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

Please submit responses to dig-comments@nist.gov by October 7, 2024.

Organization:	*ID.me*
Name of Submitter/POC:	*Wes Turbeville*
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63-Base	N/A	N/A	N/A	Clarification from NIST is sought regarding the order of precedence for requirements listed throughout the draft. For example, the main document discusses use of the NIST RMF and tailoring of requirements. Does that supersede normative requirements in other areas (e.g. 63A)? Additionally there are other elements such as allowing Trusted Referees to make risk based decisions on criteria. Does that supersede other normative requirements? Establishing a hierarchy would add clarity greatly aid in conformity assessments. As an example of one area where this is the case is 2.4.2.3. As written, NIST makes it sound as though CSPs have no alternatives to complete verification for users whose: - core attributes cannot be validated in credible or authoritative sources - information on submitted evidence can't be validated in credible or authoritative sources	
2	63-Base	3	24	1030	To promote effective risk management processes, NIST should require any agency or CSP considering adoption of "tailoring" to adopt a KPI measurements framework with auditing mechanisms The key metrics to measure include: pass rates net of fraud, fail / unsuccessful rates, abandonment rates, fraud rates, time spent verifying, and cost per user. - Note, cost per user should consider the "total cost of ownership" of the user's access – verification costs, authentication costs, end-user support costs, and fraud losses These metrics can then be sliced by demographic groups and tracked over time to assess how an agency's Risk Management process is performing and how its decisions are impacting the beneficiaries of the agency. These metrics could be independently assessed by an organization such as Kantara. They could be used to: - Inform policy decisions by OMB - Inform technical guidance from NIST on the effectiveness of different compensating controls or verification methods in different situations - Support accountability and transparency activities from Inspector Generals or Government Accountability Office (GAO)	
3	63A	1.2	2	416	For IAL1, ID.me has several points: The impact of changing the definition of a term used in previous NIST drafts is non-negligible. Data structures used by CSPs and identity proofing vendors reference NIST in terms of language and meaning. When the same term changes in terms of meaning, this has downstream implications that impacts industry negatively. We encourage NIST to be consistent when it comes to language and meaning. We remind NIST that NIST removed the concept of NIST 800-63-2 Level of Assurance 2, which would be the legacy equivalent of what is proposed for Identity Assurance Level 1 here, precisely because agencies had applied the NIST 800-63-2 Level of Assurance 2 controls to high-risk programs that should have been protected by Level of Assurance 3. The result was a series of high profile scaled data breaches where the vulnerability exploited was identity proofing and specifically Knowledge Based Authentication. Financial losses to taxpayers were significant and tens of thousands to hundreds of thousands of Americans were impacted for each incident. Without strict, consistent, and clear guidelines for when IAL1 is appropriate and when it is not appropriate, we see history repeating itself in a negative way with NIST 800-63-4. Our assessment is that the approach is well-intended but poorly executed in terms of guidelines. This is a general observation we will support with specific comments later in the text.	Keep IAL1 defined as is, and call the -4's IAL1 proofing a different term.
4	63A	2.1.1	6	529	**Identity resolution** may not be possible for users not present in records without using biometrics to start a reference point to a single unique person in the CSP's records. Additionally, identities that are present in records might be synthetic or malicious identities. Given the stated purpose of IAL2 is to prevent scaled attacks, allowing a person to establish an identity for the first time via a CSP and to perform identity resolution through biometrics while preventing that same face from scaling an attack is an effective technical solution to increase access while mitigating fraud risk.	NIST should explicitly include biometrics and 1:many duplicate face check as a method of identity resolution that will mitigate the risk of synthetic identity proofing attacks and also provide an inception point for resolution for individuals who do not have a presence in records, a driver's license, etc.

5	63A	2.1.1	6	534	**Identity validation** may not be possible for individuals who do not have a presence in records. There are techniques that go beyond records validation to associate a person with a particular place or address.	NIST should explicitly include device based checks and geofencing (e.g. there are geographic compliance tools used by the gaming industry) to check if an individual is associated to a specific geographical location like an address. For example, a student at the University of Virginia could download a native app, turn on Wi-Fi, and the device could associate the student with the University of Virginia campus. This effectively solves the problem of address validation in a more accessible manner if records coverage is lacking.
6	63A	2.1.1	6	539	**Identity Verification** similarly is not effective to prevent scale fraud without biometrics because the attacker might be related to the synthetic identity they created but the identity is not valid. This creates a circular reference error where a malicious actor is verifying a fake identity they injected into records for validation purposes. Scaled data breaches like the National Public Data breach mean it is easier than ever for malicious actors to register a phone number to a set of stolen Personally Identifiable Information, create a high-quality fake of a driver's license using generative AI or paying a few dollars for a high-quality physical counterfeit that is indistinguishable from the original, and then taking a selfie to the photo on the ID. Given this reality, the only effective method to stop a scaled attack is biometrics and duplicate face check to prevent the same fraudster from scaling attacks this way.	For this reason, the biometric step for selfie with presentation attack detection combined with biometrics for identity resolution is the critical step to stop the scaled fraud in federal spending noted by GAO. If that means the country saves more than $200 to $500 billion lost to fraud per year, we can use the resulting savings to provide better customer service to help that person get access.
7	63A	2.1.3	8	595	**Remote Attended Identity Proofing:** NIST says the location and devices are not controlled by the CSP. Did NIST mean "not controlled by the applicant?"	ID.me believes that for security reasons in handling of PII, NIST should require that the location and devices used by the Proofing Agents & Trusted Referees are both controlled by the CSP.
8	63A	2.2	9	617	**Core Attributes:** The concept of Core Attributes makes sense. At the same time, we are troubled by the omission of certain attributes we believe are core along with a lack of recognition of the attributes needed to perform identity resolution from a CSP to an RP. **ID.me Rationale:** date of birth is a critical field to separate family members who have the same name and address (e.g. Senior and Junior) as well as to determine if the age of the person depicted in the selfie matches the age associated with the identity. Phone number and email are obvious mandatory fields as identity proofing and binding to secure authenticators is just the beginning of lifecycle management. Digital addresses are needed to notify the user of activity tied to their account and to keep it safe from takeover. Finally, the match key that government agencies need to match a verified identity to associated records is the SSN or the ITIN. It should not be controversial to separate the value of an SSN or ITIN for identity resolution from a CSP to a Relying Party from restrictions on use of SSN as an authenticator or as a strong form of verification evidence. It is obvious that a Name, Address, and Driver's License number would be wholly insufficient to grant an identity proofed American access to records at the vast majority of government agencies. In summary, we do not understand why so many Core Attributes are omitted from the bundle of specified Core Attributes and we are deeply concerned by the omission. The list of Core Attributes is insufficient for safety or to allow the effective delivery of services for CSPs to RPs for the vast majority of users.	Core Attributes should be explicitly expanded to include: - Date of Birth - Phone Number - Email Address - Federal Government Identifier e.g. (SSN or ITIN or Selfie) - Identity Proofing Evidence Identifier e.g. (Document Number)
9	63A	2.3	9	646	**Identity Resolution:** ID.me disagrees with the stated goal for identity resolution. The goal for identity resolution should be to accurately identify one unique individual within a given population. Data minimization is a separate goal that has potentially negative implications for safety and accuracy, which is why attribute minimization should not be tied to goals associated with identity resolution. To the extent prescriptive restraints tied to data minimization lead to less accurate or unsafe identity resolution, the two concepts are potentially in tension with one another and should be considered separately. Further, limiting identity resolution to attributes – rather than noting the ability to leverage biometric traits – points to a continuing self-imposed limitation on identity resolution that forces a de facto reliance upon data brokers, which in turn imposes severe structural bias against low-income and minority populations that limits digital access.	Identity resolution should focus specifically on techniques to accurately separate one unique individual from all others. NIST should be agnostic to the type of technique used, whether records based or biometric, as long as the outcome of the identity resolution process results in the separation of one unique, real-world identity from all others. Metrics associated with types of techniques should be transparent. We are very confident that synthetic identities in records sources and real-world people/identities who are not present in records will show a much higher failure and fraud rate as opposed to biometric techniques paired with Presentation Attack Detection to perform resolution. Data minimization and privacy requirements are SHOULD controls that point to best practice without restricting the ability of the CSP to keep users safe and to protect government agencies and other customers from fraud, waste, and abuse.
10	63A	2.4.1.1	11	679	**Fair Evidence Requirements:** The requirement for physical or digital security features will effectively wipe out most FAIR pieces of information. Bank and utility bills make up the vast majority of FAIR documents used in the nearly 10 million supervised remote identity proofing sessions we have administered. Additionally, FAIR documents often contain attributes like Name and Address but do not include SSNs or DOBs. As a result, parents and children who share the same names will be indistinguishable in terms of a unique match; however, the degree of identity resolution is sufficient to match to the applicant who has the same name and address. Requiring absolute unique identity resolution on a FAIR piece of evidence would go further than what DHS requires with REAL ID. We believe this section needs significant revisions to allow for security and accessibility.	NIST should revise the text in section 3 to read "The evidence contains sufficient attributes to provide a high probability of identity resolution to the claimed identity." NIST should eliminate the text in section 4. NIST should combine sections 4 and 5 as an OR requirement. "The information on the evidence can be validated by an authoritative or credible source OR the information on the evidence can be verified through an approved method, as provided in Sec. 2.4.2.2." Then, in Sec. 2.4.2.2 - Add a bullet point in this section that reads: "Geolocation check using a device with appropriate technologies to provide a high level of confidence to associate the location of the individual with an address that is self-asserted or listed on identity evidence." NIST should explicitly allow for linking documents like a marriage certificate or a court order showing official proof of a name change to allow an individual to associate their name with an associated identity who is listed on the FAIR document or to their previous name. DMVs have guidance on linking documents NIST should incorporate into NIST 800-63-4.
11	63A	2.4.1.2	11	688	**Strong Evidence Requirements:** the first bullet that references IAL2 is self-referential and confusing. Given this volume is focused on evidence need to achieve IAL1 or 2 or 3, we suggest keeping the examples focused on government agencies that issue ID cards with photos on them. The requirement on point seven for validation is potentially problematic. Many DMVs do not validate driver's license attributes and they do not match the biometric on the ID card. We are deeply concerned about the level of validation and verification infrastructure maturity for other types of ID cards like tribal ID cards, military IDs, and so on. NIST should be much more specific about the attributes required for validation.	Adjust bullet point 7 to read "Name, Date of Birth, and Address, if available on the document, can be validated by an authoritative or credible source." Bullet point 8 appears to be a typo. In the FAIR evidence section, the reference to Sec. 2.4.2.2 refers to "verification" whereas in this reference it is referred to as "validation." We believe verification is the term NIST meant to use here.

12	63A	2.4.2.2	13	749	Per our comments related to 2.4.1.1, we propose adding a bullet point in this section that reads: "Geolocation check using a device with appropriate technologies to provide a high level of confidence to associate the location of the individual with an address that is self-asserted or listed on identity evidence."	
13	63A	2.4.2.3	13	755	**Attribute Validation:** As written, this section will have a devastating impact for low-income and other historically underserved communities. If left unchanged, ID.me estimates that pass rates of individuals who are in the lowest income communities will drop by approximately 50%. Americans who live overseas will likely be almost wholly excluded from digital access to their government and potentially any access to their government as they cannot easily visit an in-person location. In many ways, the point of Trusted Referee we pioneered with NIST in -3 was to provide a digital enrollment pathway for an individual who doesn't have a presence in records. We want to solve for: - Students studying at a university where their address is not in records - Americans who are living overseas. - Homeless Americans who may not have a permanent address. - Americans who don't have credit history or a presence in alternative records. - Americans who are not listed accurately in records e.g. recently moved, name change, core attribute transcription errors, etc. In a remote context, address validation is particularly important because it links a person to a specific geographic area. The immutable Core Attributes are DOB and SSN. Face is the key biometric identifier, which is already inherently public, that changes slowly over time. Name & Address & Name History & Address History are also tied to the Core Attributes.	Leave the current text intact **as the first of three options** for attribute validation and identity resolution. Then add two additional options: - "For individuals whose core attributes are referenceable in records except for address e.g. (Name, DOB, and SSN), the CSP MAY use a geolocation check using a device with appropriate technologies to provide a high level of confidence to associate the location of the individual with an address that is self-asserted or listed on identity evidence." - "For individuals whose core attributes cannot be validated in records, the CSP SHALL use a Duplicate Face Check upon enrollment subject to applicable FMR and FNMR rates (Section 3.1.11) and a geolocation check using a device with appropriate technologies to provide a high level of confidence to associate the location of the individual with an address that is self-asserted or listed on identity evidence. The CSP will provide a flag for agencies to review for individuals who are validated in this manner."
14	63A	2.4.2.4	13	759	**Validation Sources:** As NIST is acutely aware, standardization and consistency is really important. While the changes here might be conceptually more precise, they are harmful in the context of a mature ecosystem with organizations operating at scale. With more than 60 million Americans identity proofed in ID.me's system to NIST 800-63-3 IAL2, a new definition for records sources in NIST 800-63-4 represents a serious challenge for lifecycle management of existing credentials, data schema, and mapping the **same records definition that now means two different things** in an orderly way. In this text, NIST is changing previously used definitions of words in prior versions of NIST 800-63 as Issuing Sources now means Authoritative Sources and Authoritative Sources now means Credible Sources. We strongly urge NIST not to make this semantic change as changing the meaning of previously used terms is deeply challenging when it comes to data structures and to backwards compatibility with previous versions of NIST 800-63. Because authoritative sources are effectively issuing sources "an authoritative source is the issuing source," we ask that NIST retain the previously used designation of an Issuing Source for a given attribute, like an SSN tied to SSA or a driver's license number tied to a DMV. It is intuitive that an organization might serve as a proxy for an Issuing Source with appropriate provenance. Authoritative Sources should be consistently defined along the lines of what NIST is calling a Credible Source.	Retain the language and definition of an Issuing Source. Retain the language and definition of an Authoritative Source. Modify the definition incrementally as needed along the lines of how a Credible Source is defined but do not delete terms and change the meaning of previously used terms. Through devices, users can directly serve as a Credible Source, particularly when it comes to proving possession of phone numbers, email addresses, and geolocation. With appropriate technologies, a device can provide reliable geolocation estimates, similar to checks performed in the gaming industry, to associate an individual with a particular geographic location. These device based checks are at least as secure as addresses in Credible Sources, and arguably more secure depending on the methods credit bureaus use to associate attributes with users. Additionally, granting users the ability to validate their address and geolocation via a device will dramatically improve accessibility, particularly for populations who are less likely to be present in records.
15	63A	2.5.1	14	780	**Identity Verification Methods:** We applaud NIST for expanding the number of verification methods that are acceptable. Given advancements in generative AI and deep fakes, we urge NIST to require the use of Presentation Attack Detection for all remote capture of a selfie and to require the use of appropriate deep fake detection tools and Presentation Attack Detection as needed when the live agent is interacting with the applicant. Already, ID.me agents cannot identify a video stream deepfake in over half of the situations where that technology is used without countermeasures to assist the agent in detecting the deep fake. Over the next few months, we assess those countermeasures will lose their efficacy. As a result, biometric tools to detect deep fakes and Presentation Attack Detection are critical security controls to protect Americans from identity theft and to secure agencies from fraud and allowing unauthorized users access to private information. Thank you for explicitly banning Knowledge Based Verification.	NIST must require Presentation Attack Detection for images collected when the applicant is remote (versus on-site) and the use of deep fake detection tools for live video streams when the applicant is meeting with an agent.
16	63A	2.5.1	15	817	We just wanted to say "thank you" for re-emphasizing that KBV has no place in identity verification.	
17	63A	3.1.2.2	19	951	**RP Fraud Management:** We are delighted to see calls for a bi-directional feedback loop to combat fraud and identity theft between CSPs & RPs. That is awesome!	
18	63A	3.1.2.2	20	963-973	**RP Fraud Management:** The way this is written is overly burdensome to CSP's because it opens them to a continuous string of reviews – likely conducted in different ways – by each relying party. If a CSP has 50 federal relying parties, should the CSP be subject to 50 annual reviews by agency fraud teams? Additionally, the way it is written is that it is subjective and not directly testable for conformance by an auditor or assessor. Additionally, having open-ended requirement for reviews without clear guidance on how to conduct them increases the risk of exposure of a CSP's counter-fraud tactics, techniques, and procedures (TTPs).	Remove requirements 5 and 7 from Section 3.1.2.2, as they are untestable as written If removal is not an option, reframe the entire requirement to be in-line with an assessment cycle that is testable and auditable by an assessor to determine if a CSP and RP are conformant or not. Additionally, NIST should add language to enable creation of reusable evidence and test results, which could be independently assessed by an external entity (i.e. Kantara). This would increase the efficiency and effectiveness of these requirements because agencies can leverage results of reviews conducted by other agencies, similar to how multiple agencies can leverage a single FedRAMP package and complete their own ATO review process. In the absence of a formal program like FedRAMP, NIST could add language requiring re-use of results of assessment for conformance. For example: "When RPs leverage the same CSP, RPs SHALL accept reusable evidence, results, and conformance assessments related to fraud programs."

19	63A	3.1.2.3	20	977	**Treatment of Fraud Check Failures:** For #3, the CSP should provide a layer of trained human review but not necessarily a Trusted Referee. We have fraud personnel who are not Trusted Referees who would be better suited to reviewing the session.	NIST should allow CSPs to designate an account as fraud without human review if there is an overwhelming amount of signals and evidence providing a high degree of certainty the session is fraud. In those high certainty situations, the user can file a ticket to prompt a review but the CSP shouldn't be obligated to proactively manually review sessions tied to bots or criminal organizations. For more ambiguous fraud scenarios, we agree that human review should be required but not necessarily a trusted referee. The CSP should be able to route the session for review to the agent and team with the appropriate training and skill to best adjudicate the situation.
20	63A	3.1.3.2	22	1028	**Additional Privacy Protective Measures:** A normative requirement to limit PII to the minimum necessary is a well-intentioned but deeply misguided requirement. CSPs need to be able to collect sufficient attributes to effectively mitigate risk. For example, the CEO of a Fortune 500 company will quite obviously be a much more prominent target for fraud and identity theft as the profit to an attacker is much larger. Veterans suffer from identity theft at significantly higher rates than the general population according to FTC data. From a risk based perspective, it is critical that CSPs and agencies are able to apply a higher degree of protection to healthcare providers who have prescription privileges, elected officials, prominent celebrities and members of the business community, journalists, and other individuals who are more likely to be targets of bad actors. Given the regulated nature of CSPs, the way this text is written will make it more difficult to mitigate the risk of fraud and identity theft as it varies across user populations. Additionally, these considerations should also take into account lifecycle considerations as the CSP needs to protect the applicant from scams and account takeover post identity proofing for subsequent authentication.	Change text to "The CSP SHALL take steps to limit the use of attributes to only those attributes reasonably associated with performing identity proofing, authentication, and lifecycle management tasks while appropriately mitigating the risk of identity theft and fraud as appropriate across user populations."
21	63A	3.1.3.2	22	1036	**SSNs:** The vast majority of SSNs have been publicly breached at scale along with associations to other attributes like Name, Date of Birth, and Address. From National Public Data to Equifax, it is probable that the Name, Date of Birth and SSN combinations of most American adults are available on the dark web. SSNs should never be used as authenticators or as identity verification evidence for this reason. At the same time, SSNs are still incredibly useful for identity resolution within a CSPs identity proofing process and also post identity proofing they are the de facto match key for the vast majority of CSP to RP interactions. We do agree that tokens such as a UUID should be used after the initial exchange of an encrypted SSN to help with identity resolution from a CSP to an RP. All of this to say, what problem is the government solving by limiting SSN retention given that the vast majority of all Americans SSNs have been breached and SSNs are still the de facto essential attribute needed for interoperability post-authentication?	
22	63A	3.1.4	22	1053	Goals in this section are tied to addressing differences in access, treatment, and outcomes for members of one group versus another. These goals should be considered separately for identity proofing versus an identity proofed user authenticating to a new government agency. While parity on access and outcomes are possible for identity proofing, parity on treatment can only be achieved in a reusable model. For example, calling for parity in terms of treatment during identity proofing issuance is impossible while complying with the other normative requirements e.g. an individual living overseas whose attributes are not present in records or a member of a tribal population who needs video chat assistance as well as an interpreter. The very presence of different proofing pathways designed to serve the needs of different populations means that treatment will differ to provide paths to the same end – a successfully proofed user. For example, the mitigation in Section 9 accounting for a change to name and gender on identity documents lists Trusted Referees. While the Trusted Referee can enable access and a positive outcome, the treatment is different. For all of these inherent challenges with identity proofing that are not tied to the process of logging in post-identity proofing, agencies should consider the size of the CSPs preverified population when considering equity and the aforementioned goals.	
23	63A	3.1.5	23	1087	**General Security Requirements:** NIST should encourage CSPs to collect and retain information during identity proofing that will be helpful for authentication and lifecycle management post-identity proofing to prevent account lockout and account takeover.	
24	63A	3.1.6	24	1105	**Redress Requirements:** Approximately 80% of the fraud attacks ID.me sees today are associated with scams where the individual is acting under the direction of an attacker. To provide context, ID.me observed nearly 1.3 million accounts targeted for scams during a 90 day period during 2023 alone. While we agree with NIST's intentions in this section, this section must also account for social engineering and scams. If ID.me were merely providing help desk support, our job would be much easier and our team much smaller. As it stands, we are adjudicating sophisticated fraud more often than not, so we aim to make our process easy to navigate and use for individuals who simply need help but also safe so we can protect individuals who are being exploited by scammers and aren't aware of it. We would like NIST to add language to this section that accounts for the CSPs responsibility to provide appropriate protections to victims of scams.	
25	63A	3.1.7	24	1113	**Additional Requirements for Federal Agencies:** will there be mandatory baseline training and education requirements on authentication, identity proofing, and lifecycle management for involved officials at agencies?	We strongly encourage adoption of a metrics based scorecard as noted in our response to section 3.1.4 so there is an objective and science based method of measuring a CSPs performance overall and for members of specific populations so agencies have more insight into comparative performance between solutions.

26	63A	3.1.8	25	1145	**Postal Addresses:** Given that mail is subject to theft and that family members commit identity theft, this process seems reasonably secure but also slow and prone to identity theft attacks from family members, which disproportionately impacts underserved populations. - The Identity Theft Resource Center and Black Research Collective have written a report detailing identity theft in urban black communities: https://www.idtheftcenter.org/wp-content/uploads/2023/09/Identity-in-Practice-Report-FINAL-2.pdf - According to ITRC and BRC, 40% of surveyed identity theft victims said the fraud was carried out by someone they know. Of those, 59% were family members. - Making matters worse, those victimized by a family member "shared many stories about their reluctance to take action against parents, siblings, aunts, and uncles." (https://www.idtheftcenter.org/wp-content/uploads/2023/09/Identity-in-Practice-Report-FINAL-2.pdf) - Additionally, enabling verification via confirmation code makes it easier for abusive spouses to exploit their victims because they don't need the victim to participate in the verification process to gain access to government services in the victim's name - The allowance for a confirmation code leaves these communities exposed in a way that other verification methods in the -4 draft would prevent. **What data does NIST have that led NIST to believe that confirmation codes can be "applied to a remote, unattended IAL2 identity proofing process that demonstrably mitigates the same risks as the current IAL2 process?"**	**ID.me Proposal:** - Remove option for confirmation code for verification at IAL2 - Commit to studying it as an option so that NIST has sufficient data to understand fraud, equity, and security implications across demographic groups.
27	63A	3.1.9	26	1164	**Requirements for Continuation Codes:** This section seems overly prescriptive for a specific method. Why can't the applicant just authenticate a new session at AAL2 as long as the first session that involved the incomplete proofing involved first binding the AAL2 authenticators? If this is intended to describe linking an identity proofing session that begins online to an in-person identity verification event, this section makes more sense.	Link this method to the most relevant identity proofing pathway. We would link AAL2 authentication to resume an unsupervised IAL2 proofing session that was not completed in a prior session whereas a Continuation Code makes sense for an online to in-person verification flow.
28	63A	3.1.10	26	1185	**Requirements for Notification of Identity Proofing:** "SHALL be sent to a validated postal address, email address, or phone number." NIST would do well to clarify lifecycle management. For example, an individual who is not present in data brokers or credit bureaus could complete identity proofing to NIST IAL2 so long as biometric identity resolution and address validation using device geolocation are in place. At that point, does the email address count as validated if it a) wasn't validated by an authoritative or credible source but b) was confirmed as in the possession of a user who went through identity proofing at IAL2 i.e. inherently validated. The answer should be yes – an identity proofed user should have the freedom to update their address of record or add a new address of record over time – but NIST should make this explicitly clear.	This section should be more inclusive. Specifically, it should address user populations where many individuals do not have a presence in records as well as life cycle considerations for all applicants where the validated attribute might not be an accurate attribute as people change emails, phone numbers, and physical addresses over time.
29	63A	3.1.11	27-29	1207-1280	**Requirements for the Use of Biometrics:** The requirement for the CSP to collect consent for all collection of biometrics is onerous, particularly if the biometric will be used for authentication.	CSPs should have to have an explicit, informed consent screen any time a new type biometric is collected OR if the use of an already collected biometric has changed but otherwise consumers should be able to opt-out. At minimum, consumers should have the ability to check a "don't show me this again" box.
30	63A	3.1.11	27-29	1207-1280	**Requirements for the Use of Biometrics:** This normative requirement should be deleted. Generative AI and deep fakes – coupled with synthetic identities making identity resolution tied to records prone to scams, breached data enabling bad actors to associate phone numbers controlled by the attacker with legitimate PII in records, and scams that compromise legitimate copies of driver's licenses and passwords – mean that biometrics are more important than ever for IAL2 Identity Proofing. Additionally, point five doesn't reference that the Identity Assurance Level and protections against scams and account takeover are inherently weakened when the biometric is deleted. This requirement is tantamount to forcing DMVs to issue a driver's license with the photo section cut out. That would of course degrade the security and integrity of the credential and make the credential more prone to unauthorized use. Additionally, there is no reference to fraud – the text says "at any time." What data is NIST using to support this normative requirement for deletion that would advance security and privacy?	For IAL2, CSP retention of the biometric should be mandatory along with retention of other PII for the default period. We recommend pointing to federal records retention guidelines to provide appropriate protections against fraud. There should be appropriate exceptions for retention when federal, state, or local law require a shorter retention period NIST should issue guidance based on empirical data to indicate if deleting the biometric compromises the assurance level of the credential e.g. moving it from IAL2 to IAL1.
31	63A	3.1.11	27-29	1207-1280	**Requirements for the Use of Biometrics:** NIST should provide the independent testing for biometric algorithms. There is a significant amount of activism and partisan ideology in academia. We would much prefer a federal agency like NIST or CISA to perform independent testing of algorithms so CSPs have a "golden list" of high-performing algorithms from which to use, similar to the FedRAMP Marketplace.	NIST should point to the NIST FRVT test results as the source for independent testing with CSPs having the optional ability to leverage a trust framework body like Kantara or an NVLAP laboratory to perform testing.
32	63A	3.1.11	27-29	1207-1280	**Requirements for the Use of Biometrics:** Thank you for establishing minimum thresholds set for false match and false non-match. These accuracy guidelines will help build public trust in the accuracy of the technology employed by CSPs.	
33	63A	3.1.11	27-29	1207-1280	**Requirements for the Use of Biometrics:** Thank you for making Presentation Attack Detection mandatory in a remote setting. Omitting liveness from NIST 800-63-3 was a significant mistake that we are glad to see rectified.	
34	63A	3.1.11	27-29	1207-1280	**Requirements for the Use of Biometrics:** We are pleased to see Duplicate Face Match (1:N) explicitly authorized as a fraud control with mandatory false positive thresholds. This is a terrific addition that will reduce identity theft and fraud.	
35	63A	3.1.12	30	1310	**Requirements for Evidence Validation Processes (Authenticity Checks):** The way this is written, it is not clear how extensive of results need to be published. Additionally, given the technical nature of some of this testing, interpretation by the public can lead to misinformed conclusions if media or other readers don't understand the theory or metrics behind the technology and testing. Results should be placed in the hands of professionals and trained experts who can then provide the public with informed opinions and conclusions	Recommend changing to say, "CSPs SHALL make results of testing that are relevant to fraud prevention and equity considerations available to government agencies. CSPs SHOULD make results of testing available to other subject matter experts such as policy think-tanks, non-partisan research institutions, or independent accreditation bodies."

36	63A	3.1.13	31	1340-1352	**Exceptions & Error Handling:** ID.me supports the use of Trusted Referees and Applicant References as aids during the identity proofing process. However, those resources should be deployed when those resources can assist the applicant through the identity proofing process.	NIST should clarify that Trusted Referees should be included but that CSPs have latitude to determine when the Trusted Referees should engage with the applicant. Without these boundaries, costs to agencies would significantly increase.
37	63A	3.1.13	31	1340-1352	**Applicant References** are noted as a method to vouch (validation) for an applicant's attributes, condition, and identity. How should CSPs think about the trustworthiness of an Applicant Reference in a standardized way? What does NIST mean by the "condition" of the applicant specifically? Please clarify.	
38	63A	3.1.13.1	31	1353-1387	**Trusted Referee Requirements:** As the company that pioneered the use of Trusted Referees to increase accessibility and has identity proofed nearly 10 million Americans to IAL2 using this method, ID.me has a vested interest in ensuring the ongoing viability of this method while safeguarding against ever more sophisticated fraud attacks, including the use of generative AI and adversarial biometrics to commit fraud through this method. As written, it is unclear how these steps, without additional safeguards, meet the intent of IAL2 to prevent scalable, remote attacks on high-value applications.	**ID.me Proposal - Identity Resolution:** Add "The CSP SHALL use biometrics and duplicate face check to perform biometric identity resolution." **ID.me Proposal - Generative AI protections:** Add "The CSP SHALL use biometrics and appropriate deep fake detection technologies to authenticate the accuracy of the media displayed to the Trusted Referee." **ID.me Proposal - Geolocation:** Add "The CSP SHALL use geolocation verification technologies to associate the applicant with their physical location OR use an Applicant Reference who can vouch for the physical location of the applicant after being themselves associated with a specific geolocation." **ID.me Proposal - IAL2 Status:** Provided the above conditions are met, NIST should deem these credentials to be IAL2. In this method, identity resolution, attribute validation, and identity verification are all included in the steps above albeit using the CSP as the inception point for an identity the same way that a DMV can use a birth certificate, which does not have a photograph on it, and documents that prove residency and address to issue a REAL ID. Given the prevalence of synthetic identities and injected malicious data in credible sources, we believe biometric identity resolution is both more accurate and secure than traditional methods.
39	63A	3.1.13.2	32	1388-1411	**Trusted Referee Uses:** Why is it mandatory to offer trusted referees for biometric failures but not for records validation failures? Please provide the basis in fact that calls for mandatory interventions for biometrics, but not for issues with data brokers, which are actually far more common and structurally biased against lower income groups.	Biometric enrollment with liveness and duplicate face check for identity resolution should be a SHOULD overall but a SHALL, mandatory, for instances where there are no records to validate the applicant's attributes.
40	63A	3.1.13.2	32	1388-1411	**Validation Comment:** Section 3 (c) allows for Trusted Referees to compare Fair & Strong/Superior evidence to validate attributes but it doesn't specify if that works for IAL2.	NIST should add language to 3.1.13.2 to clarify their intention that this applies to IAL2 as well.
41	63A	3.1.13.2	33	1398	**Trusted Referee Uses:** In our experience, attribute validation through credible or authoritative records significantly underperforms biometrics in terms of both absolute pass rate and consistency across demographics - The way the language is written, NIST is requiring a fallback for a step that has been shown in government testing to have a high pass rate and performs consistently across demographics and is not requiring a fallback for a step that has a higher fail rate, particularly for underserved, low-income populations - NOT making offering TR for records validation a Normative requirement will disadvantage underserved populations **Additionally:** - **Having the offer of Trusted Referee for failures in validation as a "SHOULD" is inconsistent with 2.1.3**, which makes an "Attended process" normative if CSP offers "Remote Unattended Process." - Both Remote Attended and Onsite Attended processes call for the CSP to "to include resolution, validation, and verification" either through secure video session with a proofing agent (Remote Attended) or in the presence of a proofing agent (Onsite Attended).	Revise language to: "CSPs **SHALL** offer trusted referee services for failures in completing automated validation processes, such as in cases of mismatched core attributes or the absence of the applicant in a record source."
42	63A	3.1.13.3	33	1412-1434	**Applicant Reference Requirements:** ID.me thinks it is good to leave flexibility for CSPs. At the same time, there is little to no guidance to help us think about how to incorporate Applicant References into our processes in a standardized way that mitigates risk. Directional examples of Applicant References that would be OK and not OK would be helpful.	
43	63A	4.1.2	36	1517-1524	**Evidence Collection (at IAL1):** NIST should require a facial portrait for all evidence used at IAL1 that is not inherently tied to validation e.g. phone number, credit card, bank account, etc. There is an obvious difference in strength between someone who uses a driver's license to verify their identity versus someone who uses a document that does not contain their photo. This creates a "weakest link in the chain" problem that effectively de-normalizes IAL1 as a consistent assurance level for security purposes. ID.me has also helped expose situations where caretakers were abusing elderly adults in their care by using their documents for fraudulent gain. NIST should take care to note the security and identity theft risks associated with confirmation codes sent to physical addresses, as individuals in nursing homes will be prime targets, in addition to the administrative burden placed on applicants who have to wait and spend time to return a code that is mailed to them.	"CSPs SHALL collect FAIR evidence that can be digitally validated (e.g. phone number) OR a STRONG piece of evidence that includes a facial portrait of the applicant."
44	63A	4.1.3	36	1525-1529	**Attribute Collection:** the way this is written effectively creates a path of vulnerability to achieve IAL1. The level of attribute validation associated with the evidence should be related to the level of evidence strength. If an applicant can prove possession of a phone number with tenure to the core attributes of the claimed identity, then that is an effective combination of validation and verification to achieve IAL1. If the applicant submits a FAIR piece of evidence without a photo and can also self-assert a significant portion of their core attributes, then the absence of validation and a biometric link between the applicant and the claimed identity presents an extraordinary amount of risk to the true owner of the claimed identity and to taxpayers. At minimum, it should be self-evident that the level of assurance in an IAL1 credential achieved through the latter path is not equivalent to IAL1 achieved through the phone number pathway.	NIST needs to re-write this section to achieve a reasonably similar level of trust in an IAL1 credential and to eliminate any pathways that are weaker than other methods of achieving IAL1.

45	63A	4.1.5	37	1542-1548	**Attribute Validation:** The normative SHALL requirement for the CSP to validate all core attributes and the government identifier is not feasible, may not be applicable if evidence submitted does not contain a government identifier, and not consistent with earlier statements that CSPs MAY collect self-asserted attributes during evidence collection. **Feasibility:** There is no ubiquitous attribute validation service – or anything close to ubiquitous – that validates government identifiers on all of the various Strong and Superior evidence forms e.g. driver's licenses, permanent resident cards, tribal IDs, passports, etc. We are deeply concerned about the way this is written as it reflects a lack of understanding about market maturity. This requirement would make it impossible for CSPs to conduct identity proofing to IAL1 for a significant portion, potentially the majority, of applicants on this step alone.	Biometric identity resolution and duplicate face check on enrollment is a far more accessible, ubiquitous, and secure method of performing identity resolution upon enrollment, particularly if coupled with a geolocation check of the device using technologies leveraged in the gaming industry.
46	63A	4.1.6	37	1549-1567	**Verification Requirements:** These requirements are so similar to IAL2 that we do not understand why NIST would introduce the complexity of a new pathway at IAL1 that will substantially increase operational cost, regulatory compliance, and cost to government agencies and, by extension, taxpayers. A Strong or Superior piece of evidence with a selfie plus liveness check is two pieces of evidence – something you have and something you are – and with attribute validation requirements you're basically already at IAL2, or so close the difference is negligible. Additionally, it is so simple to open a deposit account using breached Personally Identifiable Information that pathways like micro-transactions will be easy for criminal actors to use to bypass more secure checks like biometrics with liveness or a phone number with tenure to the identity.	NIST should provide operational guidance on using bank accounts for identity verification. It is intuitive that a bank account that was just opened and has little money in it should be far less trusted as evidence than a bank account that is ten years old with thousands of dollars in it. This proofing type needs some level of normalization. NIST should require the use of biometrics and deep fake technology in any remote session where a CSP agent meets with an individual to visually compare their face to the photo on the ID.
47	63A	4.1.7	38	1568-1593	**Remote Attended Requirements:** Recording and retention of the video proofing sessions should be mandatory for purposes of non-repudiation. This evidence is also critical to assist individuals who are experiencing Account Lockout or who experienced Account Takeover and need to recover their account. This data should be held along with the other default data retention. Previously, this mapped to federal agency requirements associated with the National Archives and Records Administration retention requirements. We recommend NIST point evidence retention requirements to the NARA requirements with an allowance to shorten the period if there is a state law that requires a shorter retention period and the CSP wishes to extend the state law to all Americans.	Change 4.1.7 (5) to "CSPs SHALL record and maintain video sessions for fraud prevention and prosecution purposes, identity resolution, and to assist the applicant with account lockout and account takeover issues if they arise to ensure effective lifecycle management and accessibility." We agree with the bullet points that follow in this section. Change 4.1.7 (6) to begin with: "CSPs SHALL use appropriate biometric and deep fake detection technologies to ensure the authenticity of the media the agent is viewing." We agree with the rest of the text as currently written in this section which should follow this initial text.
48	63A	4.1.10	39	1621-1638	**Initial Authenticator Binding:** We disagree with the premise of the sequence of steps described. In practice, authenticator binding often precedes identity proofing. Authenticators ensure the same user is authenticating sessions associated with their account over time. In a flow where an applicant begins a registration process online and then goes onsite to complete identity proofing in-person, it is intuitive that the login credentials they set up would be established prior to the completion of identity proofing. The same thing is true for remote identity proofing where an individual will create authenticators, submit documents for review, and then later meet with a Trusted Referee. While we believe it's fine to bind authenticators at the time of identity proofing or later, it's also critical that applicants and CSPs can bind authenticators prior to identity proofing so the proofed identity can be bound to the established authenticators	Add bolded text: "One or more authenticators can be associated (bound) to the 1625 subscriber's account, **either prior to identity proofing,** at the time of identity proofing, or at a later time."
49	63A	4.2	40	1643-1654	**Identity Assurance Level 2 Requirements:** What empirical evidence is NIST relying upon to justify achieving IAL2 without the use of biometrics in a remote context? Further, what are the harms to people who are at higher risk of identity theft due to the absence of biometrics if a threat actor is able to successfully claim their identity? What is the harm to a victim of identity theft when they cannot use a biometric audit trail to prove that a malicious actor who compromised their identity isn't them because there is no audit trail that can be used for repudiation. Based on ID.me's use of biometrics during the pandemic, pass rates increased while fraud rates and associated identity theft rates decreased Given the rise of generative AI after the pandemic that makes remote human inspection untrustworthy, it is completely irresponsible for NIST to advance a non-biometric pathway based on current threat conditions and how quickly threat actors are expanding their use of deep fake technologies that require biometrics to defeat them.	NIST should require the use of biometrics for identity resolution and identity proofing, specifically a selfie with Presentation Attack Detection, for all IAL2 credentials issued in a remote context.
50	63A	4.2.4	41	1672-1690	**Evidence Validation:** See earlier comments regarding FAIR evidence specifically.	
51	63A	4.2.5	41	1691-1700	**Attribute Validation:** The normative SHALL requirement for the CSP to validate all core attributes and the government identifier is not feasible. **Feasibility:** There is no ubiquitous attribute validation service – or anything close to ubiquitous – that validates government identifiers on all of the various Strong and Superior evidence forms e.g. driver's licenses, permanent resident cards, tribal IDs, passports, etc. We are deeply concerned about the way this is written as it reflects a lack of understanding about market maturity. This requirement would make it impossible for CSPs to conduct identity proofing to IAL2 for a significant portion, potentially the majority, of applicants on this step alone. **Disparate Impact:** In general for all individuals who might have a driver's license with a state that doesn't participate in attribute validation and specifically for individuals who are a) not included in credible sources like data brokers or b) do not have a government ID associated with a national attribute validator service (e.g. a Tribal ID), biometric identity resolution and duplicate face check on enrollment is a far more accessible, ubiquitous, and secure method of performing identity resolution upon enrollment, particularly if coupled with a geolocation check of the device using technologies leveraged in the gaming industry.	**Individuals with a Presence in Records:** Change text to "CSPs SHALL validate all core attributes by against an authoritative or credible source AND SHALL validate either the government identifier against an authoritative or issuing source OR perform biometric identity resolution upon enrollment." **Individuals without a Presence in Records:** Add text that says "For individuals where the CSP cannot validate attributes in records, the CSP SHALL perform biometric identity resolution to validate the face is not associated with another identity, and perform a geolocation check to associate the individual with the claimed geographic location using appropriate technologies, and MAY use the attributes contained on the SUPERIOR, STRONG, or FAIR evidence to enroll the individual into a digital IAL2 credential."

52	63A	4.2.6.1	42	1706-1734	**IAL2 Verification - Non-Biometric Pathway:** Based on advancements with deep fake technology and adversarial use of Generative AI, ID.me does not believe there should be a non-biometric pathway to achieve IAL2 in NIST 800-63-4. As of this writing, ID.me agents are unable to detect deep fakes in a video chat session more than 50% of the time. As the sophistication of adversarial technology increases, the efficacy of a human agent performing a remote, physical match of a person on a video feed to the photograph on a STRONG piece of identity evidence will obviously decline. **Question for NIST:** What scientific data did NIST rely upon in determining that sending a postal code or having an applicant meet with a human agent remotely, without using biometrics, would be as secure as a biometric method?	**Biometrics should be mandatory at IAL2.** As we have shared with NIST, **our use of biometrics and liveness during the pandemic increased pass rates** relative to the legacy NIST 800-63-2 Level of Assurance 3 policies we had deployed by deterring bad actors. Today, in the age of generative AI, it would be irresponsible to ignore the increasing power of malicious actors to use generative AI tools to easily defeat the countermeasures described in this section. As written, this IAL2 non-biometric pathway will lead to significant identity theft and harm to people and significant financial loss to taxpayers.
53	63A	4.2.6.2	43	1735-1761	**IAL2 Verification - Digital Evidence Pathway:** NIST is not considering key security features associated with the identity proofing types that should be considered as they are directly related to risk and trust. These concepts must be included as they are critical to establishing whether digital evidence is FAIR or STRONG. - **Tenure:** is a critical concept. A phone number that has been associated with an applicant for 20 years is more trustworthy than a phone number that has been associated with an applicant for three days. Same for a checking account. - **Financial Value:** is a critical concept. A checking account that has $5,000 in it – or a history of exceeding certain financial thresholds like $500 – is more trustworthy than a checking account with $25 dollars in it. - **Transaction History:** a checking account that has significant activity on it for food and drink and bill payments and gas and so on is more trustworthy than a checking account that has little to no transaction history.	Thresholds associated with Tenure, Financial Value, and Transaction History should be used to classify the same type of evidence – like a phone number or checking account – as FAIR, STRONG, or SUPERIOR. NIST should re-write this section and take into account feedback from industry to establish normative guidance as to how to think about the relationship of tenure, financial value, and transaction history when it comes to Evidence Strength. Delete the distinction between STRONG and SUPERIOR when it comes to the Authenticator Assurance Level. Specifically, delete the SUPERIOR classification unless it is supplemented with additional guidance related to our comments above. Based on our reading, an individual could simply go into their bank account and update their MFA method from SMS OTP to a FIDO token at AAL3 and they would achieve SUPERIOR. Because it would be fairly trivial for a bad actor to compromise SMS OTP and to perform the same action, the distinction between AAL2 and AAL3 does not warrant the increase in assurance level as changing authenticators is not fundamentally related to an increase in trust in the underlying evidence.
54	63A	4.2.6.3	43	1762-1776	**IAL2 Verification - Biometric Pathway:** We are confused by the meaning of the word "portrait" in the following sentence tied to 3, b. "Comparing, via automated means, a non-facial portrait biometric stored on identity evidence, or in-records associated with the evidence, to a live sample provided by the applicant." What is a "non-facial portrait biometric?" Specific examples to clarify meaning would be quite helpful.	
55	63A	4.3.3	45	1801-1812	**Attribute Requirements:** ID.me faces millions of account takeover attempts and identity proofing attacks every year at IAL2. Biometrics and liveness detection are critical to ensure accessibility and identity theft prevention for the exact reasons NIST notes here – account recovery, non-repudiation, lifecycle management. We would also note that biometric duplicate face checks at enrollment can mitigate, and nearly completely eliminate, synthetic identity based attacks, which are one of the fast growing types of fraud, identity theft, and associated harms to victims of identity theft.	This language in 4.3.3 2 should be mandatory for identity proofing at NIST IAL2. "The CSP SHALL collect and retain a biometric sample from the applicant during the identity proofing process to support account recovery, non-repudiation, and establish a high level of confidence that the same participant is present in the proofing and issuance processes (if done separately). CSPs MAY choose to periodically re-enroll user biometrics based on the modalities they use and the likelihood that subscriber accounts will persist long enough to warrant such a refresh."
56	63A	4.3.10	48	1909-1918	**Initial Authenticator Binding:** in the text, the CSP is required (SHALL) to distribute or enroll the authenticator during the identity proofing session in section 1, but then section 2 talks about scenarios where the CSP binds the authenticator outside of the onsite identity proofing event. These scenarios are contradictory without an explicit exception to the first scenario. Additionally, in the context of deep fakes, remote workers, and technology firms inadvertently hiring North Koreans, biometric identity resolution and biometrics during identity proofing and for lifecycle management should be extended to NIST IAL2 with enhanced checks for IAL3 issuance.	Add an "OR" at the end of section 1. The biometric requirements for this section should also apply to all remote identity proofing pathways for NIST IAL2. IAL3 issuance should include biometric identity resolution and duplicate face check as mandatory.
57	63A	5.3	51	1961-1970	**Subscriber Account Maintenance and Updates:** Once an individual has been bound to AAL2 authenticators and identity proofed to IAL2, the individual should be able to update their attributes without validation. At minimum, NIST should provide alternative pathways for individuals to update their attributes without a complete reliance on data brokers, particularly as the validation requirement will exclude significant portions of users populations like individuals who live overseas and members of tribal communities. Data brokers can also have significant lags in the timeliness of their data e.g. a person who moves to a new home might now see their address updated in records for weeks after their physical residence has changed. The validation requirement is made more problematic by the fact that criminal actors can quite easily associate phone numbers with stolen PII by registering a phone number to the stolen identity. As written, this requirement will harm accessibility to non-fraudulent users while providing a fairly trivial burden to bypass for malicious actors.	NIST should explicitly include device based checks and geofencing (e.g. there are geographic compliance tools used by the gaming industry) to check if an individual is associated to a specific geographical location like an address. For example, a student at the University of Virginia could download a native app, turn on Wi-Fi, and the device could associate the student with the University of Virginia campus. This effectively solves the problem of address validation in a more accessible manner if records coverage is lacking. NIST should explicitly allow an AAL2 & IAL2 proofed subscriber to update their phone number if the individual is able to prove possession of the phone number via a short-link or confirmation code. NIST should encourage CSPs to use a biometric with presentation attack detection check to ensure the subscriber matches the same person who went through identity proofing. After a biometric check confirms the user is the same, users should be able to update core attributes tied to their identity without validation.
58	63A	5.4	51	1971-1990	**Subscriber Account Suspension or Termination:** CSPs should also provide a service to RPs to communicate status changes tied to subscriber accounts so RPs can take appropriate action if they had granted access to a compromised account.	Add "CSPs SHALL provide a method to communicate account status changes to RPs." Add "CSPS SHOULD take measures to rapidly reinstate accounts compromised by social engineering by educating victims about the scam, stripping off any malicious authenticators, and binding the legitimate owner of the claimed identity to their IAL2 credential at AAL2."
59	63A	6	53	1991-2011	**Threats and Security Considerations:** The majority of the attacks ID.me fights today are social engineering scams and account takeover schemes.	Add **Social Engineering Scams** where an attacker convinces a victim to take action during identity proofing or to compromise authenticators that results in the attacker controlling the login credentials for the subscriber account. Add **Account Takeover** attacks which may be performed via technical means, social engineering means, or hybrid means where automated credential stuffing attacks set up targeted phishing attacks.
60	63A	6.2	56	2018-2033	**Collaboration with Adjacent Programs:** We applaud NIST for including these very important capabilities in NIST 800-63-4. Communication, collaboration, and cooperation is key to keeping individuals and taxpayer funds safe.	

61	63A	7.1	57	2039-2048	**Collection and Data Minimization:** ID.me agrees that unnecessary PII collection should be avoided, but this section should be written very carefully to avoid an overly conservative interpretation by accreditation bodies. Risk is not homogenous across users. Elected officials are subject to higher levels of risk relative to most Americans, which is why they have security details. The same could be said of prominent corporate leaders, journalists, celebrities, and activists. NIST should explicitly acknowledge heterogenous risk levels among user populations that should warrant a tailored approach.	"CSPs SHALL take reasonable steps to minimize Personally Identifiable Information by ensuring attributes collected are related to the identity proofing process and to prevent fraud and identity theft."
62	63A	7.1.1	57	2049-2068	**Social Security Numbers:** Given the widespread breaches that have compromised the vast majority of Social Security Numbers for American adults, we question whether risk of identity theft is truly heightened through use of Social Security Numbers. We certainly agree with the drive to protect privacy and to enhance security. At the same time, the proverbial toothpaste is out of the tube so to speak. SSNs are quite valuable for identity resolution for CSPs and for matching subscribers to RP records as this section notes. We question why SSNs are being singled out over, say, phone numbers or bundles of Name, Date of Birth, Address in terms of actual risk based on market conditions.	
63	63C	1, 3-5.11	1, 9-77	418,617-2	**Introduction:** In the opening of SP 800-63C, NIST stated that it is specifically interested in comments and recommendations on user-controlled wallets and if they are described clearly enough to support real-world implementations. ID.me is pleased to see NIST leaning into the concept of digital wallets, but ID.me believes there are a few areas that would benefit from clarification: the definition of a digital wallet and delineating the different types of wallets. On page 1 of the C volume, NIST equates a "subscriber-controlled *device* onboarded by the CSP" to a digital wallet. ID.me strongly believes linking the definition of wallets to devices and client-side examples is too narrow. A digital wallet is any wallet provider that binds attributes and credentials to authenticators and leverages federation and other techniques to make those attributes and credentials move with the user. For example, PayPal is a well known digital payment wallet that does not require the use of a native mobile app to use the service. Digital Wallets can be: - **Server Side:** Server side models include ID.me, PayPal, and CLEAR. - **Client Side:** Client side models include Apple and Google. - **Hybrid:** Wallets can combine attribute and credential storage with server and client side storage depending on the nature of risk, user preference, and other considerations. Importantly, the current language throughout Sections 3 and 5 does not distinguish between CSPs that issue legal identity credentials (e.g. ID.me) and "IdP / Wallet" services that receive credentials from other issuers (e.g. Apple with an mDL). In order to increase clarity on the different types of wallets, ID.me recommends that NIST state separate definitions in relation to each credential to make the wallet and credential issuer relationship clear.	For Digital Wallets that can specifically issue IAL2 or other legal credentials, we recommend NIST adopt the term Issuer Digital Wallet. - **Issuer Digital Wallet.** An Identity Provider (IdP) that can issue legal identity credentials, provision attributes, and bind them to authenticators for re-use. This term would be interchangeable with a Full Service Credential Service Provider (CSP) that issues IAL2/AAL2 credentials. These Issuer Digital Wallets can also act as Holder Digital Wallets for credentials issued by third party organizations. Examples would include ID.me, Login.gov, CLEAR, and 1Kosmos. These can be either server-side or client-side. - **Holder Digital Wallet.** An IdP that can issue, receive, store, and transmit credentials and attributes but does not issue legal ID credentials directly. Examples would include Apple Wallet, Google Wallet, and SpruceID. These can be either server-side or client-side.