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:	*SSA*
Name of Submitter/POC:	***Jeffrey Walsh***
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment Type	Comment	Suggested Change
	All	N/A	N/A	N/A	Substantive	Incorporate AI guidance.	We recommend that the NIST guidance recognize applicable AI guidance (e.g., M-24-10) to the extent it interplays in the identity proofing or authentication process. For instance, Section 3.8 discusses requirements for AI and ML in identity systems.
	63-Base	1	1	362	Admin	Misspelling.	Change "considerations **and** organization "to considerations **an** organization"
	63-Base		2	379	Admin	The term 'culturally appropriate' is not defined.	If no definition or concrete examples exist, the clarity of the sentence would be improved by removing the term 'culturally appropriate', which may come across as either confusing
	63-Base		2	383-384	Admin	The last sentence in the paragraph is confusing as it is not clear as to which requirements/functions/entities (and their relationships) it is describing.	Recommend clarifying the language to read "This revision addresses these challenges by clarifying requirements **FOR ALL STAKEHOLDERS** based on the **ROLE OR** function **OF A GIVEN** entity **WITHIN** the overall digital identity model."
	63-Base		4	448	Admin	Punctuation.	Change "CSP issued" to "CSP-issued"
	63-Base		5	487-488	Admin	Punctuation. ADD 2 commas - one after each "manage"	...that they manage, and that their service providers and business partners manage, on behalf...
	63-Base		5	504-505	Admin	Punctuation. Why is Federated Assurance Levels capitalized and not the preceding types?	Make all types consistently cased in the sentence (uppercase?)
	63-Base		6	539-540	Admin	Grammar/structure - repeated terms?	Remove "supported by the privacy risk assessments that are"…
	63-Base	1.3.2	6	541	Admin	Grammar.	Change 'storing' to 'storage'
	63-Base	1.3.2	6	543	Admin	Punctuation.	Remove extra space: "Organizations ,"
	63-Base		6	546-548	Admin	Punctuation and capitalization? Use semi-colons? Why is Fair Information Practices capitalized? Missing word?	…in understanding what PII is**;** the relationship between protecting the confidentiality of PII, privacy, and the Fair Information Practices**;** and safeguards for protecting PII.
	63-Base	1.3.2	6	549	Admin	Was the base volume intentionally excluded from the list of volumes?	Add it if appropriate
	63-Base	2	10	632	Admin	Word missing.	Should be: "The SP 800-63 guidelines use digital identity models that reflect technologies and architectures that **are** already currently available in the market."
	63-Base	2.1	10	640	Admin	Punctuation.	Extra hyphen. Should be: "Subscriber — The…"
	63-Base	2.1	10	646	Admin	Misspelling.	Should be "relying."
	63-Base	2.1	10	646	Admin	Inconsistent capitalization	Change "Identity provider" to either "identity provider" or "Identity Provider".
	63-Base	2.2	11	672	Substantive	The responsibility to "guard against theft" is not borne by the subscriber alone, but is a shared responsibility between the CSP and subscriber. The subscriber does have a responsibility, however, to not engage in **willful** disclosure of authenticator secrets to others, as occurs in credential sharing.	Change "control" to "exclusive control"; and "e.g., guard against theft" to "e.g., take reasonable measures to guard against theft and not willfully provide others with their authenticator secrets")

	63-Base	2.3.1	13	712 - 714	Admin	Grammar - missing verbs	Should be: "Symmetric keys are generally chosen at random, **are** complex and long enough to thwart network-based guessing attacks, and **are** stored in hardware or software that the subscriber controls."
	63-Base	2.3	13	730	Substantive	Driver's license authentication method	Could a driver's license not be used as an online authentication method if verified through the authoritative source?
	63-Base			730-732	Substantive	The example of using a driver's license to 'authenticate' to a person is confusing even to people with some level of DI expertise (see above), especially in a document where authentication is defined as "the process by which a claimant proves possession and control of one or more authenticators bound to a subscriber account to demonstrate that they are the subscriber associated with that account."	Remove lines 729-732.
	63-Base		15	775	Admin	Wording - change the word "in"…	Minimizing data "maintained by", perhaps?
	63-Base	2.4	15	775-776	Substantive	RP will still need to continue to store user PII to take in the verifying user data, as well as the assertion from the federated partner correct?	Readers found this confusing. Recommend a change to: "Minimizing the data, including PII, that RPs need to collect, store, or dispose of"
	63-Base		15	790	Admin	Wording - change the word "detailed"…	The following lists detail OR The following list details…
	63-Base		15	791	Admin	Wording - change the word "the"…	in which **an** organization…
	63-Base		19	874	Admin	Missing words	for **access to** an online service…
	63-Base	2.5	19	891	Substantive	Regarding the wallet, it states the RP establishes a trust agreement with the CSP through the user of federation, and that this arrangement allows the RP to accept assertions from the subscriber controlled wallet without a need a direct trust relationship with the wallet. Therefore, the wallet does not hold completely trustworthy documents, it still needs to send assertions from the CSP to the RP with each transaction?	Provide clarification
	63-Base		20	Fig.5	Admin	Is this Fig.5 image out of place?	Should this be before or after the relevant bulleted lists rather than seemingly in amongst the list items?
	63-Base		21	916	Admin	Missing words	for **access to** an online service…
	63-Base		21	920	Admin	Wording - change "including"…	…bundles can be found **in** Sec…
	63-Base	3	22	931	Substantive	"Risk to the online service" -- the online service is merely a façade to a broader program, and harms from the first dimension will be the program, not the online service. For example, if a person can falsely represent themself as a beneficiary and redirect a benefit payment, the harm is to the program, not the online service.	Change "risks to the online service" to "risks to the online service or underlying program"
	63-Base		22	943	Substantive	This presuposes an understanding of what federation means, which is not a clear concept for many readers	Define federation.
	63-Base		23	956	Admin	Wording - remove 'or necessary'	For example, assuming that aspects of the identity system are not sufficiently privacy-enhancing, usable, equitable, or able [or necessary] to address specific real-world threats:
	63-Base		23	959	Substantive	Legitimate users may face barriers to identity proofing. For example, where proof of address is required as a fraud prevention measure, that will create a barrier to a homeless individual with a pre-paid phone. Bias is a type of barrier that involves prejudice. It is therefore covered under the concept of a barrier, so should only be explicitly called out if there is evidence of prejudice in government identity proofing processes. If such prejudice existed that would be a serious issue, so if there is evidence specific examples should be provided.	Remove the phrase "including biases" which implies that prejudice is part of the identity proofing processes used by agencies.

	63-Base		23	964-965	Substantive	It is understandable that usability issues can be a barrier to some individuals presenting an authenticator successfully. For example, authenticator apps may change numbers too quickly for some users to successfully enter them as a second factor. However, what 'bias' or prejudice could be at play during a failed authentication attempt? Not mentioned is that the *availability* of an authenticator may be an issue, such as when someone loses their phone or fido token.	Replace 'including biases' with 'including availability'
	63-Base		24	997	Substantive	Recommend *requiring* that DIRMs be conducted prior to a system being granted an Authority to Operate. If Digital Identity risk is not understood, then a system may be made available to the public where the risks of digital identity errors are unknown. This can lead to users, data, and systems being exposed to unnecessary risks that could remain invisible to an agency, particularly when those risks primarily involve loss of sensitive data where users may never learn where their data was stolen from, and where the agency may remain unaware of a breach for extended periods.	Change 'SHOULD' to 'SHALL'
	63-Base		24	999	Substantive	Recommend requiring that agencies obtain DIRM evidence from CSPs. If this is not required then it may be overlooked, which increases the vulnerability of users to impacts such as theft and identity theft.	Change 'SHOULD' to 'SHALL'
	63-Base		24	1000	Admin	Missing word	...adherence to the DIRM **process** as…
	63-Base		27	1083	Admin	Privilege is not defined	Add to glossary
	63-Base	3.1	27	1101	Substantive	The partitioning of service into "user groups" implies that (1) all users in a group implicate the same risk, and (2) all users in a group will engage in equally risky transactions. Neither is true of many services. Many services expose many transactions to users that both collectively and individually encompass different risks. In the example of "tax preparers who file tax returns on behalf of their clients", considerations might include, for instance, the number of clients, the value of the returns, individual returns of unusually high value. The concept of a "user group" of tax preparers does not capture this granularity.	The construct of "impacted entities" and "user groups" misses a key third dimension: "transactional scope", which defines the span of control and limitations associated with the user's activity. In the case of the tax preparer, there may be several transactional scopes (e.g., "fewer than 10 returns", "10-100 returns", etc.) The transactional scope is a key driver of risk -- an individual who can file 10,000 returns can be expected to cause far greater harms than an individual who can file 10.
	63-Base		24	1021-1022	Substantive	The impacts on the agency itself also needs to be assessed, as well as any other impacted entities. For example, beneficiaries may not be direct users of an application for appointed representatives for those beneficiaries, but should nevertheless be considered since their information would be exposed if a DI error were to occur.	"...for each user group of the online service**, as well as for the impacted entities including the agency itself**."
	63-Base		24	1028	Substantive	See comment for lines 1021-1022. The impacted entities analysis needs to be considered during the user group analysis.	Recommend adding this sentence after 'respectively.' in line 1028: "The risks to impacted entities, if a particular user group were to be impacted by a DI error, should be incorporated with the direct impacts to that user group." H98
	63-Base		25	1059	Admin	There are up to three xALs that may require modifications. The current wording implies that only one level may change.	"potentially modifying the assurance level**(s)**...
	63-Base		25	1064-1066	Substantive	What are 'enabling tools'? What are the different types of 'operational approaches'? These concepts are undefined. If they are necessary, they should be clarified. If not, we recommend dropping them.	Change: "...and complete and document the normative mandates and outcomes of each step regardless of operational approach or enabling tools." to: "...and complete and document the normative mandates and outcomes of each step."

	63-Base		25	1068	Admin	The current wording is verbose and potentially confusing: "The purpose of defining the online service is to establish a common understanding of the context and circumstances that influence the organization's risk management decisions. The context-rich information ascertained during this step is intended to inform subsequent steps of the DIRM process. The role of the online service is contextualized as part of the broader business environment and associated processes, resulting in a documented description of the online service scope, user groups and expectations, data processed, and other pertinent details."	Suggested simplification: "The purpose of defining the online service is to understand its functionality and establish a common understanding of its context, which will inform subsequent steps of the DIRM process. The role of the online service is contextualized as part of the broader business environment and associated processes, resulting in a documented description of the online service scope, user groups and expectations, data processed, and other pertinent details."
	63-Base		26	Fig.6	Admin	Fig.6 process diagram seems out of place here	Recommend placing this Fig.6 process diagram BEFORE Section 3.1
	63-Base		26	Diagram Step 2	Substantive	Step 1 in the diagram includes impacted entities, but those entities are not considered during the rest of the DIRM process, which seems to be a significant oversight. Not all impacted entities will be 'direct users' so will not be part of a user group, such as the agency itself. In the case of an application for the appointed representatives of beneficiaries, the beneficiaries themselves would be impacted by a breach, but at are not direct users of the system.	Amend Step 2 so that it explicitly includes impacted entities: Step 2: Conduct Initial Impact Assessment for each User Group and impacted entity.
	63-Base		27	1084-1086	Substantive	…"accessibility and language requirements, and culturally responsive communication alternatives" What are 'culturally responsive communication alternatives', and how are they different from 'accessibility and language requirements'?	Either remove the phrase 'culturally responsive communication alternatives' or replace it with examples or a definition.
	63-Base		27	1090-1091	Substantive	This reads as though it is asking for an estimate of whether different types of evidence are available to a given population... generally, yes. BUT is the intent for RP to estimate the percentage of a given prospective population (of users of a particular service) whose members actively maintain that required identity evidence?	Clarify the language to focus on whether users of a given service are likely to POSSESS the required identity evidence
	63-Base		27	1120	Admin	Missing word?	…agencies SHALL document all [word?] impacted when conducting their assessments.
	63-Base	3.2	28	1128	Admin	The first dimension of risk is to the online service per line 931.	Change "the first dimension of risk (i.e., risks to the identity system)" to "the first dimension of risk (i.e., risks to the **online service**)"
	63-Base	3.2	28	1146-1147	Admin	The following sentence is confusing and seems unnecessary given the information that precedes it: "The effort focuses on defining and document the impact assessment to promote consistent application across an organization."	Remove the sentence
	63-Base	3.2	29	1163	Substantive	Section 3.1 defines potential harms to both user groups and impacted entities	Update the sentence to include user groups: "SHALL consider potential harms for each of the impacted **user groups and** entities identified in Sec. 3.1"
	63-Base		29	1172	Admin	missing oxford comma?	...planned resource constraint**s,** or an inability or…
	63-Base		29	1174	Admin	missing oxford comma?	...standin**g,** or reputation:
	63-Base		29	1177-1179	Admin	wording and sentence structure - commas?	Re-word the sentence… "…resulting in the fostering of a negative image, the deterioration of existing trust relationships, and an inability to forge potential new trust relationships in the future."
	63-Base		30	1186	Admin	missing oxford comma?	...or exposure of intellectual propert**y,** or unauthorized disclosure of other...
	63-Base	3.2	30	1191-1192	Admin	Missing words	Change to "actual or potential **loss of** employment or sources of income"
	63-Base		30	1192-1193	Admin	missing oxford comma?	...loss of accessible affordable housing**,** and/or other financial loss.
	63-Base		30	1194-1195	Admin	wording and sentence structure - commas?	Re-word the sentence… "...Harms to the organization may include costs related to fraud or other criminal activity, **as well as** loss of assets, devaluation, **and/**or **a general** loss of business **volume**."

	63-Base	3.2	30	1198	Substantive	The significance of the impact category which captures physical danger up to and including loss of life will be substantially diluted if it treats non-falsifiable 'emotional well-being' as equivalent to physical harms, rather than as an impact that arises as a result of a physical harm.	Retain the impact of having a rating above zero in the physical harm category by removing "mental or emotional well-being" as a primary impact and emphasizing it as a secondary impact, such as how "psychological injury" is appropriately included in the unauthorized access to information category. Suggested change: "Harms to individuals may include death; damage to or loss of physical well-being **which may also result in emotional harms**; or impact to environmental health..."
	63-Base		30	1201-1203	Substantive	wording and sentence structure - commas? No mention of environmental impacts…	Re-word the sentence… "...include damage to or loss of the organization's workforce, **damage to the surrounding environment,** and the **subsequent** impact of unsafe conditions…"
	63-Base	3.2.2	30	1205	Substantive	Section 3.1 defines potential harms to both user groups and impacted entities	Update the sentence to include user groups: "...impacts **on user groups and** entities identified in Sec. 3.1"
	63-Base	3.2.2	30-31	1206-1274	Substantive	categories, such as a loss of Medicare coverage. Such a loss of coverage can lead to financial loss, endanger someone's health, and lead to extreme stress at a time when someone may be suffering from serious health conditions. Delays in receiving disability benefits can also lead to a cascade of negative consequences that can be incredibly detrimental and hard to	Consider adding an additional Impact Category such as "Quality of Life Degradation"
	63-Base	3.2.2	31	1225	Substantive	Under "Degradation of mission delivery", consider using "program" rather than "organization" to measure impact. For an organization that operates many programs, a harm that seriously degrades the program (to the point it can no longer operate) may have limited impact on the broader organization -- but nonetheless result in harms to individuals who rely on the specific program.	On lines 1225, 1228, and 1231, change "organization" to "program" (or "organization or program")
	63-Base	3.2.2	32	1259 & 1263	Substantive	While it is possible to anticipate the types of medical treatments that would be required for minor physical injuries, it is not possible to anticipate whether a minor injury may lead to the need for mental health treatment.	Remove "including mental health treatment".
	63-Base		32	1261	Admin	missing commas	...to prevent further**,** or reverse existing**,** damage.
	63-Base		32	1265	Admin	missing commas	...to prevent further**,** or reverse existing**,** damage;…
	63-Base		32	1269	Admin	missing commas	...to prevent further**,** or reverse existing**,** damage,…
	63-Base	3.2.2	32	1276	Admin	missing comma	Low, Moderate**,** or High
	63-Base	3.3	34	1332	Substantive	In assessing the initial IALs, organizations do not select specific individual controls, but rather a set of controls commensurate with the risk of the service. Suggest a language change to clarify this expectation.	Change "The purpose of the initial assurance level is to identify baseline digital identity controls" to "The purpose of the initial assurance level is to identify a baseline set of digital identity controls"
			34	1347	Admin	AAL is defined later in the document as "the level of assurance that the claimant is the same individual to whom the credential or authenticator was issued." This is a simpler and clearer definition.	Recommend replacing: "The robustness of the authentication process itself, and the binding between an authenticator and a specific individual's identifier." with "the level of assurance that the claimant is the same individual to whom the credential or authenticator was issued."
	63-Base		35	1363-1364	Admin	Unnecessary wording - simplify…	IAL2 **requires** the collection of additional evidence and a more rigorous process for validating…
	63-Base	3.2.2	36	Table 2:AAL2	Substantive	"Support" for MFA is not the same as a requirement for MFA.	Change "Support multifactor authentication" to "Requires multifactor authentication" or "Enforces…"
	63-Base	3.2.2	36	Table 2:AAL3	Substantive	"Providing" (the option of) phishing resistance is not the same as a requirement for phishing resistance.	Change "Provide phishing resistance" to "Requires phishing resistance"
	63-Base		38	1440	Substantive	While not common, the guidance has historically allowed individuals to identity proof directly to an application (with no authenticator). If this remains allowed, it is inconsistent with the statement that "authentication is required for online services that do offer access to personal information..."	If access based on identity proofing is still allowed, add "...where the online service does not require separate identity proofing at each encounter."

	63-Base	3.3.3.2	38	1448	Substantive	The statement that EO13681 requires AAL2 for services that make personal information available is not strictly accurate. An AAL1 implementation that required MFA as a supplemental control would be acceptable. AAL2 introduces other requirements, such as shorter reauthentication intervals, which may add unnecessary burden for low-impact services and are not covered by 13681.	Lines 1442-1448 (including the EO13681 reference) can be moved to Section 3.4 and considered in the tailoring phase. In the specific case of EO13681, a baseline of AAL1 is appropriate if the impact of an authentication error is LOW. During tailoring, the organization may choose to adjust controls or xALs to achieve compliance where necessary. For instance, if an organization sets a baseline of AAL1 for a service that exposes PII, it may (per EO13681) adjust the xAL to AAL2 or incorporate MFA as a supplemental control, both of which would be consistent with 13681.
	63-Base	3.4	40	1494 - 1495	Admin	Grammar.	Should be: "These risks inform the tailoring process and seek to identify…"
	63-Base	3.4	40	1501 - 1502	Admin	Readability.	Should be: "This process focuses on assessing for unintended risks, specific environmental threats, and equity, privacy, and usability impacts."
	63-Base	3.4	40	1505	Admin	grammar - remove 'of'	Change 'aligning **of** digital identity controls' to 'aligning digital identity controls'
	63-Base		40	1507-1512	Substantive	Marginalized and historically underserved populations are those which are often most severely impacted by DI errors that can result in things such as stolen benefits or identity theft. Yet the tailoring instructions direct agencies to focus exclusively on frustrations with the DI controls themselves.	Add: "These considerations should be weighed against the disproportionate impacts that may be experienced by these same populations in the event of a DI error."
	63-Base		40	1517	Admin	missing commas	...are given due consideratio**n,** for tailoring purposes. As a resul**t,** the organization may
	63-Base		41	1540	Substantive	Recommend that the SHOULD be changed to a SHALL. Without a SHALL, it will be more challenging to justify the allocation of the resources needed to implement the collection and analysis of the required MI/BI	
	63-Base		41	1544	Substantive	Keeping individuals safe is also critical.	Change to "…while supporting **security**, equity, privacy, and usability for individuals."
	63-Base	3.4.1	41	1554 - 1555	Admin	Grammar.	Should be: "Identify unintended consequences to the privacy of individuals who will be subject to…"
	63-Base	3.4.1	41	1557 - 1559	Admin	Incorrect acronym and awkward wording.	Should be: "A privacy assessment SHOULD leverage an existing Privacy Threshold Analysis (PTA) or Privacy Impact Assessment (PIA) as inputs during the privacy assessment process."
	63-Base		42	1574	Substantive	Marginalized and historically underserved populations are those which are often most severely impacted by DI errors that can result in things such as stolen benefits or identity theft.	Extend the final sentence: "The intent of this assessment is to mitigate potential impacts on marginalized and historically underserved groups and limit disproportionate impacts from the requirements of the identity management functions **while providing adequate protections against impacts of the fraud and impersonation that can occur when those functions fail.**"
	63-Base		42	1576	Admin	Readability/wording?	...result in **unnecessary** challenges **within** the end-user experience.
	63-Base	3.4.2	43	1614	substantive	By itself, a Federal background investigation does not substitute for evidence validation (i.e., an attacker could provide a counterfeit identity document naming the individual who was the subject of the investigation). It could, however, provide confirmation in the authenticity of alleged attributes. (For instance, if an address was confirmed in a recent federal background investigation, it could lend legitimacy to the authenticity of that address.)	"A Federal agency could choose to use information confirmed as part of a prior Federal background investigation to compensate for the identity evidence verification with authoritative sources or core attribute requirements under these guidelines."
	63-Base	3.4.3	44	1644	Admin	Punctuation.	Should be: "An organization could choose to implement risk-scoring analytics, coupled with re-proofing mechanisms, to confirm users' identity when their access attempts exhibit certain risk factors."
	63-Base		44	1669	Substantive	Wording mischaracterizes the subject of programmatic gaps related to balancing risk management objectives	...may hinder identity management systems in a manner that balances risk management objectives.

	63-Base	3.5.2	46	1714	Substantive	It is problematic for unique users to include both legitimate users and imposters in measuring metrics such as pass rates. DI is a dual-objective problem, where it is objectively proper for agencies to fail imposters and pass legitimate users. Requiring CSPs to include imposters in their pass rate will impart a performance penalty on programs with high imposter rates, and incentivize allowing through imposters.	At the end of 1715, add the sentence: "In calculating metrics, where permitted by documented organizational policy, organizations MAY exclude attempts arising from known or suspected improper use, activity that violates the organization's policies, or technical anomalies."
	63-Base	3.5.2	46	Table 4	Substantive	Fail rate - it is unclear if the term "unable to successfully complete all the steps" applies to users who may have started the process but remain pending (e.g., a user who was sent a confirmation code that is not yet expired)	Add "Pending rate" as a metric, representing percentage of unique users who have started but not yet completed the identity proofing process. Pass rate + Fail rate + Pending rate should sum to 1.
	63-Base	3.5.2	46	Table 4	Substantive	Adjusted fail rate - transactions may not be terminated for suspected fraud, but instead fail through normal controls and later be identified. The adjusted fail rate should include these transactions.	Change "terminated based on suspected fraud" to "suspected to be fraudulent"
	63-Base	3.5.2	46	Table 4	Substantive	Authentication failures - clarification of "authentication event" would be helpful. Is the event an instance of a user attempting to sign in (where they may use multiple authenticators), or use of a single authenticator as part of an authentication attempt?	Clarify meaning of "authentication event"
	63-Base	3.5.2	46	Table 4	Substantive	With respect to fraud, this guidance is only considering identity fraud, not all fraud. An applicant who, for instance, misrepresents the severity of their medical condition in the course of applying for disability benefits, should not be considered in this metric.	Ensure metrics relating to fraud are scoped only too identity fraud, and not other types of fraud a program may encounter (e.g., eligibility fraud)
	63-Base	3.5.2	46	Table 4	Substantive	(Re fraud metrics) "Percentage of digital transactions" is not a particularly useful metric for measuring fraud, as some schemes may require multiple transactions using the same credential; in the case of credentials issued under a false identity, the more useful metric is "Percentage of credentials reported..."	See comment
	63-Base	3.5.2	46	Table 4	Substantive	(Re fraud metrics) NIST may want to rename "confirmed fraud" to "administratively-confirmed fraud" to avoid contention with fraud confirmed by the judicial system, e.g., in a criminal conviction. See GAO-14-704G ("Green Book"): "Whether an act is in fact fraud is a determination to be made through the judicial or other adjudicative system and is beyond management's professional responsibility for assessing risk."	See comment
	63-Base	3.5.2	46	Table 4	Substantive	In general, these metrics are defined at a high level that may not comport with existing metrics an organization may employ. It is important that organizations have flexibility to define metrics and measures as is suitable for the organization. Defining the table as a SHOULD, as NIST does, is appropriate.	No change - NIST struck a good balance between providing metrics and offering flexibility to adopt and refine as appropriate.
	63-Base	3.5.2	46	ble 4 - All Rows	Substantive	While it is clearly important that legitimate users who are improperly rejected have redress mechanisms available, the section as written seems one-sided, focusing almost entirely on avoiding adverse impact and giving limited attention to ensuring that these redress channels do not provide adversaries with opportunities to commit fraud by exploiting weaknesses in these channels. It is important that CSPs offer redress options that are not only broadly available, but also secure and robust to exploitation.	Add language to the effect of: "Organizations SHALL assess the integrity and performance of their redress mechanisms and implement appropriate controls to prevent, detect, and remediate attempted identity fraud involving the organization's redress mechanisms.

	63-Base		48	1726	Substantive	There is a real risk that focusing exclusively on equity & accessibility will result in greater harms being done to vulnerable individuals whose money and data are then stolen due to a reduction in effective controls.	Change to: "A primary purpose of continuous improvement is to improve Equity and Accessibility outcomes for different user populations **in a way that does not result in a substantial increase in fraud or theft of PII or personal or sensitive information."**
	63-Base	3.6	48	1748	Admin	Grammar.	Should be "impact" instead of "impacts."
	63-Base	3.6	49	1766	Substantive	Avoid "people" as a term related to redress.	Regarding redress, suggest replacing "people" with "individuals" or "natural persons" since corporations and some unincorporated groups are also considered "people." Also would avoid having to provide redress to non-person entities such as bots, etc.
	63-Base	3.7	50	1800	Admin	No reason for "Could" to be capitalized.	Should be: "...TTPs that could impact identity proofing…"
	63-Base	3.8	50	1820 - 1823	Admin	Poorly worded.	Suggest: "The potential applications of AI/ML are extensive. These technologies may also introduce distinct risks or result in disparate outcomes, biased outputs, or the exacerbation of existing inequities and access issues.
	63-Base	3.8	51	1836	Admin	No italics needed because it is not a document title. For consistency, no parentheses needed, just brackets. Also, 'the' is missing.	Should be: "...systems SHALL implement **the** NIST AI Risk Management Framework [NISTAIRMF]."
	63-Base	3.8	51	1841	Admin	Recommend expanding the acronym	Should be: "U.S. Artificial Intelligence Safety Institute."
	63-Base			1989	Admin	Capitalization of FedRAMP	
	63-Base	App. B	67	2322	Substantive	The term "Digital Identity" is defined in a very narrow technical context ("an attribute or set of attributes"), where the term is used much more broadly throughout the guidance.	Consider a broader definition. "The unique representation of a subject involved in a digital transaction" (e.g., from 63-3). Suggest "digital transaction" rather than "online transaction" because not all digital transactions occur online.
	63-Base	App. B	69	2360	Substantive	The definition provided for FIPS is an explanation, not a definition.	Consider the definition from FIPS 201-3: "A standard for adoption and use by federal departments and agencies that has been developed within the Information Technology Laboratory and published by NIST, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology to achieve a common level of quality or some level of interoperability."
	63-Base	App. B	69	2734	Substantive	The definition of tailoring does not include modification arising from consideration of organizational threats and risks, as described on lines 1559-1591.	Define as: "The process by which xALs and specified controls are modified by: considerations for the impacts on privacy, usability, and equity on the user population; **considerations for organizational risks**; applying scoping considerations…" (bolded text added)
	63A	Title page				Ryan is listed as an author twice on the first and second pages	
	63A	2.4.2.4	13	760 - 767	Substantive	Inadequate authority.	We recognize that SSA issues Social Security numbers (SSN). We are concerned that the reference at section 2.4.2.4 implies that SSA will provide verification of SSNs for digital identity verification purposes. SSA does not have legal authority to provide SSN verifications to assist with digital identity verification purposes under current Federal law. Accordingly, we do not believe it appropriate to imply that it is appropriate to obtain SSN verifications from SSA as the authoritative source in connection with identity verification needs.
	63A	1	1	378	Admin	Punctuation.	Should be: "...single known individual."
	63A	1	1	382 - 383	Admin	Redundant. A regulation is also a requirement.	Should be: "...real-life subject is required by regulation (e.g., financial industry Customer Identification Program)."
	63A		1	406	Admin	Grammar.	Change "employ" to "employing"
	63A	1.2	2	412 - 413	Admin	Punctuation.	Should be: "...specific real-life person."
	63A	1.2	2	414 - 415	Admin	Punctuation.	Should be: "Evidence is not validated, and attributes are neither validated nor verified."
	63A	1.2	2	419 -420	Admin	Punctuation.	Should be: "...credible sources, and steps are taken…"
	63A		2	428-429	Admin	Unnecessary wording - simplify…	IAL2 **requires** the collection of additional evidence and a more rigorous process for validating…
	63A	2.1	5	505	Admin	Grammar.	Should be: "...applicants involved in the identity proofing process are who they claim to be."
	63A		7	540	Admin	Misspelling.	Verifi**c**ation
	63A		8	590	Admin	Missing comma?	...whether they are attende**d,** and where they take place.
				591	Substantive	Would this identity proofing type include individuals using Interactive Voice Recognition (IVR) as a communication channel?	It would be easier to understand if examples of remote unattended proofing processes were listed. Agencies need specific guidance for identity proofing when IVR, which is a digital channel, is used to provide services.

	63A	2.1.3	8	611	Substantive	The requirement to provide a remote unattended path is overly restrictive. Programs that routinely interface with applicants in-person may not have need for such a path. Further, given the weak document authentication metrics described in Section 3.1.12, organizations may have a legitimate security interest in not offering a remote unattended path, particularly when offering such a path is unnecessary to provide digital access to its service population.	Change to "CSPs that offer services at IAL1 or IAL2 SHOULD provide a Remote Unattended identity proofing process and SHALL offer at least one attended identity proofing process option." (Substantive change in bold)
	63A	2.1.3	8	612	Admin	Misspelling.	Should be: "at least."
	63A	2.4.1.1	10	665	Admin	Capitalization confusion.	Recommend not capitalizing "FAIR" since this also refers to the FAIR data principles: Findable, Accessible, Interoperable, and Reusable.
	63A	2.4.1.1	10	672	Admin	Incorrect name.	Should be: "...Red Flags Rule and accompanying guidelines..."
	63A	2.4.1.1	11	674	Admin	The list contains two number 1 items	674 should be 2, etc.
	63A	2.4.1.1	11	99, & 727, 797	Admin	Incorrect term.	Suggest "facial photo" or "facial image" instead of "portrait," because a portrait could also be a painting, drawing, or other representation of someone's likeness. Line 799 and elsewhere states "image." If used, portrait should be defined.
	63A	2.4.1.1	11	679	Substantive	FAIR evidence requires that "the evidence contains physical security features" but not all examples of fair evidence in Appendix A contain security features in all cases (e.g., student and employee ID cards). Many are printed on stock PVC cards with commodity printers that are specifically marketed for printing corporate ID cards. There is no repository to validate such cards (e.g., how can an examiner be expected to know that an identity card from a school or employer is legitimate?) A document that could be reproduced with a $500 printer and stock PVC card (500 for $40 on Amazon), and perhaps a $1 stock holographic overlay, does not have "physical security features" in any practical sense.	Appendix B should be compared against the standards in 2.4.1.1. Documents that do not conform should be removed from Appendix B. Because card printers can be purchased on the open market for a few hundred dollars (and blank PVC cards for a few cents apiece), the fact that a document is printed on a PVC card should not be considered a security feature. Holographic overlays that can be purchased on the open market should likewise not be considered security features. Unless they contain specific, specialized security features that are known to and can be verified by proofing agents, student IDs and corporate IDs should not be considered FAIR evidence.
	63A	2.4.2.2	13	748	Substantive	The listed evidence validation methods are listed as a set that implies they are roughly equivalent in strength, which is not the case. Provide an indication as to the effectiveness of each method such as listing them in order from least to most effective.	Acceptable methods for validating presented evidence include **the following, ordered from the least effective to the most effective method:** Visual inspection by trained personnel for remote identity proofing; Automated document validation processes using appropriate technologies; Visual and tactile inspection by trained personnel for onsite identity proofing; Cryptographic verification of the source and integrity of digital evidence, or attribute data objects.
			13	763	Admin	Social Security cards (lowercase c)	
				764+	Admin	Social Security number (lowercase n), change throughout	
	63A	2.4.2.4	13	759-774	Substantive	"The CSP SHALL use authoritative or credible sources that meet the following criteria. An authoritative source is the issuing source of identity evidence or attributes, or has direct access to the information maintained by issuing sources, such as state DMVs for driver's license data and the Social Security Administration for Social Security Cards and Social Security Numbers. An authoritative source may also be one that provides or enables direct access to issuing sources of evidence or attributes, such as the American Association of Motor Vehicle Administrators' Driver's License Data Verification (DLDV) Service."	We recognize that SSA issues Social Security numbers (SSN). We are concerned that the reference at section 2.4.2.4 implies that SSA will provide verification of SSNs for digital identity verification purposes. SSA does not have legal authority to provide SSN verifications to assist with digital identity verification purposes under current Federal law. Accordingly, we do not believe it appropriate to imply that it is appropriate to obtain SSN verifications from SSA as the authoritative source in connection with identity verification needs.

	63A	2.5.1	14	785	Substantive	A confirmation code sent to an email address proves access to that email address but cannot provide any identity verification confidence. ONLY confirmation codes sent to postal addresses and phone numbers confirmed to be strongly associated with the applicant are useful for identity verification.	Add: through the return of a confirmation code **sent to a postal address of phone number verified as strongly associated with the applicant in records**,
	63A	2.5.1	14	789	Substantive	Here, the term 'verifiable credentials' is being used generically, but it may be confused with the W3C VC specification. Recommend the use of a generic term instead.	change: 'verifiable credentials' to 'User Controlled Verified Credentials'
	63A	2.5.1	14	792	Substantive	The use of the term "micro transaction" seems to envision a generalization of microdeposits. However, the term "micro" in this context seems inapplicable to non-financial transactions.	"Transaction verification. An individual is able to demonstrate control of a piece of evidence by returning a value based on a transaction made between the CSP and the issuing source of the evidence (e.g., a micro transaction to a bank account)
	63A	2.5.1	14	798	Substantive	Since the top algorithms now perform facial comparisons more accurately and equitably then humans, an option should be provided to allow an algorithmic comparison during an in person proofing session. The is also a role for attended facial image capture for biometric comparison as deep fakes become an increasing threat.	Add this sentence: "Optionally, the photo on the identity evidence can be scanned and algorithmically compared to a photo of the applicant taken by the proofing agent."
	63A	2.5.1	14	808	Substantive	Real-time deep fake technology that can transform the visage of an individual so they appear to resemble someone else already exists and grows more powerful each month. Efforts should be made to detect and counter this technology.	Add something like: "In both cases, steps must be taken to counter deep fake technologies that can transform the face of an imposter in real-time or near real-time to resemble that of the purported applicant."
	63A	2.5.1	15	816	Substantive	Fingerprints, iris patterns, voiceprints, and 'live' facial image captures have all been defeated by bad actors. There needs to be an awareness of the risks, and countermeasures should be taken. Ideally, all remote biometric capture technologies used for identity proofing should require at least annual red-teaming and certification against current threats.	Add something like: "Steps must be taken to counter deep fake and prosthetic technologies during biometric capture and analysis."
	63A		15	817-818	Substantive	The guidance states that knowledge-based verification (KBV) or knowledge-based authentication SHALL NOT be used for identity verification. However, no alternatives are proposed for agencies who use Interactive Voice Recognition (IVR) as a channel of communication, even though it is a digital channel.	Include Caller authentication technologies and methods to determine caller identity in order to prevent impersonation of an account owner without using knowledge-based authentication. Extend guidelines, or provide supplemental guidelines, to include authentication strategies for individuals who use Interactive Voice Recognition (IVR) as a channel of communication.
	63A	3.1.1	16	General	Substantive	The guidance does not specify to whom the practice statement must be made available.	Add: "Where the CSP and RP are not the same organization, the CSP SHALL make the practice statement available to RPs."
	63A	3.1.1	16	General	Substantive	The guidance in Section 3.5.2 (base) encourages CSPs to develop performance metrics, but there is no current requirement to define those metrics in the practice statement.	Consider adding to the list: "A technical description of performance metrics reported by the
	63A	3.1.1	16	844 - 847	Admin	Confusing.	Suggest: 5. CSP policies and processes for validating and verifying identity evidence, including training and qualification requirements for personnel who have validation and verification responsibilities; 6. Specific technologies the CSP employs for evidence validation and verification;
	63A	3.1.1	17	861 - 862	Admin	Awkward wording.	Suggest: "CSP policy for managing and communicating service changes to RPs, such as changes in data sources, integrated vendors, or biometric algorithms."
	63A	3.1.1	17	879	Admin	Capitalization.	Should be: "Resolution, validation, and verification processes…"
	63A	3.1.2	17	883	Admin	Grammar - remove 'a'	change '… is a critical functionality…' to '… is critical functionality…"
	63A	3.1.2.1	18	885	Substantive	3rd party red teaming exercises are a pro-active tool that should be used to stress-test any identity proofing solution.	Add to the CSP Fraud Management list: "CSPs SHOULD conduct independent red teaming exercises annually to validate the effectiveness of their fraud prevention measures. "

	63A	3.1.2.1	18	890 - 891	Substantive	Inadequate.	A Privacy Risk Assessment of all fraud checks and fraud mitigation technologies prior to implementation is okay, but privacy professionals mainly only check for privacy compliance and not anti-fraud measures. That would be a Fraud Risk Assessment. Different team with different skillset supported by different authorities.
		3.1.2.1	18	894	Admin	clarity	Change "an attempt to compromise their involvement in the identity proofing process" to "an attempt to impersonate them during an identity proofing process"
	63A	3.1.2.1	18	903	Substantive	The specific date of death is not necessary to indicate that the subscriber is deceased. A yes/no response is sufficient.	Change "Date of Death Check" to "Death Check"
			18	914	Substantive	Recommend to specifically add age of email address and the email domain, as they have been seen in recent fraud schemes.	Add the following fraud check: "Address Check – For email, evaluate the age of an **email** address and the strength of association between the applicant and that address. Risk factors associated with the ownership of the email domain should also be considered. For mailing address, determine whether the address is a known virtual PO Box or has other high-risk characteristics."
	63A		19	932-933	Substantive	While only a MAY employ condition, shouldn't KBV be broadly discouraged explicitly given the inherent weaknesses in such mechanisms?	Define the limited contexts in which KBV MAY be allowable…
	63A	3.1.2.1	19	939	Substantive	This statement is one-sided; agencies should continuously monitor performance not only for disparate performance but also for functional effectiveness.	Add to item: ", and to ensure continued design and operational effectiveness in mitigating fraud risks."
	63A	3.1.2.1	19	950	Substantive	Agencies must also be cognizant of insider threat risks and should implement appropriate controls (e.g., separation of duties, least privilege, mandatory vacations, analytics, etc.) to limit exposure.	Consider adding a point to the effect of: "CSPs SHALL implement controls to mitigate insider threat risks, such as establishing and ensuring continued suitability of employees and contractor personnel, requiring separation of duties, reviewing activity for suspicious behavior, and integrating proofing activities into their insider threat programs."
	63A	3.1.2.2	20	961	Substantive	Existing guidance (OMB Circ. A-123, GAO 15-593SP) requires agencies to build a fraud risk program.	Change to: "RPs SHOULD integrate digital identity proofing risks into their fraud risk management program consistent with their missions, regulatory environments, systems, applications, data, and resources." Possibly cross-reference to A-123/GAO framework.
	63A	3.1.2.2	20	984	Substantive	This requirement is too specific. Establishing thresholds and actions relates to rule-based detection. Other approaches (ML, Social network analysis (SNA), anomaly-based) may not have thresholds, and to the extent thresholds exist, they may be dynamic as threats change. Anti-fraud thresholds are also sensitive and broad disclosure may give rise to significant insider threat risks since they can allow bad actors who are privy to thresholds to operate under the thresholds to evade detection. While providers should make available their anti-fraud practices and governance, they should not be required to disclose specific thresholds.	Change (1) to language to the effect of: "CSPs SHALL establish and document actions related to each of their fraud checks and practices for managing and operating these measures, and provide these actions and practices to RPs."
	63A	3.1.2.3	20	987 - 988	Admin	Redundancy and grammar. (remove 'see' and 'a')	Should be: "See Sec. 3.6 of [SP800-63] for more information about redress."
	63A	3.1.3.1	21	1000 - 1002	Substantive	Expanding the definition of PII is misguided. Sentence also contains redundancy.	As written, we are expanding the definition of PII to include all images, videos, and scans. While these may contain PII, they are not themselves PII. Also, a facial image is a biometric, so it is redundant to list both.
	63A	3.1.3.1	21	1008 - 1010	Substantive	Does not fully capture the risk.	Why are we only concerned about non-PII that is aggregated by an algorithm? Suggest: "Any non-PII that, when aggregated or processed, could be used to identify a person." Before algorithms, aggregation was manual, but there was still plenty of risk creation.
	63A	3.1.3.1	21	1018	Admin	Spelling.	Should be "reassess."
	63A		22	1027	Admin	Sec. 5 reference formatting	Should be "See Sec. 5."?
	63A	3.1.3.2	22	1039		SSNs are a unique identifier so an attribute derived from them would not be valuable. However, other privacy preserving techniques, such as encryption or hashing can be of value.	Remove: "(e.g., transmitting and accepting derived attribute values rather than full attribute values)" Potential replacement: "(e.g., transmitting and accepting hashed, encrypted, or partial values rather than values transmitted in clear text or full attribute values)"
	63A	3.1.5	24	1090	Substantive	As written, the implication is that only 1 means should be taken to prevent automated attacks.	Change 'implement a means' to 'implement means'

	63A	3.1.5	24	1098	Substantive	The RMF only applies to information security and privacy risks, with other risks being managed through other frameworks (e.g., GAO guidance for fraud risks)	Change "The CSP SHALL assess the risks associated…" to "The CSP SHALL assess the information security and privacy risks associated…"
	63A	3.1.5	24	1102	Substantive	Given the increasing supply chain threats from nation state and other highly sophisticated threat actors, recommend that this SHOULD be changed to a SHALL.	Change 'SHOULD' to 'SHALL'
	63A			1152+	Admin	Base64 is not alphanumeric, as it includes symbols. There are a few references to this	
	63A	3.1.8	25	1154	Substantive	The guidance allows codes to be delivered using a QR code. QR codes may give rise to equity issues, as they require some technical acumen and a smartphone to use.	Consider guidance (e.g., general equity guidance) requiring that if a QR code is provided, a human-readable code must be provided as well
	63A	3.1.8	26	1163	Substantive	It is not clear why the guidance that applies to continuation codes on lines 1181-1184 would not also apply to confirmation codes.	Apply the throttling and storage requirements on 1181-1184 to confirmation codes.
	63A	3.1.10	26	1186	Substantive	An applicant may have more than one validated address.	Change "sent to the applicant's validated address" to "sent to a validated address of the applicant"
	63A	3.1.10	26	1193	Substantive	Recommend that email address NOT be a primary option for a proofing notice. Email addresses are typically checked less frequently (if at all), are far more subject to takeover, are often changed with no forwarding capability, and are generally a less secure communication mechanism than postal or phone. Email is useful as a secondary communication mechanism in this scenario, particularly for individuals who may have moved or switched phone numbers.	Change to: "SHALL be sent to a validated **postal address or phone number strongly associated with the applicant in authoritative records. Notification SHOULD also be sent to a validated email, if available."**
	63A	3.1.10	27	1203	Substantive	In some cases, the CSP may have knowledge that the applicant is under custodial care, has a court-appointed guardian, or similar circumstances. Should the CSP be permitted to send the NOP to that individual rather than the applicant?	If so, add at line 1203: "MAY be sent to an applicant's representative, attorney, guardian, or similar party in place of, or in addition to, the applicant where appropriate (e.g., the applicant is known to the CSP to be incapacitated)."
	63A	3.1.11	27	1208 - 1212	Substantive	Definition conflates several discrete terms. Biometrics is the measurement of life, not an automated recognition as described.	Change to: "Biometric **matching** is the automated recognition of individuals based on their biological **or** behavioral characteristics such as, but not limited to, fingerprints, voice patterns, or facial features (biological characteristics), and keystroke patterns, angle of holding a smart phone, screen pressure, typing speed, mouse movements, or gait (behavioral characteristics)."
	63A	3.1	27	1230	Substantive	Is there a recommended CSP retention period? Or industry standard, or whatever the CSP and RP agree to?	Provide guidance, or a reference to guidance.
	63A	3.1.11	28	1234	Substantive	Organizational policies may restrict whether a request to delete a subscriber's biometric information should be honored (e.g., during an active fraud investigation). Deletion of a biometric can also impair or prevent non-repudiation defenses for IAL3, where a biometric sample must be collected.	Replace "statute" with "policy" on line 1234. (Having both law and statute is redundant.)
	63A		28	1256	Substantive	Biometric matching is typically used for identity verification rather than resolution .	change 'resolution' to 'verification'

	63A	3.1.12	29	1290	Substantive	While we understand from the workshop the motivation beyond a 10% FAR/DFRR, the proposed rate is extremely high -- 1000x the allowed FAR for biometric presentation attacks. If that is the highest rate that can be meaningfully obtained given current technology, it raises the question of whether doc auth should be permitted at all, particularly through unattended remote channels. Further, NIST revealed in the workshop that even 10% is not attainable for all FAIR evidence.	Given data available on the strength of document authentication, NIST should consider whether doc auth continues to be suitable for IAL2 validation. NIST should also consider the requirement to offer a remote unattended path (line 611) in light of this weakness.
	63A	3.1.12	30	1310	Substantive	Results of Doc Auth testing are sensitive security information where public disclosure could be exploited by adversaries to commit identity fraud, particularly given the high FAR in current technology.	Remove (6), or at the least, replace with "CSPs SHALL make a summary of their results publicly available."
	63A		30	1326	Substantive	If trusted referees are provided with tools, but are not required to use them, they will likely not use them because their use will result in higher costs for the CSP. A requirement should therefore be added to require their use.	Change to "...barcode readers)**, and SHALL be required to use the appropriate available tool to inspect the presented evidence."**
	63A	3.1.12	31	1336	Substantive	Language may suggest that employees' performance reviews measure their ability to visually inspect evidence. Is this what NIST intends? Do the contemplated certification programs exist?	Change SHALL to SHOULD
	63A	3.1.13.1	31	1358	Substantive	Certainly, some members of the listed demographic groups will be able to identity proof to a specific IAL.	Change "demographic groups includes" to "demographic groups may include"
	63A	3.1.13.1.	31	1360	Substantive	Individuals with no access to online services to not need to be identity proofed since they will not be able to then use online services.	Change "individuals with **little or no** access to online services" to "individuals with **limited** access to online services"
	63A	3.1.13.1	32	1374	Substantive	The examples pertain to tampered documents but not counterfeit/fabricated documents	Change "material types" to "fabrication or counterfeiting"
	63A	3.1.13.1	32	1380	Substantive	The record should also include the outcome (e.g., the TR's actual decision)	Add to the list of records required: "the trusted referee's decision and, if negative, their rationale."
	63A	3.1.13.2	33	1398	Substantive	Given that CSPs are now required to provide TRs, should the statement on line 1398 be SHALL rather than SHOULD?	See comment
	63A		33	1432	Substantive	Shouldn't the CSP conduct the risk assessment rather than the RP, since they are conducting the identity proofing?	Change RP to CSP
	63A	3.1.13.4	34	1459	Substantive	Given the applicant reference will often be a close associate of the applicant, it may be useful to include a statement that the AR's role is only to support identity proofing, and that the AR has no entitlement to the authenticator.	On line 1459, add language to the effect of: ", and clarify that applicant references are not entitled to access the applicant's subscriber account or access online services on the applicant's behalf."
	63A		36	1501	Admin	Unnecessary word - remove "the"	"...to detect () fraudulent claims to..."
	63A		36	1503-1505	Admin	Readability - Sentence structure	**At IAL1**, the use of biometric matching, such as the automated comparison of a facial portrait to supplied evidence, **is optional - allowing for alternate** pathways to proofing and enrollment where such collection may not be viable.
	63A		36	1516	Admin	Incorrect word - "of"	"...in alignment **with** requirements..."
	63A		37	1545-1546	Admin	Readability - Sentence structure - is correlate the correct word?	"...correlate the data/attributes **from all sources (evidence, self-asserted, and as presented by credible and authoritative sources)** for consistency."
	63A		38	1580	Admin	Grammar - missing article	"...records **the** session.."
			38	1583	Admin	Unnecessary word - remove the first "to"	"...gain consent from the applicant **()** prior to initiating a..."
	63A		38	1587-1591	Substantive	The listed mitigation will help with pre-recorded deep fakes but is inadequate for real-time and near-real time deep fakes where the image of a live impersonator is being manipulated to appear similar to the target user.	Add a requirement to to take steps to detect real-time deep fake technology that uses live actors.
	63A		40	1637	Admin	Grammar - 'a' rather than 'an'	"Return of **a** confirmation"

	63A	4.2	40	1648	Substantive	Biometrics improve security. Requiring the capture of a facial image during identity proofing is a powerful deterrent for community and family-level bad actors. If biometrics are optional at IAL2 then an agency that requires biometrics for security reasons will not be able to accept an IAL2 credential that was established by an agency with a higher risk tolerance. This breaks the consistency and trust that enables federation.	Either require biometrics for IAL2 or split IAL2 so that the use of biometrics during identity proofing is clearly captured and transmitted to all RPs so they can make a decision on its use or absence, and make sure the pathways are clearly marked such as IAL2-B (biometrics) and IAL2-O (other). These two pathways are *not* equivalent from a security and fraud-deterrence perspective. The non-biometric pathway is highly vulnerable to attack by family members, caregivers, and acquaintances, which can lead to devastating financial and life consequences for disabled beneficiaries and the elderly who rely on their benefits. Capturing the facial image of the individual who is applying for benefits is a strong deterrent to impersonation, particularly for individuals who are personally acquainted with a victim. There is no equivalent deterrent in the non-biometric pathway. Individuals with common names are also highly vulnerable to attacks when address verification is used for proofing without sufficient additional controls. Records may show that a number, email address, or home address is strongly associated with a James Smith, for example. There are 38,313 James Smith's in the United States. This is a common attack that is happening at scale today. https://www.statista.com/statistics/279713/frequent-combinations-of-first-and-last-name-in-the-us/
	63A	4.2	40	1649-1651	Substantive	These options DO have different security and assurance outcomes, which effectively waters down the security of IAL2 to the least security option. Also, digital evidence will either be part of the biometric or non-biometric pathway. Why create a third pathway just for digital evidence? Wouldn't it really need to be four pathways in that case? Digital non-biometric and digital biometric?	Acknowledge that these pathways are not equivalent from a security and assurance perspective and rank them, perhaps: IAL2-High (biometrics), IAL2-Moderate (non-biometrics), IAL-low(?). Otherwise, trust and interoperability and therefore the ability to leverage federated credentials will break - an agency that requires IAL2 with biometrics will not be able to accept an IAL2 credential that originated with another agency.
	63A	4.2.2.1	40	1658	Substantive	See comment re line 611; offering a remote unattended option should not be compelled, especially given weaknesses in doc auth	Remove
	63A	4.2.4	41	1685	Substantive	A SUPERIOR document that cannot be cryptographically verified should not be automatically considered to be STRONG. E.g., a PIV card (if not cryptographically verified) is only required to have a single Level 1 security feature (FIPS 201 sec 4.1.2) and cannot be verified by a credible source (63A, section 2.4.1.2). Further, because the FIPS spec does not detail the specific security features, the document cannot be verified as required by 2.4.2.2.	Change "SHALL be considered STRONG evidence" to "SHALL be evaluated for strength in the same manner as other evidence that does not contain cryptographic security features."
	63A		41	1697-1698	Admin	Readability - Sentence structure - is correlate the correct word?	"...correlate the data/attributes **from all sources (evidence, self-asserted, and as presented by credible and authoritative sources)** for consistency."
	63A	4.2.6.1	42	General	Substantive	The combination of evidence validation and postal address confirmation, specified in 2(a), is not at the same level as the digital evidence or biometric pathway, particularly given weaknesses in remote document authentication and availability of services that can make mailings available remotely, such as virtual PO boxes. It does not provide the same confidence in identity as the other IAL2 options and threatens to weaken IAL2 as a whole. It should be considered a form of IAL1+, not IAL2.	2(a) should be considered permissible for IAL1 (or a level between IAL1 and IAL2), but not IAL2.

	63A	4.2.6.1	42	1716	Substantive	The verification requirements for IAL2 could require two separate verification codes. If a person has an SSN card (that has neither a portrait nor address associated with it), or a credit card, or similar, how does the CSP get the associated address? Even if it were possible to get an associated address, would the applicant need to receive two separate confirmation codes (one for the fair evidence, one for the strong evidence)? This creates a significant user burden, and verifying FAIR evidence in the manner outlined is impractical (e.g. credit cards, SSN cards, SNAP cards, etc. do not generally have a portrait).	As with 800-63-3, require verification of the strongest piece of identity evidence, not all evidence.
	63A	4.2.6.1	42	1718	Substantive	Receiving a code at an email address is not in any way equivalent to receiving a code a mailing address or phone number. Email can be accessed anywhere in the world, is likely not protected with MFA, and is highly vulnerable to attacks and breaches.	Remove email address as an option
	63A	4.2.6.1	42	1720-1724 & 1730-1734	Substantive	The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading.	Add a sentence that indicates that these are not equivalent in terms of fraud prevention.
	63A	4.2.6.2	43	1743	Substantive	An ISO/IEC 18013 mDL is already cryptographically verified and unlocked with a biometric. What additional value is to be gained using a microdeposit, confirmation code, AAL2 account, etc.? Or verifying FAIR evidence?	Consider if the burden of the additional verification checks is appropriate for IAL2 for mDL use cases.
	63A	4.2.6.2	43	1745	Substantive	What is meant by a 'validated account'? Does it need to be an account owned by someone with the same name? That is not sufficiently granular for someone with a common name. Does it need to be an account associated with someone's name and SSN? Does length of ownership matter? Note: Association with an address is insufficient. Bad actors can provide a target's legitimate home address and then opt to only receive communications via email.	Provide guidance, or a reference to guidance.
	63A	4.2.6.2	43	1746	Substantive	Recommend prohibiting email. See Comment for 1718.	
	63A	4.2.6.2	43	1762+	Substantive	For all of these methods, provide a reference/link to security and other requirements such as liveness and deep-fake detection that are presumably in another section of the document.	
	63A	4.3.6	46	1847+	Substantive	For all scenarios that involve comparing a portrait on evidence to a person's face over video where the CSP does not control the end user device, there must be an awareness of the rapidly evolving danger posed by real-time face-swap deep fake video manipulations. Measures must be in place to detect this technology if video is to be used for identity proofing. https://www.youtube.com/watch?v=w0Wkhz4G6OA	Provide requirements and guidance to counteract the threat of the rapidly evolving and accessible real-time face-swapping capabilities.
	63A		47 & 48	1863 & 1901	Substantive	Make it clear that more stringent controls are acceptable and can be considered	Add phrase in bold: …are**, at a minimum,** protected consistent with FISMA Moderate..."
	63A		47	1870	Admin	Change to: "If the CSP records **a** session"	
	63A		47	1873	Admin	Remove extra 'to': "from the applicant [to] prior to initiating"	

	63A	5.1	50	1928	Substantive	A requirement should be added that restricts the number of active subscriber accounts per unique individual to ONE. Allowing more than one subscriber account per person 1.) Is fiscally wasteful - tax payer dollars are unnecessarily used to repeatedly identity proof the same individual 2.) leads to an increase in fraud, particularly for accounts obtained without a biometric match. Fraud is inherently inequitable since the most vulnerable individuals are the ones that suffer the most harm when their benefits are stolen or denied because of the actions of a bad actor.	Add something like: "For accounts that require identity, the CSP SHALL maintain a one-to-one mapping between subscriber accounts, credentials, and unique individuals. A CSP SHALL NOT allow a subscriber to have multiple credentials at IAL1 or above. A CSP SHALL allow individuals to register multiple email addresses per account, and to choose which email address to use when authenticating to an RP."
	63A	5.4	51	1976	Substantive	The CSP should not be *required* to terminate/suspend the subscriber account for a policy violation. For example, if a user is known to have shared their password with a relative, the issue can be cured by issuing new authenticators and warning the subscriber to not do so in the future. This guidance would require CSPs to suspend or terminate the account, which is heavy-handed and could result in loss of access to services.	Change line 1972 to: "The CSP SHALL document its policy for terminating and suspending accounts in its practice statement. Reasons to suspend or terminate an account may include:"
	63A		54	Table 2	Substantive	The example given in 'False Claims' may be committed by a legitimate user. Providing evidence to fraudulently claim a privilege that one is not entitled to is out of scope. Change this example to one that applies only to identity proofing.	Change to something like: "An attacker registers an address they control with the attributes of a legitimate user."
	63A		54	Table 2	Substantive	Add clarity so readers unfamiliar with this technology that these attacks can happen in real time.	Change to "A **real-time** deepfake video**, which may utilize face swapping and voice manipulation,** is used to impersonate an individual portrayed on a stolen driver's license."
	63A		55	Table 3	Admin	"indications **or** malicious traffic." -> "indications **of** malicious traffic."	
	63A		57	2046	Substantive	While it is true that PII retained by a CSP can be vulnerable to unauthorized access, it is also critical to the detection and successful prosecution of fraud. When privacy at the CSP is prioritized over the ability to detect and prosecute fraud, legitimate users end up suffering even greater losses of privacy and may suffer devastating financial losses when their RP accounts are then compromised.	Add something like "However, some PII retention is critical to the detection and successful prosecution of fraud, which should be taken into consideration when decisions are made regarding what PII to retain and for what length of time."
	63A	7.1.1	57	2067	Substantive	"The SSN should only be collected where it is necessary to support identity resolution…". As noted in sec. 2.2, collection may also be needed as a core attribute.	Expand statement to allow collection of the SSN as a core attribute.
	63A		59	2112	Substantive	Redress mechanisms can be highly vulnerable to impersonation attacks	Change to "provide effective **and secure** mechanisms for redressing applicant complaints or problems"
	63A		59	2124	Substantive	Bad actors are *known* to have used identity proofing processes to verify PII. To prevent this, the 'should not inform' should be changed to SHALL NOT inform.	
	63A		66	2357	Substantive	Strongly recommend that email be removed as an option due to the vulnerabilities discussed earlier	
	63A	9.2	71	2532	Substantive	The list of mitigations does not include tailoring/compensating controls, which could be effective here.	complaints
	63A	9.2	71	2533 - 2537	Substantive	Misdescription of risk.	"Description: Records held by authoritative and credible sources are insufficient to support the validation of core attributes or presented evidence for applicants belonging to certain user groups, such as those who self-exclude themselves from programs and services due to fears of surveillance or other concerns that might result in a record of their association." This is an incorrect description. Here, the records are sufficient, but the applicant is choosing not to interact with the program or service while simultaneously introducing unnecessary risk into the program or service.

	63A		72	2567	Substantive	Change 'sex assigned at birth', which is political language used exclusively by only one party in the United States, to the neutral 'sex' or 'sex at birth'.	
	63A		72 & 73	2572 & 2592	Substantive	Remove 'residual bias'. 'Technological limitations' accurately and completely captures any challenges with image capture without anthropomorphization.	
	63A	9.3	72	2573	Substantive	The statement that "CSP-controlled kiosks...employ state-of-the-art facial and biometric capture techniques" is questionable -- is NIST endorsing CSPs' biometric capabilities?	Change to "Provide the option for applicants to use onsite attended or unattended proofing, which may provide better capture than an individual can provide in an uncontrolled environment."
	63A		73	2587	Substantive	Consider replacing 'biased' with the more accurate term 'poor quality'.	
	63A		73	2598	Substantive	People have limitations when it comes to accurate facial verification, which is very different than implying that people who are unable to accurately perform verifications are prejudiced.	Replace "biases" with "limitations"
	63A		73	2601	Substantive	When high quality images are used, best of breed algorithms now perform facial verifications more accurately than trained human agents. So, providing an automated option for individuals who have failed verification by a human would reduce false non-matches.	Replace the first mitigation (which is, in all practical ways, identical to the more concisely worded second mitigation), with "1. Provide the option for applicants to have a photo taken which will be algorithmically compared to the portrait on their strongest piece of evidence."
	63A	Appendix A	78	Tab4	Substantive	Some documents (SNAP, debit, SSN card) indicate that they "must be presented with other evidence containing a photo." Can this be the STRONG document (in the case of IAL2) or must it be separate evidence? What are the requirements for this "other evidence"?	Clarify in the document body.
	63A	A.1	79	N/A	Admin	Acronym.	Should be "SNAP."
	63A	ppendix B	83	N/A	Admin	Missing acronyms.	Missing CIP, FIPS, ICAO, KYC, REAL ID, SAOP, SNAP.
	63B	1	1	374	Substantive	"accessing the service" should be "accessing a service", since it the service a user is returning to is not necessarily the one they originally accessed. For instance, it may be necessary to establish that a user accessing a service to track a claim (Service B) is the same person who filed the claim (Service A), despite these being different services.	Change "the service" to "a service"
	63B	1	1	391	Substantive	The protections in this document -- regardless of the AAL -- are ineffective if the subscriber willfully discloses their authenticator secrets (either carelessly or maliciously). The guidance should recognize this limitation explicitly. See also comment on base volume, line 672.	Consider adding: "This guidance recognizes that subscribers are responsible for reasonably protecting their authentication secrets and not willfully disclosing to others (e.g., credential sharing). The protections at AALs are intended to protect against credential theft and are not intended to protect against willful disclosure of credential secrets by a complicit subscriber."
	63B	1	1	397	Admin	Grammar.	Instead of "AALs characterizes...," should be "AALs characterize...."
	63B	2	4	471	Substantive	The wording is ambiguous -- "as desribed in 800-63C" applies to IdPs but not RPs, but can be read to apply to both.	Change "authenticate to RP or IdP as described in [SP800-63C]" to "authenticate to an IdP as described in [SP800-63C] or RP"
	63B	2	4	481 - 483	Substantive	Improper reference.	The scope of EO 13681 is consumer financial transactions, so it is improper to say that the EO mandates multifactor authentication more broadly.
	63B	2	4	484	Substantive	Same as comment for base volume, line 1448: The statement that EO13681 requires AAL2 for services that make personal information available is not strictly accurate. An AAL1 implementation that required MFA as a supplemental control would be acceptable. AAL2 introduces other requirements, such as shorter reauthentication intervals, which may add unnecessary burden for low-impact services and are not covered by 13681.	Lines 1442-1448 (including the EO13681 reference) can be moved to Section 3.4 and considered in the tailoring phase. In the specific case of EO13681, a baseline of AAL1 is appropriate if the impact of an authentication error is LOW. During tailoring, the organization may choose to adjust controls or xALs to achieve compliance where necessary. For instance, if an organization sets a baseline of AAL1 for a service that exposes PII, it may (per EO13681) adjust the xAL to AAL2 or incorporate MFA as a supplemental control, both of which would be consistent with 13681.
	63B	2.5	10	Fig1	Substantive	Consider adding to table the allowance to reauthenticate using a single factor at AAL2.	See comment
	63B		17	857	Substantive	Concrete examples of out of band devices would be helpful.	Provide examples
	63B	3.2.5	33	1360	Admin	British spelling.	Should be "imposter" not "impostor."

	63B	Appendix C	95	N/A	Admin	Missing acronyms.	Missing USB, NFC, QR, OWASP, ASCII, NFKC, and NFKD.
	63B	Appendix D	112	3565	Admin	Incorrect term.	Should be "System of **Records** Notice."
	63B	2.2	6	Section 2.2	Substantive	Realistically, almost all publicly facing applications will require AAL2, and those AAL2 applications will vary significantly in risk from a low/limited impact service where a single individual checks the status of their benefits application (but cannot see the application itself), to a service where a DI error could lead to serious consequences, such as a service used by an attorneys managing dozens of beneficiary claims each who can read the highly sensitive medical records associated with each claim. To protect both types of applications using the same AAL is inappropriate since the risks are so different. 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 impact applications such as applications that allow status for a single user to be accessed. However, for higher risk applications used by populations such as doctors, legal representatives, and accountants, phishing resistance is both appropriate and usable even where full AAL3 compliance may not be either warranted or possible. Yet this guidance would have phishing resistance be optional for both low risk single user access services and moderate risk services used to manage the data of more than one user.	STRONGLY recommend that CSPs be required to offer RP's multiple options for AAL2 to give agencies risk-based options including the flexibility to meet the needs of their customers as well as the ability to enforce greater security when necessary and when the customer base supports stricter options. Please add this requirement: CSP's SHALL support the following AAL2 options: 1. Restricted factors allowed, phishing-resistance optional 2. Restricted factors disallowed, phishing-resistance optional 3. Phishing-resistance mandatory
	63B		11	689	Substantive	Allowing CSPs and agencies to permit the same phone number as the second factor for hundreds of individuals, or for dozens of individuals living in different locations, does not provide sufficient protection against fraud.	Change 'MAY' to 'SHALL'
	63B		14	746	Substantive	Strongly recommend changing this MAY to a SHOULD for 'Passwords obtained from previous breaches' and context-specific words (other than username) and to a SHALL for 'Dictionary words', and 'Username'. To context-specific words, I would also add names of sports teams, mascots, and other pop culture references. Making those changes would increase security and the SHALLs are simple measures to implement.	See comment
	63B		14	758	Substantive	Excessively' large is undefined and this language may lead implementors to use an *insufficiently* large blocklist.	Remove this statement. It is unnecessary and may lead to a reduction in security. If there is justification, such as studies that have shown that a blocklist that contains x entries results in a significant degradation in user password registration experience, provide that information.
	63B		21	940	Substantive	Strongly recommend removing VOIP, which has the same security flaws as email. VOIP should NOT be allowed for authentication or verification. It is very high risk. It should be permissible for notifications only.	See comment
	63B		27	1177-1179	Substantive	I would only consider subscriber-controlled wallets as multi-factor if they are bound to a single device, such as a smartphone. If they are cloud based wallets or are exportable or replicable they should NOT be considered multi-factor.	Add (bold): "As such, **non-exportable single device-bound** subscriber-controlled wallets..."
	63B		37	1512	Substantive	Allowing a second factor to be as far as two city blocks away from the endpoint would seem to introduce unnecessary risk.	Reduce the allowed distance between wireless authenticators and endpoints to the smallest usable and enforceable distance.

	63B		28-29	1216-1217	Substantive	100 is excessively high. The maximum number of tries that a legitimate user requires to successfully authenticate will be far lower. Such a high number is only required by bad actors.	Lower the limit, preferably to 3 but certainly no more then 10.
	63B		30	1274	Substantive	Skin tone is a measurable characteristic that can impact facial verification algorithms. While there is a correlation between skin tone and race and ethnicity, neither race or ethnicity, which are culturally defined, impact biometric measurements or algorithms directly.	Change racial background and ethnicity to skin tone.
	63B		30, 73	1274, 2477	Substantive	While 'gender' used to be a synonym for 'sex', that is no longer the case and someone's stated 'gender' may not correspond to their biology. Since it is biology that impacts biometrics rather than self-identification, 'gender' should be changed to 'biological sex'. (For example, biological females experience greater challenges than biological males with fingerprint capture due to differences in their average ridge depth and finger size.)	Change 'gender' to 'biological sex'.
	63B		30		Substantive	50 and 100 seems excessively high. Why where these numbers chosen?	Reduce the maximum number of attempts to one that corresponds with the maximum number of attempts legitimate users have been demonstrated to require.
	63B		43	1705	Substantive	This is a decision that will impact RP security, so a risk analysis by the CSP is insufficient. All impacted RPs must be involved and must agree.	Add something like: "Any alternative methods SHALL be pre-approved by the CSP's customers."
	63B		43	1723	Substantive	Email is FAR too risky to use as a recovery address. Email is a cloud-based application that typically does not require MFA to access, and may be protected using only a password that has already been breached.	Remove email.
	63B		44	1734	Substantive	See comment for 1723	Remove email.
	63B		75	2535	Substantive	The current wording implies that all or most facial matching algorithms are problematic, which is false - the top algorithms perform well for all tested ethnicities.	Change to "**Some** facial matching algorithms…"
	63B		75	2535	Admin	Awkward wording that unintentionally emphasizes missing fingers	Change to " Some subscribers may have conditions that interfere with fingerprint collection, such as …."
	63B		76	2550	Substantive	This is not an issue of 'technological skill' and is already sufficiently covered by rows 2542-2545. Also, it opens the door for bad actors to 'assist' with 2nd factor code entry, which is typically referred to as a phishing attack.	Recommend removing this example.
	63B		76	2552-2553	Substantive	Old age does not necessarily lead to challenges with holding small objects, which this language implies. Again, the challenges that some individuals experience as they get older are already covered adequately by rows 2544-2545.	Recommend removing this example.
	63B		76	2554-2555	Substantive	Selectively calling out three of the *dozens* of reasons people may struggle with memory (an issue already adequately covered by rows 2544-2545) is inappropriate. At best it is not useful. At worst it perpetuates stereotypes and can be seen as insulting or alienating.	Recommend removing this example.
	63B		113	3603	Substantive	Allowing VoIP such as google voice introduces considerable risk with no compensating benefit.	Reinstate the requirement that VoIP numbers are NOT allowed for out-of-band authentication. It is equivalent to the security of email, which is NOT secure.
	63C	Table 1	4	N/A	Substantive	Confusion of terms.	"A priori" is a legal term that does not make sense in the context used.

	63C		7 & 63	587 & 2348-2353	Substantive	Since the allowable proofing steps for IAL2, and the allowable 2nd factors at AAL2, lead to dramatically different types and degrees of risks, providing the xAL alone is insufficient to achieve adequate and equitable risk management, fraud analytics, or continuous monitoring and improvement. Without this information, RPs will have to assume the least secure and most fraud-prone methods were used for both IAL and AAL and may have to step up their users, which will lead to user inconvenience and increased cost (i.e., wasted taxpayer dollars).	Add the required information (bold): "The IdP SHALL inform the RP of the following information for each federation transaction: •The IAL of the subscriber account being presented to the RP, or an indication that no IAL claim is being made. **If an IAL claim is made, an indicator corresponding to the set of controls used to obtain that IAL SHALL be provided.** • The AAL of the currently active session of the subscriber at the IdP, or an indication that no AAL claim is being made. **If an AAL claim is made, an indicator referring to the type of 2nd factor used SHALL be provided."**
	63C		12	720	Admin	plural	change 'identity attribute' to 'identity attributes'
	63C		17	919-920	Substantive	Shouldn't FALs also be established?	Add FAL: "Trust agreements SHALL establish terms regarding expected and acceptable IALs**, AALs, and FALs** in connection with the federated relationship."
	63C		18	932	Substantive	The trust agreement as described contains information that can be exploited by a bad actor. It should NOT be made available to users, who may well be bad actors seeking to exploit the system's security.	Define a separate agreement for users that contains information they may require, but which does not include exploitable information.
	63C	3.5	22	1046 - 1047	Admin	Punctuation. Misplaced commas.	Should be: "...at “www.example.com,” “service.example.com,” and “gateway.example.com,” then..."
	63C	3.6	23	1094	Admin	Missing article	"..between **the** IdP and RP"
	63C	3.9.1	28	1277	Substantive	Unclear language.	Regarding "When an IdP uses consent measures for this purpose..." it is unclear to which purpose we are referring. If referring to "predictability" and "manageability," then it would be the plural "purposes." If referring to something else, we should be clear.
	63C	3.9.1	28	1267 - 1271	Substantive	Misleading language.	"The IdP MAY additionally transmit the subscriber’s information in the following cases, if stipulated and disclosed by the trust agreement:" Regarding the above in conjunction with the third bullet, an IdP can be compelled to comply with law or legal process regardless of whether there is disclosure in the trust agreement. If an entity is doing something illegal, it is unlikely to voluntarily disclose it.
	63C	3.9.1	28	1279 - 1283	Substantive	Misleading language.	"An RP MAY disclose information on subscriber activities to the associated IdP in the following cases, if stipulated and disclosed by the trust agreement:" Regarding the above in conjunction with the third bullet, an RP can be compelled to comply with law or legal process regardless of whether there is disclosure in the trust agreement.
	63C		29	1288	Substantive	As written, this restricts controls to the moderate baseline.	Change to 'moderate **or higher**'
	63C	3.10.2	30	1344	Admin	Colloquial language.	Consider "should" instead of "it may be a good idea to...."
	63C	3.10.3	30 & 58	1356-1358 & 2172-2173 & 2185-2187	Substantive	Deleting all identifying information in response to someone's request can be easily exploited by bad actors trying to avoid prosecution or detection.	Only delete all information for non-proofed accounts (IAL0). For proofed accounts, retain sufficient information for a pre-determined period of time (perhaps 1 year from last date of account access) to detect suspicious behavior and to prosecute unauthorized access or theft. Deactivating an account should NOT result in the complete removal of information that may later be needed for fraud response.
	63C	3.10.3	31	1361	Substantive	While it is critical to ensure secure storage, it is also critical to retain the ability to detect duplicate accounts and to obtain the information necessary to detect and prosecuted fraud. Excessive privacy at the CSP inevitably leads to far greater losses of privacy at the RP, and leads to theft and privacy violations that can't be effectively prosecuted.	Add something like: "The methods used for secure storage SHALL NOT interfere with fraud analytics or the ability to prosecute individuals who obtained an account fraudulently."
	63C	3.10.3	31	1363	Admin	Incorrect word order.	Should be "are logs" instead of "logs are."

	63C	3.10.3	31	1364	Substantive	This is a dangerous requirement for IAL1+ accounts that will interfere with the detection and prosecution of fraud.	Remove or update this to allow fraud to be detected and prosecuted.
	63C		32	1406	Substantive	The private key is used to sign the assertion, not the public key. The public key is then used to verify the signature.	Change 'the public key used to sign the assertion" to "the public key required to verify the signed assertion"
	63C		32	1414	Admin	typos	1. change 'it' to 'is' 2. remove 'if'
	63C		34	1487	Admin	transposed words	change 'be not' to 'not be'
	63C		34	1498	Admin	Where are the protections listed? Is 'here' supposed to be a hyperlink? Is a list supposed to follow 'here'?	Correct the issue
	63C	3.13	36	1552	Admin	Incorrect word.	Should be "on its own" instead of "own its own."
	63C	3.1.4		1568-1569	Substantive	Does 'the authenticator…SHALL be phishing resistant' mean that authentication must be at AAL3? If so, that should be clear. If not, this is another example of why an AAL2 phishing-resistant required option is needed. As the guidelines are currently written, the use of a VOIP text message as a 2nd factor and the use of a FIPS certified YubiKey are at the same level of assurance.	Either change 'phishing resistant' to AAL3 or creating a phishing resistant AAL2 option and make that the requirement. (Also, disallow VOIP for anything other than user notifications. It's equivalent to an email address for security.)
	63C	3.16	42	1685 - 1686	Admin	Awkward header.	Instead of "Authentica-tors" split between two lines, suggest moving the entire word to the second line of the header.
	63C		47	1807-1808	Substantive	The trust agreement as described contains information that can be exploited by a bad actor. It should NOT be available to users.	Change "The terms of the trust agreement SHALL be made available" to something like "**A summary of the** terms of the trust agreement, **which SHALL NOT contain security details or sensitive information that could be exploited,** SHALL be made available…"
	63C	4.6.1.2	51	1981	Admin	Punctuation. Misplaced commas.	Should be: … “www.example.com,” “service.example.com,” …
	63C		62	2297 & 2306	Substantive	It is critical that RPs and IdPs be informed when either suspects that an account has been compromised, especially when RPs are involved that hold highly sensitive data or allow access to funds. If other means of notification, such as email, are allowed, then changing this to a SHALL should not be a problem.	2297 - Remove this item from the 'SHOULD' list and change to: "The IdP **SHALL** send a signal **or other notification** regarding any subscriber account suspected of being compromised." 2306 - "The RP **SHALL** send a signal **or other notification** regarding any subscriber account suspected of being compromised."
	63C	4.9	63	2346	Admin	Spell out acronym upon first-time use.	"MAC" appears several times in the document and is not spelled out until line 2346.
	63C	5	69	Section 5	Substantive	Recommend removing the section on wallets, and all references to wallets, until, at a minimum, a reference implementation architecture that incorporates all the recommended requirements has been tested during an operational pilot. Without that, these requirements are based on speculation so may contain significant security and usability issues.	Remove all normative and informative sections related to wallets. Issue a supplement to 63 C when following a successful operational pilot.
	63C		71	2539-2540	Substantive	Does this mean that if an agency is acting as an RP, and wants to be able to utilize mDLs for address information, that the agency will need to have trust agreements with the DMV for each US state and territory? If so, that doesn't seem practical and would *severely* restrict the use of mDLs.	Clarify that a trust agreement between an RP and a broker such as AAMVA is permissible, or change to SHOULD.
	63C		71	2543	Admin	Missing article	Should be "as **an** IdP"
	63C		73	2597	Admin	Missing conjunction	Change to 'window, **and** SHALL'
	63C		73	2604	Admin	typos	changing 'singing' to 'signing'
	63C		73	2604 & 2606	Substantive	This phrasing implies that the attribute bundles are signed with the public key, which is not the case. They are signed with the private key and verified by the public key.	Change from 'the attribute bundle signing public key' to 'the public key required to verify the signed attribute bundle'
	63C		73	2609	Admin	It is more accurate and understandable to say that the RP 'obtains' the identifier and key rather than it 'learns' them.	Change 'learns' to 'obtains'
	63C		73	2609	Substantive	This phrasing implies that the attribute bundles are signed with the public key, which is not the case. They are signed with the private key and verified by the public key.	Change 'assertion signing public keys' to 'assertion verifying public keys'
	63C		73	2612	Substantive	Public keys can't 'present' attributes, but they can verify them.	to present' should be 'to verify'

	63C		73	2609-2613	Admin	This paragraph needs to be rewritten for both clarity and accuracy. See also comments above.	Change this: "The RP learns the identifier and assertion signing public keys of the subscriber-controlled wallet as part of the attribute bundle signed by the CSP, presented in the federation transaction. The RP trusts the CSP's onboarding process of the wallet to provide assurance that the public key being presented can be trusted to present the attribute bundle in question." to this: **"Through the federation transaction, the CSP provides the RP with the wallet identifier, the signed attribute bundle from the subscriber-controlled wallet, and the public keys required to verify that bundle."**
	63C		73	2615	Substantive	How does the 'RP introduce its properties'?	Provide an explanation.
	63C		73	2618	Substantive	Which 'trust agreement'?	Be specific
	63C		73	2626	Substantive	Perhaps the writer is confusing how asymmetric cryptography works for signatures vs encryption? Digital Signatures: The *private key* is used to sign a message. The corresponding public key is then used to verify that the message was signed by the expected private key. Encryption: The message is encrypted using the recipient's *public key.* The recipient then uses their private key to decrypt it.	Change 'signed by the CSP's public key' to 'signed by the CSP's private key'.
	63C		73	2614-2627	Substantive	This paragraph needs to be rewritten for both clarity and accuracy. See also comments above.	Rewrite the paragraph.
	63C		75	2674-2675	Substantive	The assertion can NOT include the same key that was used to sign the assertion. Note: This document has repeatedly confused which key is involved in signing vs validating an assertion. I did not have the time to carefully read all 135 pages, so someone else should do a careful review to ensure that all such instances are corrected.	Change: "This MAY be the same key that the subscriber-controlled wallet uses to sign the assertion." to **"This MAY be the public ds key that corresponds to the private key used by the subscriber-controlled wallet to sign the assertion."**
	63C		75	2679	Substantive	Language that again implies that the public key was used for signing…	Change "for the key" to "that corresponds to the key"
	63C		75	2687	Substantive	Do to the new variance in IAL methods that yield wildly different fraud vulnerabilities, IAL alone will be an insufficient indicator of risk.	Add (bold) : 'IAL: Indicator of the IAL of the subscriber account being represented in the attribute bundle, **as well as an indicator corresponding to the set of controls used to obtain that IAL,** or an indication that no IAL is asserted.'
	63C		75	2688	Substantive	Authenticator strength is also important to know, and because the strength of the 2nd factor is allowed to vary wildly from an SMS OTP to FIPS-certified hardware, it's important to relay which class of authenticators was used.	Add: "5. AAL: The AAL used to authenticate to the wallet, or an indication that no AAL claim is being made. If an AAL claim is made, an indicator referring to the type of authenticator(s) used SHALL be provided."
	63C		76	2697	Substantive	Recommend that non-exportable key storage be required rather than recommended. Key export introduces a significant exploitable security flaw.	Change 'SHOULD' to 'SHALL'
	63C		76	2703	Substantive	PII does not include the entire universe of private and potentially sensitive data.	Change to (addition in bold): "contains PII **or other private or potentially sensitive data**"
	63C		76	2704	Substantive	Message level encryption should be required whenever PII or other sensitive data is passed through a third party.	Change SHOULD to SHALL
	63C		76	2727-2728	Substantive	Line 2664 in Section 5.8 states that the assertion from a subscriber-controlled wallet SHALL contain a cryptographic nonce only if it is provided by the RP. Line 2701 in Section 5.9 also indicates that it is optional for the RP to provide a nonce. Line 2727 then implies that the RP is required to provide a nonce.	Either require that the RP provide a nonce (recommended) and update lines 2664 & 2701, or change lines 2727-2728 to indicate that the requirement only applies if the RP had provided a nonce in its request.

	63C		76	2731	Substantive	It is inevitable that some bad actors will be able to obtain signed attribute bundles from CSPs. It is also inevitable that bad actors will succeed in stealing signed attribute bundles from insufficiently protected wallets. (It is only the eventual scale of this fraud that is currently unknown). It is therefore *critical* that RPs are able to determine whether a particular attribute bundle has been reported as having been fraudulently obtained so as to prevent its use.	Change MAY to SHALL.
	63C		78	2754	Substantive	Additional common attacks include: interception of the password and 2nd factor with a keylogger or redirecting users to a realistic but fake IDP where the password & 2nd factor are captured and relayed to the IDP. Also see https://githubcom/pushsecurity/saas-attacks	Add information on additional attacks and mitigations. To mitigate against credential theft by fake IDPs and keyloggers, users can be prominently shown logs of their previous visits, or at least the most recent visit, along with instructions for when they see a login that they don't recognize.
	63C		78	2763-64	Substantive	What does this mean, exactly? "there are potential limitations on the tailoring to proofing strategies and the visibility into the proofing process that an IdP can offer to different RPs."	Provide clarification
	63C	8	86	2938	Admin	Incorrect standard name.	Should be: "Ergonomics of Human-System Interaction."
	63C		87	2971	Admin	Broken link - Account Chooser redirects to a list of the wg's	Fix link. Perhaps: https://openid.net/wordpress-content/uploads/2011/12/ac-integration-spec.html
	63C		87	2993	Admin	Typo - remove 'as' in "commercial as IdPs" & adjective recommendation -'some'	Change to "**some** users may be less comfortable with commercial IdPs"
	63C		87	2996	Substantive	There are much better, and perhaps more common, reasons to use commercial IdPs.	Recommended addition in bold: "based on their historical interactions with government services**, or on their knowledge that commercial IdPs provide better customer experience and greater protection against fraud.**
	63C		87	2996	Admin	word choice	Change 'perceptions' to 'preferences'
	63C		88	3020	Admin	word choice	change 'that prevent' to 'which prevents'
	63C	8.2.1	88	3024 - 3025	Admin	Grammar. Inconsistent subject-verb agreement.	Elsewhere in the document, "data" is treated in the singular. Recommend "…data is treated" instead of "data are treated" for consistency.
	63C	8.2.1	88	3032	Admin	Grammar.	Should be "encourages" instead of "encourage."
	63C		89	3056	Substantive	Non-preference attributes need to be verified before they can be updated by a user. It is common for bad actors to change attributes in a user account to further their purposes, such as replacing the legitimate user's address with one that they control.	"...update **preference** attributes**. Attributes that may be relied upon by RPs, such as postal address and phone number, require validation and verification, and should be subject to fraud prevention analysis, before they are updated in the system."**
	63C		89	3062-3064	Substantive	What is the use case for this? It would appear to provide bad actors with a way to cover their tracks.	Reconsider including this. If it is retained, provide a concrete example and update the wording so it is not an avenue for exploitation.
	63C		89	3065-3067	Substantive	This is going to be exploited by bad actors. See previous comments regarding allowing users to delete their data.	Change to something like: "Provide **non-proofed (no IAL or IAL0)** users means to….**For IAL1 and above, accounts should be deactivated and the information retained for one year from the request in order to support any subsequent fraud investigations."**
	63C	8.2.2	90	3085	Admin	Spelling.	Should be "subsection" instead of "sub-section."
	63C		90	3109	Substantive	Redress methods are exploitable by bad actors seeking to change a legitimate users information.	Addition in bold: "Provide **secure** and effective redress"
	63C	8.2.2	91	3125 - 3126	Admin	Redundant.	Suggest: "Users may have concerns regarding trust, privacy, security, or single-point-of-failure."
	63C		93-94	3209-3212	Substantive	While this entire paragraph is phrased in a way that is unnecessarily conspiratorial, lines 3209-3212 paint IdPs as so potentially malevolent that I started reaching for my tin foil hat while reading it.	Remove those lines and rework this paragraph so that it portrays more realistic threats and realistic solutions.
	63C	10.3	98	3315	Admin	Spelling.	Should be "interagency" instead of "inter-agency."
	63C	10.1	103	3473	Admin	Inconsistent spelling.	Interchangeable use of "a priori" and "apriori" throughout.
	63C	Referenc es	106	3569 - 3571	Admin	Incorrect title.	Should be: "...errata set 2" instead of "…errata set 1."
	63C	Appendi x A	N/A	N/A	Admin	Missing acronyms.	Missing IdAM, API, and CN.

	63C		114	3846	Substantive	This definition contains a list of communities that may not consider themselves 'underserved', excludes other communities that do consider themselves 'underserved', and uses terminology that significant numbers of some of the listed groups themselves find highly offensive.	In all four volumes, shorten the definition to its non-controversial and non-political core meaning "The consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment"