state: "A CSP SHALL only consider a source to be credible if it:"
Kantara-156	63A	4.4.1	14	659	4.4.1 is confusing. It seems to be pseudo-normative since it appears to be setting conditions on how proofing should/may be performed and it seems to be making such determinations based on proofing type (addressed previously), yet there are no normative key words. If these ideas are important they should be expressed normatively. If the following normative sections do actually enforce these points then need they be set out here?	State normatively in appropriate places and remove from here.
Kantara-157	63A	4.4.1	14	663	Enrollment code verification as specified in Sec. 5.1.6. is not sufficient guidance. It needs expanded.	When enrollment codes are used for identity verification, the address needs to be strongly associated with an individual in an authoritative or credible source. Postal address. For identity verification, postal address should be preferred and email address should be disallowed.
Kantara-158	63A	4.4.1	14	668	In general, consistency of terms and usage would alleviate confusion. Here, the phrase "remote (attended and unattended) physical facial image comparison" is confusing and probably isn't needed, as it's the image comparison that is important. The text goes on to explain the attended or unattended part. Here, and section 5.4, are the only normative sections where the terms attended and unattended are used, suggesting they are unnecessary (and therefore confusing; especially as you transition away from "unsupervised")	Remote (attended and unattended) Physical facial image comparison. The CSP operator performs a physical comparison of the facial portrait presented on identity evidence to the facial image of the applicant engaged in the identity proofing event. The CSP operator may interact directly with the applicant during some or all of the identity proofing event (attended) or may conduct the comparison at a later time (unattended) using a captured video or photograph and the uploaded copy of the evidence. If the comparison is performed at a later time, steps are taken to ensure the captured video or photograph was taken from the live applicant present during the identity proofing event.
Kantara-159	63A	4.4.1	14	668	Facial image comparison is subjective and non equitable or inclusive. Racial bias exists in substantiated double blind tests proving 'facial blindness.'	While a live operator SHALL be available to observe and ensure the integrity of a session they should NOT be relied upon for facial comparison. Neural dissonance, facial blindness, and racial bias preclude this from a valid verification method. Instead ever-improving, baselined, and measured biometric matching can score the likelihood of facial match and the resultant score can be substantiated by the operator along with supervision of the session to ensure integrity, liveness.
Kantara-160	63A	4.4.1	14	673	Storage of captured video & the evidence introduces a whole set of security/PII concerns. Users may exploit this to playback a recording via a user's home web cam - effectively spoofing or injecting video that without a LIVE operator cannot be validated for authenticity. There is no check/balance to ensure that an operator would later return to the video for review.	There is the possibliity of an attacker replaying the video to subvert the system
Kantara-161	63A	4.4.1	14	682, 683	As a specific case of the point made in Kantara-156, this is the sole instance of the phrase "mathematical algorithm", so where is this normatively asserted?	Resolution should be accommodated by fixing the bigger picture, per Kantara-156
Kantara-162	63A	4.4.1	15	684-688	Expectation and guideline is unclear, please provide a workflow with specific examples wherewhich a user is deemed to have full control of their digital account.	Could NIST provide more detail on what is considered "full control" of a digital account?
Kantara-163	63A	5.1.1	16	699	Here, and throughout, where CSPs are required to document things; should specific documents be called out, like a "practice statement," or only identify a requirement to "document?" If the intention is a formal process where we want a policy that is traceable to a practice statement, for example, then this language makes sense. But if we only want things documented, that should be stated explicitly. If some documentation should be available to users or others, then that requirement should also be identified.	The CSP SHALL maintain documentation covering its operations detailing all identity proofing processes as they are implemented to achieve the defined IAL. The documentation SHALL include, at a minimum:

Kantara-164	63A	5.1.1	17	721	As written, this section suggests the need for CSPs to collect demographic data to assess for equity. Given the requirement to minimize collection of data (800-63-4ipd §5.5), NIST should recommend alternative ways that CSPs can assess performance of their platform across demographics. One example would be assessing performance at a zip code level, where available Census data could be used in place of collecting detailed demographic data from end-users during the proofing process. Please see comment Kantara-28 for further details on performance metrics.	See Kantara-28 for specific metrics to measure and track. When it comes to equity considerations, CSP performance metrics can be analyzed at the following levels without collecting any additional information beyond what is routinely collected in the identity proofing process today - Zip Code Level Performance - Demographic Performance, including but not limited to: + International Users + Unhoused Populations + Age Bands + Race/Ethnicity
Kantara-165	63A	5.1.1.1	17	723	As a subset of 5.1.1, why not just add it to the list there?	10. The CSP's policy and plan for when it ceases its operations, including whether the CSP's identity service is subject to retention requirements and how it will protect any sensitive data (including identity attributes, and information contained in subscriber accounts and audit logs) during the period of retention and how the CSP disposes of or destroys all sensitive data at the end of any required retention period,
Kantara-166	63A	5.1.1.1	17	724 - 731	This clause confuses the CSP as an entity (points 1 and 3) and its service (point 2).	The requirement actually needs to address both circumstances, i.e. cessation of the CSP's service per se, and cessation of the service because of the CSP's demise or whatever.
Kantara-167	63A	5.1.1.1	17	730, 731	This clause has nothing to do with ceasing operations, it stands at any time the CSP is in operation. It is certainly made more if the CSP is ceasing or has ceased operations (circumstances may not allow for a graceful degradation of the service).	Place this requirement elsewhere, where it will relate to ongoing operation. Point 1 appears to deal with the end of life for the CSP (or at least its service).
Kantara-168	63A	5.1.1.1	17	731	Many methods of disposing of or destroying data are insufficient.	Require conformity with NIST SP 800-88 or equivalent rigor
Kantara-169	63A	5.1.1.2	17	732	It is not clear why this is under Identity Service Documentation and Records. Should it have its own section?	5.1.x Fraud Mitigation Measures
Kantara-170	63A	5.1.1.2	17	737	Kantara-169 being said, it would be nice to consolidate all the Risk Assessment stuff in one spot, maybe in the 5.1.2.1 list?	In 5.1.2.1: 5. The CSP SHALL include any fraud mitigation measures, including any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography). 6. The CSP SHALL make a summary of its privacy risk assessment available to any organizations that use its services. The summary SHALL be in sufficient detail to enable such organizations to do due diligence.
Kantara-171	63A	5.1.2.1	18	757	unnecessary repetition or separation?	Remove - this is covered by §5.1.1.1 2)
Kantara-172	63A	5.1.2.1	18	762	A requirement that "the CSP SHALL consult the NIST Privacy Framework" is confusing. Do we mean for them to follow it? Or merely to have glanced at it? This should either be strengthened (to a measurable criteria) or removed. (or perhaps this is a good place for a "should")	In determining such measures, the CSP SHOULD consult the NIST Privacy Framework [NIST-Privacy] and NIST Special Publication [SP800-53].
Kantara-173	63A	5.1.2.1	18	762	A requirement to review risk assessments periodically is fine, as long as we are comfortable with potentially very long periods. Or quantify this to no more than, "at least annually."	quantify this to no more than, "at least annually."
Kantara-174	63A	5.1.3	19	793	As written, this section suggests the need for CSPs to collect demographic data to assess for equity. Given the requirement to minimize collection of data (800-63-4ipd §5.5), there should be no expectation that would include demographic characteristics to effectively measure equitable impact as it relates to race, religion or other similar demographics (even if optional for the subject to enter).	Recommend clarifying this section to reflect that any equity assessment use disaggregated data and does not require additional data collection, as outlined in the “Recommendations from the Equitable Data Working Group” report resulting from EO13985. Be explicit.
Kantara-175	63A	5.1.5	20	850	How can organizations effectively communicate the importance of digital identity management and the role of users in protecting their identies?	More details around user education and awareness inlcuding on how to identify potential social engineering attacks (i.e. phishing), and recommendations for organizations to provide clear and concise communication to users about the importance of digital identity management and their role in protecting their identities. For example are there any resources like the Identity Theft Resource Centre that could be leveraged in the guideline for users to reference.
Kantara-176	63A	5.1.6	21	864	What does validation mean? Does it exist? Or do we have evidence that its bound to the applicant? Would using an enrollment code to confirm an applicant has access to a address, validate the address?	This is first use of ' validated address' - what makes any of these addresses 'validated' as opposed to 'run of the mill'? Define what NIST means by validation - consider: "Enrollment codes are used to validate an address by confirming an applicant has access"
Kantara-177	63A	5.1.6	21	871	The requirement to "present a valid enrollment code to complete the identity proofing process" is not consistent with the definition of enrollment codes that only confirm access to an address. Confirming access to an address could occur at anytime in the lifecycle; potentially, well before proofing. An account could be created tying an applicant to an address; then one or more proofings', at various IALs could be performed to elevate an account to a given level.	Remove "2. The applicant shall present a valid enrollment code to complete the identity proofing process."
Kantara-178	63A	5.1.6	21	874	Our understanding is that a random six digit number has less than 20 bits of entropy. If we have said that it is a random six digit number, do we have to define the entropy? Can we have more than 6 digits? (Can we use the old wording?)	Consider revising: "Minimally, a random six digit number or equivalent entropy" Is this a legacy hang-over? Alphanumeric choice would ensure adequate entropy is achieved.
Kantara-179	63A	5.1.6	21	880	From these times, one has to presume that an enrollment code is not considered as something which binds an Applicant to a Supervised (In-person) proofing session? If that were intended then these times are not practical if the means of communicating the code is electronic (c) or d)).	Clarify this point. We cannot see any rational risk-based determination for these values, and many real-world circumstances MAY render them unreasonable for service delivery or useability. Why cannot the CSP choose their periods based on their usage model? Consider a discrete treatment of an authenticator for each use case, e.g. temporary authenticator vs confirmation of access to an address. Additionally, a new authenticator specifically for temporary authentication purposes as described here should be added into 63B
Kantara-180	63A	5.1.7	22	895	a definition of ' validated address ' is required.	If 'validated express' was defined in a concise and subsequently validatable manner, this is resolved. See Kantara-176.
Kantara-181	63A	5.1.8	23	930	independent entity' places no specific qualifications on their competence - better to use the exemplar phrasing as the actual requirements.	Consider "CSPs SHALL have all biometric algorithms tested by an accredited laboratory or research institution .."
Kantara-182	63A	5.1.8	23	932	Which demographic groups? Without specific groups, comparison is meaningless.	Consider referencing FRVT List and/or DHS demographic data/definitions.

Kantara-183	63A	5.1.8	23	935-956	While NIST specified FMR for biometric algorithms, it does not set performance requirements for Presentation Attack Detection. There are existing performance standards defined by independent third parties such as FIDO Alliance or ISO 30107.	NIST should include Imposter Attack Presentation Attack Rate of PAD level 1 and Level 2 as specified by ISO or FIDO Alliance in addition to FMR in line 935.
Kantara-184	63A	5.1.8	23	938	There will certainly be performance differences, perhaps we mean performance inequities (which we also should probably define).	CSPs SHALL employ biometric technologies that provide similar performance characteristics for applicants of different demographic groups . If performance inequities across demographic groups are discovered, CSPs SHALL act expeditiously to provide redress options to affected individuals and to close performance gaps. Adjust the performance characteristics accordingly.
Kantara-185	63A	5.1.8	23	939	For biometrics, it is most meaningful to measure objectively observable characteristics. 'Gender', while correlated with 'sex', is culturally defined and can change over time, whereas 'sex' is biologically determined and clinically observable. Similarly, while racial background and ethnicity are correlated with skin tone, they do not themselves impact biometric algorithms. So, directly measuring skin tone would be the most objective measurement.	Remove racial background, gender, ethnicity... and replace with scientific demographic groups to include sex, age, and skin tone. Sex, age and skin tone objectively impact performance.
Kantara-186	63A	5.1.8	23	943; 948	First, these are duplicative (10 and 12). Shouldn't this be qualified - it may not be in the power of the CSP to publish the results achieved by third parties? Note also that publishing results w/o context can have little meaning.	Delete #10 and Amend #12 to read: 'If the CSP performs its own performance and operational tests, it SHALL make them all publicly available" Similar amendment for #11.
Kantara-187	63A	5.1.8	23	943	Might this be construed as potentially impeding a competitive advantage? If minima were established then assessment could ensure that they were met without compromising any features of a service's advantage.	'all performance' should expressly exclude the internal functioning of algorithms, capture mechanisms, etc.' Better to state the minimal characteristics which need to be published, e.g. FMRs, etc.
Kantara-188	63A	5.1.8	23	953	Is this unsupervised or supervised (remote) or supervised (in-person), or ... ? Just an instance of uncertainty as to which proofing type(s) actually relate to this requirement	Kantara-113's proposed proofing type taxonomy would resolve this.
Kantara-189	63A	5.1.9	24-25	959-1002	Clarification on Trusted Referee certification requirements for Component Service IAL2 and Full Service IAL2 certification. Current and future potential identity proofing solution providers are likely unable or unwilling to provide the Trusted Referee requirement as the service is costly. As a result, there is likely to be a reduction in identity proofing solution providers, reducing choice for the consumer and increasing costs for Relying Parties, Government Agencies and the U.S. taxpayer.	Given that the Trusted Referee requirements are costly, to lower the risk of these unintended consequences while still obtaining the intended rise in identity assurance, in-person proofing solutions with large national footprints to support the affected population is suggested as Trusted Referee alternatives.
Kantara-190	63A	5.1.9	24	959	The intention of having a supervisor or representative of an applicant has become confusing and leaves room for intepretation..	We are requsting clarity as well more concise definitions of the defined roles and responsibilities.
Kantara-191	63A	5.1.9	24	960	Enhancement to phrasing	"promote equality of access"
Kantara-192	63A	5.1.9	24	964	How can we address individuals who do not possess and cannot obtain required identity evidence (homlessness, little to no access to computing devices, etc.)?	This calls for a Trusted Referee or applicant reference that could be remote or local and adequately identitified. It is our strong contention that all parties must be adequately identified to the same or higher xAL level and the adjudication package should maintain a digitally signed record of all parties to the transaction.
Kantara-193	63A	5.1.9	24	969-982	This is a change of the definition of "trusted referee." They are now "agents of the CSP or its partners," but were "notaries, legal guardians, medical professionals, conservators, persons with power of attorney, or some other form of trained and approved or certified individuals," who now appear to be "applicant references." This would be clearer, if the old examples were included.	Applicant references are individuals who participate in the identity proofing of an applicant in order to assist the applicant in meeting the identity proofing requirements, such as notaries, legal guardians, medical professionals, conservators, persons with power of attorney, or some other form of trained and approved or certified individuals. Such assistance may include vouching for the applicant's circumstances and actively assisting the applicant in completing the identity proofing process. Documented examples of relationships between "trusted referee" and "applicant" would be advantageous to both parties.
Kantara-194	63A	5.1.9.1	24	993	Rather than prescribing solutions to help fix the equal access and accessibility, please consider stating a requirement for CSPs to achieve the outcome of offering services to all applicants. And to describe trusted referees and applicant references as potential solutions.	In 5.1.9.1 insert a line: CSPs SHALL offer the means to facilitate the identity proofing and enrollment of individuals who are otherwise unable to meet the requirements for identity proofing to a specific IAL. Modify line 994 to read: "CSPs MAY provide for the use of trusted referees for remote identity proofing at IALs 1 and 2."
Kantara-195	63A	5.1.9.1	24	993, 1003, 1013	It has already been stated that this section includes normative clauses and normative key words are used in these sections. Is the word 'Requirements' necessary (and in other such instances). Maybe this is emblematic of the confusion between requirements which are published as guidance, and the parts which are informative and hence guidance?	This is not a consistently-applied titling practice, so remove the word 'Requirement'. See Kantara-114.
Kantara-196	63A	5.1.9.1	24	993	Serving audiences that have technical, geographic or other limitations in the process are more likely to require the services of Trusted Referee. In these scenarios we want to best ensure the Trusted Referee is properly empowered to achieve transaction closure with the individual. The use of trusted referees should be an alternative available to increase equity and access to services for some, but should not be required where the system alone can suffice.	Add more specifics about the capabilities Trusted Referees should have under 800-63-4. Specifically, are they allowed to make risk based decisions that are associated with risks observed around the transaction (telephony measures, device reputation, etc.) rather than purely related to the evidence presented?
Kantara-197	63A	5.1.9.1	24	994 - 996	The requirement to 'provide an option' demands that the capability be there, and that it is the service user who exercises the option to use that facility or not. Yet line 996 says "WHERE this is offered", so apparently the provision is not mandatory. Why is this seemingly being forced upon CSPs?	Delete "CSPs SHALL provide the option for the use of trusted referees for remote identity proofing at IALs 1 and 2." or Modify 994 to state "CSPs SHOULD provide Supervisors for Supervised (Remote) proofing at IAL1 and IAL2". The rest then flows.
Kantara-198	63A	5.1.9.1	24	994	What is it that makes a Trusted Referee different from the personnel referred-to in Kantara-152? These persons are actually not acting as referees, they do not know the Applicant - they are acting in a Supervisory function. Let's call them that.	Deal with the requirements for Supervisors in a single place
Kantara-199	63A	5.1.9.1	25	999 - 1000	Shouldn't this ability to make 'risk-based' decisions require that the net risk is the same ... and are these persons really going to be able to make such decisions. The reason for inclusion is understood, but it seems to be a potential weakness, a diminution of the level of risk associated with the proofing process, unless very clear guidelines are given.	It would be far better to: a) phrase this so as to allow Supervisors to make decisions based upon a clear framework of optional paths open to them; and b) require the CSP to develop such a framework (which would allows a more uniform and sophisticated risk-based approach to be determined and more uniformly applied).
Kantara-200	63A	5.1.9.1	25	999	For CSP referees and/or agents to make risk-based decisions, training as well as a systematic risk-based approach classification should be deployed to facilitate and support risk-based decisions.	Training, classification or risk/s, reporting, decision processing, reporting, and retention should be addressed to mitigate potential claims of exclusivity or inequity. Further, Supervisors should be trained equally to detect attempts to fraudulently pass through the proofing process.
Kantara-201	63A	5.1.9.1	25	1002	Trusted Referees are needed to achieve equity, however there is always a chance that the ability to bypass evidentiary requirements will lead to fraud and abuse, including through bribery. To mitigate this it is important to maintaining an association between the Trusted Referee and the applicant in the CSPs records.	Add a further requirement that the CSP maintain a link between the Trusted Referee and the applicant in their records.

Kantara-202	63A	5.1.9.2	25	1003-1012	When allowing and using an applicant reference chain-of-custody rules should apply	Include the same xAL process and data record used for the applicant along with the applicant reference within the session, retention, and submission package so that there is a chain-of-custody binding the enrollment/proofing source to the adjudication and issuance. I.e., there must be a means for someone to review and identify that an applicant reference was validated and they in effect become one of the strong forms of evidence for that identity session.
Kantara-203	63A	5.1.9.2	25	1004	IF "Applicant references are individuals who participate in the identity proofing of an applicant in order to assist the applicant in meeting the identity proofing requirements. Such assistance may include vouching for the applicant's circumstances and actively assisting the applicant in completing the identity proofing process" but IAL3 requires in-person (or remote in-person); it is unclear what role an applicant reference would have in the proofing. That is to say applicant references would not work at IAL3.	Add a further requirement that the CSP maintain a record between the CSP's Supervisor (Trusted Referee) and the applicant in their records.
Kantara-204	63A	5.1.9.2	25	1008	While Applicant References are needed to achieve more equitable outcomes, it is a position that is subject to abuse. A higher IAL and the maintenance of a link between the Applicant Reference and the applicant would mitigate that risk.	Change to "...at an IAL2 or higher." And add a requirement that the CSP maintain an association between the Applicant Reference and the applicant.
Kantara-205	63A	5.2	25	1024 - 1030	A statement is needed to say that the proofing mode and the proofing levels are too entangled. We need to suggest a method of identifiying a more useful matrix.	NIST has chosen to include various modes of identity proofing interleaved, however these methods vary by implementations. Using this method causes conflicts in both reading and intepretation.
Kantara-206	63A	5.2	25	1027	The term "CSP operator-assisted remote process" is confusing. This is understood to be a supervised remote process, albeit without the requirements of 5.5.8. Call them BOTH "remote interactions", but ID 1 as IAL3. Can we link this back to the old terms?	5.2. Identity Proofing Process This document provides requirements that apply to several different identity proofing methods. These possible methods include: • A fully automated, remote process (or unsupervised); • A remote interaction with the applicant and a CSP Supervisor • A combination of automated and remote interaction; • An in-person process, where the Supervisor is physically co-located with the applicant; and • An IAL3 remote interaction Proofing process (conforming to the IAL3 remote interaction requirements). Identity proofing at IAL1 and IAL2 allow for any of the these processes
Kantara-207	63A	5.2	26	1032	This appears to use 'IAL3 Supervised Remote' as a title of a proofing type. The need to prefix with the IAL reference shouldn't be necessary - the section addressing IAL3 proofing requirements ought to make the necessary distinction between such a type at this level versus at any other level.	describing proofing types needs no 'IAL - exclusive' labeling - let the definition of specific requirements do that.
Kantara-208	63A	5.3	26	1035, 1090, 1142	All three sections addressing requirements at IAL1, 2 and 3 respectively. Any references to proofing types would need to be updated if NIST implements a more streamlined proofing type taxonomy, as referenced in Kantara-113.	See Kantara-113 and proofing type taxonomy tab of document.
Kantara-209	63A	5.3	26	1035	NIST clearly is looking to allow for more business to be conducted without the need of the biometric elements prevalent in IAL2 proofing. There is a need 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 at IAL2 (and authenticated at AAL2). IAL1 evidence, combined with a lack of negative/concerning metadata, should allow for transactions that previously required IAL2 proofing to be performed at lower levels. 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.	Consider risk-based approaches that would allow service providers to perform more transactions at IAL1. Risk assessments regarding both evidence presented, as well as situational analysis of the interaction (device, IP, networking, etc.), would combine to provide guidance to the CSP.
Kantara-210	63A	5.3	26	1039	typo	"false negatives and applicant departures "
Kantara-211	63A	5.3	26	1044	redundant text	The following requirements apply to all CSPs providing identity proofing and enrollment services at IAL1.
Kantara-212	63A	5.3.1	26	1046	A comparison of 5.3.1, 5.4.1 and 5.5.1 suggests that this is a general requirement?	Provide a single clause addressing this
Kantara-213	63A	5.3.1	26	1048	the text of 5.3.1 is, in effect, an unlimited list with no constraints	please replace "Acceptable means include, but are not limited to" with the words "for example"
Kantara-214	63A	5.3.2.1	26	1052	Change in Rev-4 - Modified IAL1 to require validation of 1 piece of FAIR evidence AND 1 piece of STRONG evidence, or 1 piece of SUPERIOR evidence. Verification can be achieved by mailing to the validated address. Introduction of the changes to IAL1 to allow for a lower risk level of assurance provides the opportunity to improve the ability to manage risk and mission needs beyond the former IAL2 requirements from 800-63-3.	We highly recommend an approach to incorporate a risk model as STRONG evidence. At IAL1 or IAL2, identity risks can be effectively managed without mandating use of strong evidence for ALL subjects. By combining multiple pieces of fair evidence in conjunction with risk signals related to identity theft or synthetic identity fraud, organizations can more effectively meet their mission delivery needs and manage cybersecurity risk than with what is currently rated as STRONG evidence. Examples of fraud risk signals include, but are not limited to, PII data recent activity, Phone account and activity attributes, email data/attributes from ISPs, device and IP address review for high-risk indicators, anomalous credit bureau data, and behavioral characteristics. The use of these signals within advanced analytics to create an Identity Confidence model has proven extremely powerful in effectively reducing cybersecurity risk while simultaneously minimizing impact to good subjects within the private sector for years. Including an Identity Confidence model validation option better enables organizations to meet both their mission delivery and cybersecurity risk needs. It is critical to ensure any use of fraud risk signals in coordination with identity proofing include empirical evidence of its effectiveness in addressing the cybersecurity risk (false negative errors) as well as mission delivery risk (false positive errors). This can generally be shown using a variety of model performance and validation analytic techniques (e.g., Receiver Operator Characteristic Curve, Area Under the Curve, KS test, GeNIe). These techniques inherently require effective measurement systems to determine subjects' disposition as either good or bad. An alternative method of measuring model performance where there is limited performance data can be random sampling to get a high level of confidence related to the model's performance. With this approach, an Identity Confidence Score could be applied to subjects as an initial, passive option to risk rank the population. Where the confidence score renders the Identity Confidence risk LOW, then the CSP can require the current STRONG evidence to complete identity proofing.
Kantara-215	63A	5.3.2.1	26	1056	If the basis of IAL1 is equity by allowing "a range of acceptable techniques...", most underserved population would not have in possession what would be considered acceptable as STRONG evidence making the basis of IAL1 as being more equity-based possibly, if not likely, moot.	Consider risk-based approaches that would allow service providers to perform more transactions at IAL1. Risk assessments regarding both evidence presented, as well as situational analysis of the interaction (device, IP, networking, etc.), would combine to provide guidance to the CSP.

Kantara-216	63A	5.3.2.2	26	1057 - 1060	This also has limited normative value - as a 'MAY', it will be largely ignored and cannot be assessed. This comment relates to the same clause at each IAL.	It (and its peers) would be better moved to a place where it would be simply informative.
Kantara-217	63A	5.3.3	27	1061	What are 'Core Attributes' - We understand that they might be something that an observer would recognize when they see them, but different observers may not agree …	Core attributes need to be identified, preferably for each type of common evidence encountered, such as for driver's licenses and passports.
Kantara-218	63A	5.3.3	27	1068 - 1069	This clause will not be feasible for Unsupervised proofing (of any kind) - hopefully by definition	Qualify it as "When performing Supervised proofing of any type the CSP SHALL …"
Kantara-219	63A	5.3.3	27	1069	Use consistent term for 'trained personnel'	update "trained personnel" to Supervisors; ensure consistency througout document
Kantara-220	63A	5.3.3	27	1068-1069	Given that two industries (financial and utility) could serve as issuing source of Fair evidence documents, and thus resulting to about 13K entities independent of each other, there would at least be ~13K possible formats representing acceptable Fair evidence documents and requiring a trained personnel to be able to visually validate the genuineness of a huge number of documents, in which there are no standard authenticity guidelines, is a challenge.	We highly recommend an approach to incorporate a risk model as STRONG evidence. At IAL1 or IAL2, identity risks can be effectively managed without mandating use of strong evidence for ALL subjects. By combining multiple pieces of fair evidence in conjunction with risk signals related to identity theft or synthetic identity fraud, organizations can more effectively meet their mission delivery needs and manage cybersecurity risk than with what is currently rated as STRONG evidence. Examples of fraud risk signals include, but are not limited to, PII data recent activity, Phone account and activity attributes, email data/attributes from ISPs, device and IP address review for high-risk indicators, anomalous credit bureau data, and behavioral characteristics. The use of these signals within advanced analytics to create an Identity Confidence model has proven extremely powerful in effectively reducing cybersecurity risk while simultaneously minimizing impact to good subjects within the private sector for years. Including an Identity Confidence model validation option better enables organizations to meet both their mission delivery and cybersecurity risk needs. It is critical to ensure any use of fraud risk signals in coordination with identity proofing include empirical evidence of its effectiveness in addressing the cybersecurity risk (false negative errors) as well as mission delivery risk (false positive errors). This can generally be shown using a variety of model performance and validation analytic techniques (e.g., Receiver Operator Characteristic Curve, Area Under the Curve, KS test, GeNIe). These techniques inherently require effective measurement systems to determine subjects' disposition as either good or bad. An alternative method of measuring model performance where there is limited performance data can be random sampling to get a high level of confidence related to the model's performance. With this approach, an Identity Confidence Score could be applied to subjects as an initial, passive option to risk rank the population. Where the confidence score renders the Identity Confidence risk LOW, then the CSP can require the current STRONG evidence to complete identity proofing.
Kantara-221	63A	5.3.3	27	1071	How does one validate the accuracy of account or reference numbers for FAIR evidence, when there is no credible source for the majority of those numbers?	Remove the FAIR evidence validation requirements since it isn't possible to meet them.
Kantara-222	63A	5.3.3	27	1076; 1124; 1182	The phrase "For added assurance," is unnecessary - the fact that it is a normative clause is all that matters.	For added assurance, tThe CSP SHALL evaluate the core attributes, as validated by various sources, for overall consistency. Similar instances could also be simplified.
Kantara-223	63A	5.3.3	27	1084	The current sentence precludes the use of AAL2 and FAL2	Add 'and higher' to both the AAL and FAL requirements
Kantara-224	63A	5.3.3	27	1084	Should AAL be IAL?	Change to 'IAL1/AAL1' or higher'. As its written a gmail account would be acceptable.
Kantara-225	63A	5.3.4	27	1086	When used for identity verification, the enrollment code needs to be sent to a physical address controlled by the applicant.	Add a requirement that the enrollment code is sent to either a postal address or phone number strongly associated with the applicant, through an authoritative or credible source.
Kantara-226	63A	5.3.4	27	1086	typo	"see Sec 5.1.6"
Kantara-227	63A	5.4.2	28	1102	Change in Rev-4 - Modified IAL2 to require validation of 1 piece of FAIR evidence AND 1 piece of STRONG evidence, or 1 piece of SUPERIOR evidence. Verification can be achieved by comparison of a collected biometric characteristic to STRONG or SUPERIOR evidence. Introduction of the changes to IAL2 to allow for one less piece of FAIR evidence provides the opportunity to improve the ability to manage risk and mission needs beyond the former IAL2 requirements from 800-63-3. However, requirement for existing STRONG evidence (aka gov't issued ID) with biometric matching will impact equity and mission delivery needs.	"We highly recommend an approach to incorporate a risk model as STRONG evidence. At IAL1 or IAL2, identity risks can be effectively managed without mandating use of strong evidence for ALL subjects. By combining multiple pieces of fair evidence in conjunction with risk signals related to identity theft or synthetic identity fraud, organizations can more effectively meet their mission delivery needs and manage cybersecurity risk than with what is currently rated as STRONG evidence. Examples of fraud risk signals include, but are not limited to, PII data recent activity, Phone account and activity attributes, email data/attributes from ISPs, device and IP address review for high-risk indicators, anomalous credit bureau data, and behavioral characteristics. The use of these signals within advanced analytics to create an Identity Confidence model has proven extremely powerful in effectively reducing cybersecurity risk while simultaneously minimizing impact to good subjects within the private sector for years. Including an Identity Confidence model validation option better enables organizations to meet both their mission delivery and cybersecurity risk needs. It is critical to ensure any use of fraud risk signals in coordination with identity proofing include empirical evidence of its effectiveness in addressing the cybersecurity risk (false negative errors) as well as mission delivery risk (false positive errors). This can generally be shown using a variety of model performance and validation analytic techniques (e.g., Receiver Operator Characteristic Curve, Area Under the Curve, KS test, GeNIe). These techniques inherently require effective measurement systems to determine subjects' disposition as either good or bad. An alternative method of measuring model performance where there is limited performance data can be random sampling to get a high level of confidence related to the model's performance. With this approach, an Identity Confidence Score could be applied to subjects as an initial, passive option to risk rank the population. Where the confidence score renders the Identity Confidence risk LOW, then the CSP can require the current STRONG evidence to complete identity proofing. "
Kantara-228	63A	5.4.2.1	28	1106	1 x STRONG + 1 x FAIR appears to have dropped a second FAIR requirement from rev.3. This illustrates the lack of any published risk assessment which might justify this change, which could arguably be a weakening of the required rigor.	It would be very constructive and illuminating if NIST would put forward some concrete justification for any of its normative requirements for strength of evidence, both for the present draft and for the current revision. It is very difficult to make any judgements on these requirements, or indeed for comparable alternatives (where agencies are permitted to go down that path) since there is no stated risk quantification against which any determination of comparison or comparability can be made.
Kantara-229	63A	5.4.2.1	28	1106	FAIR evidence is easy to forge and cannot be validated, so is unlikely to improve confidence in an identity. At the same time, it is likely to cause user inconvenience and increase the cost of identity proofing.	Recommend removing FAIR evidence as a requirement when STRONG evidence is presented.

Kantara-230	63A	5.4.3	28	1117 - 1118	What happened to validation of FAIR evidence? Is it no longer required or is it meant to be embraced by this phrase??	If FAIR evidence is indeed intended to be included, be specific: "The CSP SHALL validate the core attributes from all pieces of evidence at all strengths collected by" Otherwise, we stand by Kantara-229 that FAIR evidence is removed as a requirement when STRONG evidence is presented.
Kantara-231	63A	5.4.3	28	1119	Account or reference numbers for FAIR evidence cannot be reliably validated. There are about 1600 electrical utilities in the United States (https://www.statista.com/topics/2597/electric-utilities/#topicOverview). What about school ID's? There are about 27K high schools and 4k colleges/universities in the US. How will those ID's be validated? There is no credible source for either.	Remove FAIR evidence validation requirements from Unsupervised Proofing. For this line, remove the validation of account and reference numbers.
Kantara-232	63A	5.4.4.1	29	1128	Based on what evidence was option 1 (biometric) and option 2 (account verification) determined to be equivalent from a security and fraud reduction perspective?	Rather than provide two options at very different confidence levels, divide IAL2 into two sub categories - with and without biometrics. For highly sensitive services and functions agencies can then have the option to mandate the biometric option.
Kantara-233	63A	5.4.4.1	29	1130	"Comparison of a collected biometric characteristic, such as a facial image, to the associated reference biometric contained on a piece of presented SUPERIOR or STRONG evidence" Is IAL2 required to "collect" a biometric? IAL3 includes this requirement in a specific clause (5.5.6) but IAL2 does not. Since 5.4.3 allows visual inspection (comparing someone to the picture on this license), it is assumed there is no need to collect.	"Comparison of a collected biometric characteristic, such as a facial image, to the associated reference biometric contained on a piece of presented SUPERIOR or STRONG evidence"
Kantara-234	63A	5.4.4.1	29	1133	This requirement could be met with a gmail account that has MFA enabled.	Change to "Demonstrate association with an IAL2 or higher digital account..."
Kantara-235	63A	5.4.5	29	1141	To reduce fraud, notification of proofing should be sent to a postal address that is strongly associated with the purported applicant in an authoritative source.	Add that requirement.
Kantara-236	63A	5.5	29	1147	Notwithstanding prior intent not to raise matters of proofing type terminology, the notion of 'in-person' including 'remote' is very confusing.	See Kantara-113 and proofing type taxonomy tab of document.
Kantara-237	63A	5.5.3	30	1164	Section titling (of this and subordinate heading phrasing) differs from its IAL1 and 2 peers, easily noticable in Table of Contents.	5.5.3 should be named Evidence and Core Attributes Validation Requirements (similar to 5.3.3 and 5.4.3) Consider if 5.5.3.1 and 5.5.3.2 are adequately named with this change.
Kantara-238	63A	5.4.3, 5.5.3	30	1165, 1176	Discussions of the IALs should be presented in a structurally consistent way. 5.4.3 and 5.5.3 should be formated consistently	Present consistently - separate 5.4.3
Kantara-239	63A	5.5.3.1	30	1165	By only including validation requirements for IAL3, there is an implication that there are no such requirements for IAL1 and IAL2.	Add 5.3.3 and 5.3.4 "Evidence Validation Requirements." These requirements are very general, but serve to indicate that the evidence must still be evaluated somehow. 5.x.3 Evidence Validation Requirements The CSP SHALL validate the genuineness of each piece of evidence by one of the following: 1. Visual inspection by trained personnel 2. The use of technologies that can review and evaluate the evidence data
Kantara-240	63A	5.5.3.2	30	1180, 1181	Basically item 2) is saying "same as above", right? It is unclear why crypto features are specifically pointed-out , since they would (at least theoretically) be considered to be core attributes ... but this term is not well defined, so therefore this is a subtle pointer to crypto features being a core attribute?	See Kantara-217: Core attributes need to be identified, preferably for each type of common evidence encountered, such as for driver's licenses and passports.
Kantara-241	63A	5.5.4	31	1184	Repetitive text could be removed to simplify text - add reference instead	State only "The requirements stated in §5.4.4.1 apply." This applied throughout the document could make for clearer text.
Kantara-242	63A	5.5.4	31	1190	IAL3 should provide a very high confidence in the identity of the applicant so should require biometric comparison.	Remove option 2.
Kantara-243	63A	5.5.5	31	1194	Section 5.1.7 does not require that the address is strongly associated with the applicant in a credible or higher source, which is needed for this step to be meaningful.	Add the requirement
Kantara-244	63A	5.5.7	31	1198	This section is specific to Biometric collection	Should be incorporated into 5.5.6.
Kantara-245	63A	5.5.7	31	1200 - 1202	"An in-person interaction between the applicant and a CSP operator" - so Supervised (In-person/co-located) proofing? "A remote interaction with the applicant, supervised by an operator" - so Supervised (Remote) [and does it matter whether the CSP's or the User's hardware/firmware is employed?] Additionally, why is the phrasing emphasized in red different in each bulleted item? Is there intended to be some subtle difference or is this lack of using consistent terms in a consistent manner? It seems that in each case a Supervisor would have to be employed and the use of agreed taxonomic proofing titles would be hugely beneficial.	Re-state in accordance with changes to adopt a proofing type taxonomy, define and adhere to the term 'Supervisor' and remove bullets.
Kantara-246	63A	5.5.8	31	1209	Remote proofing, at any level might require the applicant and operator to be continuously present, operators to have undergone training, and a secured channel.	Consider adding section for IAL1 and IAL2
Kantara-247	63A	5.5.8	31	1214 - 1216	Exemplar in normative statement	Remove "for example, by a continuous high-resolution video transmission of the applicant."- possibly include as a note.
Kantara-248	63A	5.5.8	31	1215	What should occur if an applicant leaves the identity proofing session? E.g., 1 second, 30 seconds, longer?	Suggest that a mitigation or guidance path be prescribed such that if an applicant leaves the view of the SRIP agent during an identity proofing session e.g., the session must be terminated with immediate effect along with a note indicating the causative factor. The CSP may prescribe the method of handling should the applicant leave the session for X period of time.
Kantara-249	63A	5.5.8	32	1217, 1218	points 1) and 2) appear to address the same requirement, just with different phrasing (e.g. does it matter if it is 'the CSP' or 'live operator'? Consistent with other comments, 'Supervisor' would appear to be the appropriate term.	Resolve to a single clause. Consider updating all instances of 'live operator' or 'operator' to 'supervisor' as mentioned in numerous other comments in this file.
Kantara-250	63A	5.5.8	32	1217	What is meant by 'participate' and for the 'entirety of the identity proofing session'? What is the definition of participation in this context? What is the defintion of an entire identity proofing session? Is it necessary for the operator to verbally engage with the user? Should the operator actively participate and monitor the placement of paper documents for scanning or typing of data?	Consider questions and provide guidance
Kantara-251	63A	5.5.8	32	1221	Does the biometric capture require an integrated scanner? If not, it may be possible to perform 5.5.4 with just video.	Add qualifiers
Kantara-252	63A	5.5.8	32	1221	Collection of fingerprint biometrics should mandate the use of FBI approved fingerprint capture devices and algorithms.	Collection of fingerprints SHALL use FBI approved for NGI and IQS as defined on the FBI APL in accordance with https://fbibiospecs.fbi.gov/certifications-1/faq
Kantara-253	63A	5.5.8	32	1222	Further definition of integrated is required.	Integrated directly with the compute platform performing the verification (so as to avoid man-in-the-middle attacks or other subversion), employing anti-tampering, no exposed cabling/wires, built in to a secured enclosure?

Kantara-254	63A	5.5.8	32	1226	Could equipment delivered by the organization to a user/applicant (e.g., a company laptop or phone) meet this requirement?	Include use case
Kantara-255	63A	5.5.8	32	1231	It appears that #7 is addressed in 5.1.4	delete duplication
Kantara-256	63A	5.5.8	32	1232	Are there any minimum security requirements for this channel?	Add clear requirements
Kantara-257	63A	5.6	32	1234	Table 1 - first row - 'Presence': this is confusing, not least because of the inconsistent terminology of the preceding text, as noted in several comments concerning the need for clarity on proofing types.	Explicitly state the permitted proofing types (headings in bold): Requirement: Proofing type IAL1: Unsupervised OR Supervised (Remote) OR Supervised (Co-located) IAL2: Same as IAL1 IAL3: Supervised (Remote) OR Supervised (Co-located)
Kantara-258	63A	5.6	32	1234	Table 1 - a consideration in establishing a proofing capability apart from the proofing type could be the technology involved - its specific performance, how it is configured, perhaps how it is physically protected, etc. This is not adequately brought out in the text, and should be both addressed and therefore included in this table.	Explicitly state the applicable technology by inserting a new row into the table (as row 2) (headings in bold): Requirement: Supervised Remote IAL1: No stipulation IAL2: Same as IAL1 IAL3: Controlled environment This topic needs to be addressed in detail in each IAL section in §5.
Kantara-259	63A	5.6	32	1234	Some entries in this standard are repeated for any given requirement but one has to read the full text to determine whether they are actually the same. The same requirement could be determined with a simple statement to that effect.	Where the requirement for any given IAL is the same as the preceding IAL, simply state so, i.e. "Same as IALx". This actually makes it much easier to review and appreciate this quality, rather than comparing two paragraphs of text. As noted, this practice should also be applied in the body of the text.
Kantara-260	63A	6.1	34	1237	This may not be the place to express such a requirement but there should also be a unique id for the service - where is that required, and is that unique for the broad service or does it have xAL/policy qualifiers? This becomes relevant for AAL and FAL but the need for uniqueness of the identity-proofing service, or at least that which binds the id to its credentials, is necessary.	Create at an appropriate point (possibly not in this document) a requirement to the effect of: "The CSP SHALL assign a unique identifier to each discrete proofing service which it operates, including any specific policy identifiers where these are pertinent to the use of the identity."
Kantara-261	63A	6.1	34	1238-1242	"With the exception of identity proofing for the purposes of providing one-time access .....". This may be a policy decision on the part of the CSP, the risk resides in data retention.	CSP discretion should prevail here - the SORN and data retention is in their control. Additionally, consideration should be given to a basic retention for "one-time" requests, as there is no guarantee the access need / request is a "one time" thing. In different proofing use cases, a table is recommended for "suggested/informative" retention periods.
Kantara-262	63A	6.1	34	1257	This is quite vague and hence open to interpretation and thus leading to inconsistent implementations. E.g. is it sufficient to record 'DL' in each case ("Yes, we used a DL, we validated the DL") or must it go to the level of discrete info fields from each piece of identity evidence?	At the least, minima should be specified to the extent possible - issuing authy, iss athy's unique evidence ident, account ref., ... (depending on source)
Kantara-263	63A	6.1	34	1262	Move to 5.1.2.1 (consolidate all the Risk Assessment stuff in one spot)	In 5.1.2.1: 5. The CSP SHALL conduct a include any fraud mitigation measures, including any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography). 6. The CSP SHALL include the processing, retention, or disclosure of any personal information maintained in the subscriber account described in 6.1 7. The CSP SHALL make a summary of its privacy risk assessment available to any organizations that use its services. The summary SHALL be in sufficient detail to enable such organizations to do due diligence.
Kantara-264	63A	6.2	35	1265	Should this apply at IAL1, where user may only have an AAL1 authenticator?	
Kantara-265	63A	6.2	35	1268, 1269	If this refers to the account maintained by the CSP does this not imply that the CSP maintaining this info also provides the authentication? What if not? It could be another authorized CSP seeking this access obo the subject.	Resolve
Kantara-266	63A	6.3.1	35	1274, 1275	Redundant - already stated in §6.1	Remove or simply reference §6.1
Kantara-267	63A	7	37	1313.5	Table 2 - typo "in order claim"	Change to "in order to claim"
Kantara-268	63A	7.1	38	1319.5	Table 3 - typos "technology.CSP", "indications or malicious traffic", "Death Master File).CSP"	Change: ""technology. CSP" and "indications of malicious traffic", "Death Master File). CSP"
Kantara-269	63A	8.4	42	1421	A SHALL would provide greater protection against fraud. If this isn't implemented bad actors could use identity proofing as a validation service.	Change "but should not inform the applicant" to "but SHALL NOT inform the applicant"
Kantara-270	63A	9.2.	46	1537-1542	clarify what 'necessary information (e.g. required documentation)' means	Provide an exhaustive list of documentations that are acceptable, and then provide an acceptable validation processes.
Kantara-271	63A	9.3	47	1593	Where applicable, provide a parallel run of the process on self-help step-by-step auxiliary screen or video recording to guide subjects during enrollment.	consideration
Kantara-272	63A	9.3	48	1643	Session-End confirmation can prompt subject to select a method (email, text message, etc.) to deliver narrative/instructions on the next step.	consideration
Kantara-273	63A	9.3	49	1676	How can organizations manage the risk associated with the use of biometric authentication? Biometric authentication is becoming increasingly popular as a factor for high-assurance authentication, but also introduces unique privacy and security considerations. Please emphasize/clarify this section.	Identify effective approaches for managing the risks associated with biometric authentication, such as ensuring that biometric data is properly protected and that users are fully informed about the collection and use of their biometric data.
Kantara-274	63A	10.3	53	1783	Addition of augmented lighting may assist in capturing a broader range of persons.	consideration
Kantara-275	63A	10.3	53	1802	An additional mitigation would be to fail over to a second algorithm, ideally one that performs better than the primary algorithm for certain populations.	Add that suggestion.
Kantara-276	63A	10.3	54	1812	Another mitigation is to have the biometric verification done algorithmically when in person has failed, since the best algorithms perform better than people.	Add that suggestion.

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:	*Kantara Initiative, Inc.*
Name of Submitter/POC:	*Identity Assurance Work Group*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
Kantara-277	63B	Whole doc / set	0	0	Language is causing market confusion. To the providers it is confusing if it is guidance or a requirement. All volumes of this text are presented in contradictory ways ("These guidelines provide technical requirements ...") and in §1 ("This publication [provides] technical guidelines ...", "This document provides requirements ..."). The terminology is inconsistent. Requirements define something that one has to do, whereas guidance is purely informational, to be taken or ignored at will and without consequence. It is noted that the main body of the work contains a mix of informative material and presumably normative material which uses the specific capitalized key words 'SHALL', 'SHOULD' and 'MAY' in a very specific style of presentation. The intent of which is assumed to take on the meanings imparted to these words by RFC 2119, a practice widely adopted amongst SDOs (see also ISO Directives Part 2 App.H). This dichotomy should be resolved.	Determine if these are requirements or guidelines and make the necessary changes to each volume to reflect this change to state clearly that the document defines [normative] requirements [using key words as defined in RFC 2119] whilst providing supporting, explanatory and informative guidance. Implicit in this suggested change is that all references throughout the document to 'guidance' need to be reviewed to determine whether they are truly informative as opposed to being actual normative requirements.
Kantara-278	63B	Whole doc / set	0	0	The structure of the document does not lend itself to easy determination of: a) which clauses are actually expressing normative requirements; and b) what are discrete normative requirements. This is evidenced by no consistency in style regarding whether informative discussion precedes normative requirements and by single paragraphs which bear both normative and informative text. This weakens the utility of the document [set] in either its use as an educational/informative source or as a set of formal requirements.	1 - Express each normative requirement as a distinct clause; 2 - Give each such clause a unique reference; 3 - Give the user a very clear means to determine the status of a passage of text - i.e. exclusively normative or informative. It is noted that adopting a presentational distinction would be an easier solution to achieving much greater presentational clarity than trying to extract and regroup all passages of one type or another.
Kantara-279	63B	4	6	439	This requirement means that almost all publicly facing applications will require AAL2, from a low/limited impact service where a single individual checks the status of their benefits application, to a service where a DI error could lead to serious consequences, such as an attorney managing multiple beneficiary claims. Yet, the authentication control for both would be AAL2. To meet the needs of the general population, and to implement controls commensurate with the risk, phishing resistant MFA cannot be required for Low/Limited applications, however for applications where a DI error has more serious consequences, phishing resistance should be required.	Recommend that AAL2 be subdivided into two categories - phishing-resistant optional and phishing-resistant mandatory. Having the option to require phishing-resistance is necessary to protect some data sets, however without requiring the separate levels the option may not be made available through the leading CSPs which means it won't, in practice, be available to agencies and everything will continue to be phishing-resistant optional.
Kantara-280	63B	4	6	440	"personal" information excludes many types of sensitive and valuable informatoin, such as proprietary business data and financials	Change 'personal' to 'sensitive' or 'highly sensitive'
Kantara-281	63B	4.1.2.	7	460	"SHALL use approved cryptography" lacks specificity. Approved by whom?	Change to "cryptography approved for use in the Federal Government by NIST" for clarity.
Kantara-282	63B	5.1.1.1.	14	678	"If the CSP disallows" allows the CSP to allow commonly used and expected passwords and still declare itself AAL2 compliant.	Recommend that this be made into a requirement 'The CSP SHALL disallow the use of memorized secrets that are commonly used, expected, or known to be compromised.'
Kantara-283	63B	5.1.1.2.	16	733	"Verifiers SHALL NOT..prohibiting consecutively repeated characters". This is effectively mandating that such insecure passwords as '88888888' be allowed.	Remove "or prohibiting consecutively repeated characters" as an example.
Kantara-284	63B	5.1.1.2.	16	766 & 811	"The salt SHALL be ... chosen arbitrarily" allows for the use of predictable salt values.	Recommend changing this to 'the salt SHALL...be generated by a NIST-approved RNG [SP800-90A]'.
Kantara-285	63B	5.1.3	18	819	This section does not include any 'SHALL' statements so reads as informative, yet is not labeled as such.	Recommend making any requirements clear by using explicitly 'SHALL' statements, or by clearly marking the section as informative.
Kantara-286	63B	5.1.3.1	21	854	"SHALL be encrypted" - are there any requirements for the encryption?	Make the encryption requirements explicit
Kantara-287	63B	5.1.3.1	21	864	Suitably secure' is quite vague.	Recommend making a clear requirement for the security.
Kantara-288	63B	5.1.3.1	21	869	"device SHOULD NOT display the authentication secret while it is locked by the owner". Is there a reason for not making this a 'SHALL'?	
Kantara-289	63B	5.1.3.2	22	882	Does an application need to meet certain requirements to be considered 'secure'?	
Kantara-290	63B	5.1.4.1	24	969 & 1024	"If a subscriber needs to change the device used for a software-based OTP authenticator, they SHOULD bind the authenticator application on the new device to their subscriber account". This is a device-based authenticator, so when the device is changed rebinding needs to occur.	Recommend changing this to a 'SHALL'
Kantara-291	63B	5.1.7.1	28	1100 & 1186	Although this implies that the key was generated on the device, that should be made explicit.	Change to 'that SHALL be generated on the device and SHALL NOT be exportable'.
Kantara-292	63B	5.1.7.1	28	1103	What, exactly, makes a processor 'suitably secure'?	Provide requirements.
Kantara-293	63B	5.1.8.1	29	1156	To avoid confusion with conformance of the Guidelines we recommend that NIST eliminate the practice of including back links/references to preceding requirements. In this case Sec. 5.2.12. It would be much clearer to just restate the full requirements for each authenticator. This will increase the number of pages, but that should not be a factor. Clarity is more important.	eliminate the practice of including back links/references to preceding requirements.
Kantara-294	63B	5.1.8.1	29	1157	Typo: 'requirementss'	Correct.
Kantara-295	63B	5.2.2	31	1235	100 consecutive failed authentication attempts on a single subscriber account seems to be way too permissive and poses a risk to the subsriber. Why is this number not a lot less?	We think up to 5 consecutive fails with a count-down prompting subject of the number of attempts remaining before locking the session or prompting other methods for verification.
Kantara-296	63B	5.2.3	33	1303	"Certification by an approved accreditation authority" - Approved by who?	Clarity is needed
Kantara-297	63B	6.1	41	1583	"for provisioning the associated keys " Not all authenticators utilize keys	Change to "any associated keys"
Kantara-298	63B	6.1.2.3	44	1669	"accounts that have not been identity proofed (i.e., without IAL)". This is IAL0.	Update to inlcude the term IAL0
Kantara-299	63B	6.1.2.3	44	1688	10 minutes may not be sufficient in areas with poor cell service.	consider increasing time

Kantara-300	63B	6.1.2.3	44	1689	Recommend that email not be allowed for AAL2 or above. Email addresses may not be sufficiently protected and demonstrate no physical control or access requirement, unlike phones & physical mailboxes.	Recommend that email not be allowed for AAL2 or above.
Kantara-301	63B	6.2	46	1763	Recommend changing this to a SHALL. Why wouldn't this be done?	Recommend changing this to a SHALL.
Kantara-302	63B	6.2	46	1764	Suggest changing to 'following detection of compromise" for clarity.	Suggest changing to 'following detection of compromise" for clarity.
Kantara-303	63B	6.2	47	1773	Recommend that email should NOT be used as an 'address of record'. It's often an IAL1/AAL1 account, or less.	Remove email
Kantara-304	63B	7.1.1	50	1870	Recommend changing this to 'SHALL NOT' to protect PII.	Recommend changing this to 'SHALL NOT' to protect PII.

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:	*Kantara Initiative, Inc.*
Name of Submitter/POC:	*Identity Assurance Work Group*
Email Address of Submitter/POC	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
Kantara-305	63C	Whole doc / set	0	0	Language is causing market confusion. To the providers it is confusing if it is guidance or a requirement. All volumes of this text are presented in contradictory ways ("These guidelines provide technical requirements ...") and in §1 ("This publication [provides] technical guidelines ...", "This document provides requirements ..."). The terminology is inconsistent. Requirements define something that one has to do, whereas guidance is purely informational, to be taken or ignored at will and without consequence. It is noted that the main body of the work contains a mix of informative material and presumably normative material which uses the specific capitalized key words 'SHALL', 'SHOULD' and 'MAY' in a very specific style of presentation. The intent of which is assumed to take on the meanings imparted to these words by RFC 2119, a practice widely adopted amongst SDOs (see also ISO Directives Part 2 App.H). This dichotomy should be resolved.	Determine if these are requirements or guidelines and make the necessary changes to each volume to reflect this change to state clearly that the document defines [normative] requirements [using key words as defined in RFC 2119] whilst providing supporting, explanatory and informative guidance. Implicit in this suggested change is that all references throughout the document to 'guidance' need to be reviewed to determine whether they are truly informative as opposed to being actual normative requirements.
Kantara-306	63C	Whole doc / set	0	0	The structure of the document does not lend itself to easy determination of: a) which clauses are actually expressing normative requirements; and b) what are discrete normative requirements. This is evidenced by no consistency in style regarding whether informative discussion precedes normative requirements and by single paragraphs which bear both normative and informative text. This weakens the utility of the document [set] in either its use as an educational/informative source or as a set of formal requirements.	1 - Express each normative requirement as a distinct clause; 2 - Give each such clause a unique reference; 3 - Give the user a very clear means to determine the status of a passage of text - i.e. exclusively normative or informative. It is noted that adopting a presentational distinction would be an easier solution to achieving much greater presentational clarity than trying to extract and regroup all passages of one type or another.
Kantara-307	63C	2	3	338-339	"In a federation scenario, the CSP provides a service known as an identity provider, or IdP." The CSP may or may not be the IdP. For example, GSA's USAccess may act as a CSP and issue a PIV to SSA. SSA may federate with IRS, acting as the IdP while using a USAccess-issued PIV for user authentication, and may provide additional attributes.	
Kantara-308	63C	2	4	386; 930	This use of 'subscriber' here is confusing. The person is a subscriber to the CSP/IdP, not to the RP.	Recommendation: change from 'RP subscriber account' to 'RP user account' or 'Provisioned RP account'.
Kantara-309	63C	4.2	9	513	"Government-operated IdPs asserting authentication at FAL2 SHALL protect keys. "	Strongly recommend dropping the 'government-operated' qualifier so that all IdPs accepted by government RPs have the same baseline security.
Kantara-310	63C	4.4	9	545	" or an indication that no IAL claim is being made" <-- This is IAL0	recommend that IAL0 be asserted in this case.
Kantara-311	63C	4.4	10	547	"or an indication that no AAL claim is being made"	For consistency, recommend an AAL0 level be added to the guidance and then asserted here.
Kantara-312	63C	4.4	10	560	""IAL1", the lowest numbered IAL described in this suite" Isn't IAL0 the lowest numbered IAL?	Update to reflect IAL0
Kantara-313	63C	5	13	618	"identity attributes" The IdP may also provide roles used for authorization	remove the 'identity' qualifier and just say 'attributes'.
Kantara-314	63C	5.2.1	19	784	"Protocols requiring the transfer of keying information SHALL use a secure method" What are the minimum requirements for a 'secure method'?	
Kantara-315	63C	5.2.1	19	786	"shared secrets or public keys. Any" What are the cryptographic requirements for the keys?	
Kantara-316	63C	5.3	21	829	"A subscriber's attributes SHALL be transmitted between IdP and RP only for identity federation transactions or support functions such as identification of compromised subscriber accounts as discussed in Sec. 5.5. A subscriber's attributes are not to be transmitted for any other purposes" IdPs need to be able to send attributes needed for authorization in addition to identity attributes. This statement seems to prohibit that.	Recommend changing this from for "identity federation transactions" to for "identity or authorization federation transactions".
Kantara-317	63C	5.4.2	27	1011	Typo	change "from with each other" to "from each other"
Kantara-318	63C	5.4.2	28	1023	"The IdP SHOULD signal downstream RPs when a subscriber account is terminated, or when the subscriber account's access to an RP is revoked. "	Add a requirement to provide a reason for the termination or revocation in the case of suspected fraud/account compromise. This can alert the RP to review prior transactions to look for suspicious activity.
Kantara-319	63C	5.4.2	28	1027; 1062; 1068; 1126	"Upon receiving such a signal, the RP SHALL terminate the RP subscriber account and remove all personal information associated with the RP subscriber account"	Suggest removing this statement for IAL1 and above accounts. If an individual has an account at a federal agency which offers the option to access a service using Login.gov or ID.me, for example, it is not uncommon for someone to have both credentials and then cancel one. Their account at the RP shouldn't then be deleted. Even if the user terminated all of their federated credentials, their information with the agency shouldn't be deleted - it should be retained so they can get a new credential and access their information in the future. In many cases, the account at the RP should be independent
Kantara-320	63C	5.4.5	29	1083	"the RP SHOULD employ a time-based mechanism to identify RP subscriber accounts for termination that have not been accessed after a period of time, for example, 120 days since last access." What is the rationale for doing this? Many government services are only accessed annually, or even every few years.	
Kantara-321	63C	5.5	30	1118	"An IdP MAY disclose information on subscriber activities to RPs for security purposes"	Recommend changing this to a SHOULD, or even a SHALL.
Kantara-322	63C	5.5	30	1120 - 1121	"An RP MAY disclose information on subscriber activities to IdPs for security purposes"	Recommend changing this to a SHOULD or a SHALL in the case of a compromised or fraudulent account.

Kantara-323	63C	5.7	32	1203; 1210	"The IdP/RP MAY send a signal regarding...The account is suspected of being compromised."	Strongly recommend changing this to a SHALL. It is irresponsible for account compromise to be detected without sharing that knowledge across the federation.
Kantara-324	63C	6	34	1243	"Digital signature or message authentication code (MAC)" Should there be a requirement that NIST-approved crypto be used for these?	
Kantara-325	63C	6	34	1248	" or an indication that no IAL is asserted." This is IAL0, so this statement is not needed.	Remove for clarity
Kantara-326	63C	6	35	1266	"All metadata within the assertion SHALL be validated" There may be metadata that does not require validation.	Recommend changing to: "The following metatadata...SHALL be validated:"
Kantara-327	63C	6.1	36	1301 - 1305	This section reads like a definition rather than a requirement. If it is a definition/informative, it would be helpful to explicitly label it as such. If it is a requirement, it needs to be rewritten so that any requirements contained in the section are clearly stated.	clarify
Kantara-328	63C	6.1.2.1	37	1353	"The RP would then prompt the subscriber to present the certificate from their smart card in order to reach FAL3." The presentation of the certificate does not, by itself, achieve FAL3.	I would state the additional steps required, or rephrase to something like "The RP then prompts the subscriber to authenticate using their smart card certificate in order to reach FAL3."
Kantara-329	63C	6.2.5.	44	1481	"A pairwise pseudonymous identifier (PPI) allows an IdP to provide..."	Should this be stated as a requirement, such as "A pairwise pseudonymous identifier (PPI) MAY be used by an IdP to provide multiple..."
Kantara-330	63C	6.2.5.1	44	1501	"between the IdP and the federation proxy itself. The proxy, acting as an IdP, can itself provide pairwise"	Editorial comment: Remove both instances of the word 'itself'.
Kantara-331	63C	6.3	46	1558	"The IdP can indicate in the assertion when the last time the subscriber's attributes have been updated in the subscriber account"	Consider making this a SHOULD to improve data quality.
Kantara-332	63C	7.1	48	1621	"SHOULD have a lifetime of no more than a small number of minutes in length." "a small number of minutes in length" may mean 2 minutes to one developer and 120 minutes to another. How is the maximum amount of time required for the lifetime of the assertion reference determined?	Explore that question and provide a more concrete requirement.
Kantara-333	63C	7.2	52	1666 - 1669	"Though it is possible to intentionally create an assertion designed to be presented to multiple RPs, this method can lead to lax audience restriction of the assertion itself, which in turn could lead to privacy and security breaches for the subscriber across these RPs. Such multiRP use is not recommended." Why not just prohibit this? Is there any reason this is needed in the federal government?	
Kantara-334	63C	7.3	52	1680	"authenticated protected channel." Are the minimum security requirements for creating an authenticated protected channel referenced anywhere?	
Kantara-335	63C	8	53	1698	"including the CSP which now acts as an IdP" The CSP and IdP may not be the same entity.	

PROOFING TYPE TAXONOMY (Kantara-113)

Proofing Type		*Definition*
UNSUPERVISED		Proofing performed exclusively automatically, without any human supervisory interaction.
SUPERVISED	**REMOTE PROOFING**	Proofing which uses telecommunications to permit/support human Supervisory oversight of and participation in the proofing process.
	CO-LOCATED PROOFING	Proofing at which a human Supervisor has direct physical oversight of and participation in the process.

PROOFING TYPE DEFINITIONS

Term	*Definition*
Unsupervised Proofing	Proofing performed exclusively automatically, without any human supervisory interaction.
Supervised Proofing	Proofing which demands human Supervisory interaction.
Supervised (Remote) Proofing	Proofing which uses telecommunications to permit/support human Supervisory oversight of and participation in the proofing process.
Supervised (Co-located) Proofing	Proofing at which a human Supervisor has direct physical oversight of and participation in the process.
Hybrid Proofing	A combination of any of the previously-defined Proofing Types which is controlled by the CSP according to the specific requirements for each hybrid Proofing Type element.

NOTES	*1 - 'Proofing' is used as a convenient term to mean 'identity proofing', according to the specific requirements for any given assurance level;*
	2 - 'Proofing type' is used as a convenient term to refer to one or more of the 5 defined specific proofing types.

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:	*Kantara Initiative, Inc.*
Name of Submitter/POC:	*Identity Assurance Work Group*
Email Address of Submitter/POC	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	NIST Question (Include rationale for comment)	Kantara Response
Kantara-336	63-Base	Note to Reviewers	iii	175 - 181	· What technologies or methods can be applied to develop a remote, unattended IAL2 identity proofing process that demonstrably mitigates the same risks as the current IAL2 process? · Are these technologies supported by existing or emerging technical standards? · Do these technologies have established metrics and testing methodologies to allow for assessment of performance and understanding of impacts across user populations (e.g., bias in artificial intelligence)?	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. 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 the model. With a methodology clearly communicated within the rule, solutions can be assembled to offset the value only biometrics could deliver under prior rule releases. 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. NIST should publish a quantifiable scoring system for identity proofing and authentication. 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. 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 the model. With a methodology clearly communicated within the rule, solutions can be assembled to offset the value only biometrics could deliver under prior rule releases.
Kantara-337	63-Base	Note to Reviewers	iii	182 - 183	What methods exist for integrating digital evidence (e.g., Mobile Driver's Licenses, Verifiable Credentials) into identity proofing at various identity assurance levels?	mDLs may be used as a source of signed data attributes from an authoritative source (state DMVs). They may also be leveraged as an authenticator (either at the time of proofing or by linking sometime later). However, they should adhere to some of the other suggestions presented within this comments document. Here are some specific areas for NIST to consider regarding the use of mDLs as they become more prevalent: · mDLs should all be able to present a public key certificate that can be authenticate back to a trusted issuing authority. States may publish their own public key certificates, but most will likely partner with AAMVA as participants with their new mDL Digital Trust Service. The mDL DTS will securely collect and publish the public key certificates of participating issuing authorities through a single Verified Issuer Certificate Authority List (VICAL) for all relying parties to access. NIST should consider requiring all mDLs used in proofing/authentication under 800-63-4 should make their public keys available to the community via AAMVA's mDL DTS Service, or equally trustworthy means. · mDLs should all be conforming to the ISO 18013-5 Standard for interoperability as a base requirement. This standard has been established collaboratively with an international working group and has included the leadership of AAMVA and many US state DMVs. Adherence to the standard will drive the interoperability and ubiquity required for mDLs to enjoy the same universal acceptance that physical driver licenses have historically. · Every device leveraged during a proofing/authentication process includes one-time and ongoing risk assessment

Kantara-338	63-Base	Note to Reviewers	iii	184 - 193	What are the impacts, benefits, and risks of specifying a set of requirements for CSPs to establish and maintain fraud detection, response, and notification capabilities? · 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? · How might emerging methods such as fraud analytics and risk scoring be further researched, standardized, measured, and integrated into the guidance in the future?	At IAL1 or IAL2, identity risks can be effectively managed without mandating use of strong evidence for ALL subjects. By combining multiple pieces of fair evidence in conjunction with risk signals related to identity theft or synthetic identity fraud, organizations can more effectively meet their mission delivery needs and manage cybersecurity risk than with what is currently rated as STRONG evidence. Examples of fraud risk signals include, but are not limited to, PII data recent activity, Phone account and activity attributes, email data/attributes from ISPs, device and IP address review for high-risk indicators, anomalous credit bureau data, and behavioral characteristics. The use of these signals within advanced analytics to create an Identity Confidence model has proven extremely powerful in effectively reducing cybersecurity risk while simultaneously minimizing impact to good subjects within the private sector for years. Including an Identity Confidence model validation option better enables organizations to meet both their mission delivery and cybersecurity risk needs. It is critical to ensure any use of fraud risk signals in coordination with identity proofing include empirical evidence of its effectiveness in addressing the cybersecurity risk (false negative errors) as well as mission delivery risk (false positive errors). This can generally be shown using a variety of model performance and validation analytic techniques (e.g., Receiver Operator Characteristic Curve, Area Under the Curve, KS test, GeNIe). These techniques inherently require effective measurement systems to determine subjects' disposition as either good or bad. An alternative method of measuring model performance where there is limited performance data can be random sampling to get a high level of confidence related to the model's performance. With this approach, an Identity Confidence Score could be applied to subjects as an initial, passive option to risk rank the population. Where the confidence score renders the Identity Confidence risk LOW, then the CSP can require the current STRONG evidence to complete identity proofing.
Kantara-339	63-Base	Note to Reviewers	iii	196 - 198	Are current testing programs for liveness detection and presentation attack detection sufficient for evaluating the performance of implementations and technologies?	Ideally, NIST would be provided funding to create a dedicated lab for this research with continuous testing, similar to the work currently done for static facial verification algorithms. Technologies that can defeat liveness detection will continue to evolve alongside the liveness detection technologies, yet facial verification is one of our best tools to prevent fraud
Kantara-340	63-Base	Note to Reviewers	iii	202 - 203	What additional guidance or direction can be provided to integrate digital identity risk with enterprise risk management?	Agencies need explicit and concrete guidance on how to go about developing and utilizing impact category criteria and thresholds tailored to their mission, user capabilities & needs, and risk tolerance. Also recommend providing the option of using a 0-9 scale and likelihood scores in addition to the L M H. The additional granularity has the potential to help improve decision making especially when operational needs, security, and equity must be balanced when deciding on controls. (0 = No Impact; 1-3 - Limited; 4-6 = Moderate; 7-9= High)
Kantara-341	63-Base	Note to Reviewers	iii	204 - 205	How might equity, privacy, and usability impacts be integrated into the assurance level selection process and digital identity risk management model?	Privacy: Context is critical and needs to be taken into consideration. Risking the exposure of the home address of an individual using mySSA to manage their retirement benefits is not the same as risking the exposure of an address in a witness protection program application. Equity & Usability: Without the application of the scientific method we cannot really know which controls make a service
Kantara-342	63-Base	Note to Reviewers	iii	206 - 208	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?	Agencies need to put fraud detection controls in place to understand what is happening - then mitigation techniques can be more precisely applied. Guidance will need to be provided for this to be done defectively in most agencies. (Also, fraud data needs to be shared to protect other agencies.) For some suggestions on how to qualify or quantify the ability to mitigate risk -, see 'How to Measure Anything in
Kantara-343	63-Base	Note to Reviewers	iv	210 - 213	Are emerging authentication models and techniques – such as FIDO passkey, Verifiable Credentials, and mobile driver's licenses – sufficiently addressed and accommodated, as appropriate, by the guidelines? What are the potential associated security, privacy, and usability benefits and risks?	Verifiable Credentials is currently a framework and set of principles, not a technical specification that allows for interoperability and consistent security. ISO has not completed the logical interface standard for mDLs, but it is promising and may be our best path to providing all US citizens and residents with a secure, trustable, identity credential that can be used for remote identity proofing.
Kantara-344	63-Base	Note to Reviewers	iv	230	Is there an element of this guidance that you think is missing or could be expanded?	The implications and effects related to AI/ML should be further defined. Similarly, the guidance related to continuity of operations with maintained assurance in times of disaster (e.g., pandemic). Alternative process guidance should be defined for continuing operations without limiting or reducing authentication and assurance regardless of extraneous changes in environment or operational parameters. What checks/balances can be
Kantara-345	63-Base	Note to Reviewers	iv	234 - 238	Does the guidance sufficiently address equity? · What equity assessment methods, impact evaluation models, or metrics could we reference to better support organizations in preventing or detecting disparate impacts that could arise as a result of identity verification technologies or processes?	To do this well, the following factors should be considered in impact studies: device used/capabilities, the user's proficiency with and access to technology, housing status, access to internet, internet speed, family income bracket, credit score, disability status, sex, NIS or Fitzpatrick skin tone, age, native language, English fluency, education.
Kantara-346	63-Base	Note to Reviewers	iv	239 - 241	What specific implementation guidance, reference architectures, metrics, or other supporting resources may enable more rapid adoption and implementation of this and future iterations of the Digital Identity Guidelines?	It would be very useful to have a reference implementation architecture of an IAL1 & IAL2 implementation that can be used for experimentation. Login.gov may be the best choice for this, but they would need to fully implement IAL2, including biometrics.