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

Please submit responses to dig-comments@nist.gov by March 24 April 14, 2023

Organization:	*SOCIAL SECURITY ADMINISTRATION*
Name of Submitter/POC:	*Jeffrey Walsh*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
	63-Base	Note to Reviewers	ii	139-144	Advancing equity is a fantastic goal, but practically speaking, how will this mandate be implemented? Will gathering demographics be required during identity proofing? If so, what will be the required set? Rural (where broadband and cell service may be inadequate) vs city, race/national origin/ethnicity (which ones?), income (which income bands should be grouped together?), sex, disability (receiving disability payments?, has a specific disabilities, if so which ones?), English fluency?, technology the users have access to? which technologies? (scanners, mobile phone with a camera, webcams, printers, etc.), what about proficiency with technology? (having the tech is necessary but insufficient). For maximum impact, these metrics will need to be consistent across agencies. Each agency will then have to gather additional data on identity proofing pass/fail rates, at what point in the process failure occurs, usage, etc. Will this be required? How frequently must the analysis be done? How will inequities, if discovered be addressed? Will reporting be required? To who?	Develop and provide supplementary guidance that addresses these issues.
	63-Base	Note to Reviewers	iii	187-190	Yes. Fraud checks should be considered as part of the identity proofing and authentication process for all levels, and factored into the risk analysis. This should include real time checks done during enrollment and/or authentication, as well as post-transactional analytics.	
	63-Base	Note to Reviewers	iii	188	"device fingerprinting" Device fingerprinting can be very useful but can also present challenges for populations that must share devices because of poverty or institutionalization. If device fingerprinting is used, care must be taken to ensure that users who do not have their own device are not excluded.	Provide guidance on how to utilize device fingerprinting without creating barrier for individuals who must used shared devices.
	63-Base	Note to Reviewers	iii	196	"Are current testing programs for liveness detection and presentation attack detection sufficient for evaluating the performance of implementations and technologies?" No, they are not. Ideally, NIST would have a dedicated lab for this research with continuous testing, similar to the work currently done for static facial verification algorithms. Technologies that can defeat liveness detection will continue to evolve alongside the liveness detection technologies, yet facial verification is one of our best tools to reduce fraud during identity proofing.	
	63-Base	Note to Reviewers	iii	202-203	Agencies need explicit and concrete guidance on how to go about developing and utilizing impact category criteria and thresholds tailored to their mission, user capabilities & needs, and risk tolerance. Also recommend providing the option of using a 0-9 scale and likelihood scores in addition to the L M H. The additional granularity has the potential to help improve decision making especially when operational needs, security, and equity must be balanced when deciding on controls. (0 = No Impact; 1-3 - Limited; 4-6 = Moderate; 7-9= High) Also, agencies need to collect, analyze, and SHARE the appropriate data to know what is happening, what works, and what doesn't. Is that something NIST could take the lead on?	
	63-Base	Note to Reviewers	iii	204-205	Privacy: Context is critical and needs to be taken into consideration. Risking the exposure of the home address of an individual using mySSA to manage their retirement benefits is not the same as risking the exposure of an address in a witness protection program application. Equity & Usability: Without the application of the scientific method we cannot really know which controls make a service more or less equitable, usable, OR secure. Studies must be conducted, and the results shared.	
	63-Base	Note to Reviewers	iii	206	Agencies need to put fraud detection controls in place to understand what is happening - then mitigation techniques can be more precisely applied. Guidance will need to be provided for this to be done defectively in most agencies. (Also, fraud data needs to be shared among agencies, and mechanisms for how to do so will need to be established.)	
	63-Base	Note to Reviewers	iii	207-208	"How can we qualify or quantify their ability to mitigate overall identity risk?" For some suggestions, see 'How to Measure Anything in Cybersecurity Risk' by D. Hubbard & R. Seiersen and similar books	
	63-Base	Note to Reviewers	iv	211	Verifiable Credentials is currently a framework and set of principles, not a technical specification that allows for interoperability and consistent security.	
	63-Base	Note to Reviewers	iv	211	mobile driver's licenses –ISO has not completed the logical interface standard for mDLs, but it is promising and may be our best path to providing all US citizens and residents with a secure, trustable, identity credential that can be used for remote identity proofing. Hopefully the US government is a strong participant in driving the standard in a way that it can meet those requirements.	
	63-Base	Note to Reviewers	iv	235	"What equity assessment methods, impact evaluation models, or metrics could we reference" To do this well, the following factors should be considered in impact studies: device used/device capabilities, the user's proficiency with and access to technology, housing status, access to internet, internet speed, family income bracket, credit score, disability status, sex, NIS or Fitzpatrick skin tone, age, native language, English fluency, education.	

	63-Base	Note to Reviewers	iv	239	reference architectures - It would be very useful to have a reference implementation architecture of an IAL1 & IAL2 implementation that can be used for experimentation.	
	63-Base	2	3	355	typo: 'the unique'	the unique --> a unique
	63-Base	2	3	360-62	Verifying the identities of people calling into a customer support service or a call center is out of scope for this document. How/when will this scope be addressed? This is an important consideration for SSA.	
	63-Base	2	3	367-369	"Additionally, given the broad range of individual needs, constraints, capacities, and preferences, digital services must be designed with equity and flexibility in mind to ensure broad and enduring participation." 1. Consider adding the following to the sentence "...while also ensuring a degree of trust commensurate with the risk of the digital service." 2. Should this be "digital identity services" or "digital services, including those that issue and mange digital identities, must be designed...". 3. The term "digital service" should be defined in the glossary, as distinct from the related terms "digital transaction", "system" and "application".	
	63-Base	2	3	370-381	This statement applies broadly to identity, not merely digital identity. However, the risks and best practices described in this section can apply to identity in general. There may be value in adding a statement to the effect of: "While this publication considers only digital identities, organizations should consider their digital identity approach alongside other mechanisms for identity management, such as in call centers and in-person interactions."	
	63-Base	2	3	377	Change 'with programs' to 'with their programs'	
	63-Base	2	3	381	Change 'culturally appropriate' to 'culturally-appropriate'	
	63-Base	2	3	387	physical person' Consider using "natural person" consistently. (assuming that a physical person is the same as a natural person)	
	63-Base	2	3	387	"digital authentication process" Encouraged to see the removal of a referral to "return visits", which has been the source of some ambiguity in -3.	
	63-Base	2	3	390	Consider changing "the service" to "a given service". A digital service may need confidence that the same subject previously accessed a different digital service.	
	63-Base	2	3	395	Should "usable" be included here? Should "trustworthy" be used instead of "secure" (to encompass all elements of trust, rather than only security).	
	63-Base	2	3	399-403	"Additionally, this publication provides instruction for credential service providers (CSPs), verifiers, and relying parties (RPs) and it describes the risk management processes that organizations should follow for implementing digital identity services and that supplement the NIST Risk Management Framework [NISTRMF] and its component special publications." This sentence is difficult to parse; it may be more readable as "...follow for implementing digital services. These risk management processes supplement..."	
	63-Base	2	3	407	Is it intentional that this statement refers only to "digital authentication" and not "digital identity" generally?	
	63-Base	2	3	419	The lack of consistency between the terms "digital service", "online transactions", etc., has been a major source of confusion in applying the guidance. This sentence uses "digital service" and "online transaction" in the same sentence, and it is not clear anywhere in the guidance what the difference is (or even if there is one). It is important to use terms consistently and define the terms in the glossary.	Consider rephrasing as follows: "This guidance applies only to digital transactions that accept a digital identity, including services that require identity proofing and authentication, regardless of the constituency (e.g., citizens, business partners, and government entities). Not all digital services require digital identity, and this guidance does not apply to such services."
	63-Base	2	3	447	"For non-federated systems, agencies..." This wording suggests that IAL and AAL are not required for systems that only accept federated credentials.	
	63-Base	2	3	448	There is an incongruity between IAL and FAL. Where a system does not federate, the guidance advises no FAL be assigned. In contrast, where a system does not require identity, the guidance advises an IAL called "IAL0". The final guidance might resolve the incongruity by using "FAL0" to describe an application that does not involve federation; or simply not assigning an IAL at all to transactions that do not require evidence in a real-world identity.	
	63-Base	2	3	448	Are there circumstances where an AAL is not required because the subscriber identity-proofs directly to the digital service without using an identity credential?	
	63-Base	2.3	6	490	"Effective enterprise risk management is multidisciplinary by default and involves the consideration of a diverse set of factors and equities."	To improve clarity, consider rewording the sentence to something like: "Enterprise risk management is most effective when it is designed to be multidisciplinary and to consider a diverse set of factors and equities. "
	63-Base	2	3	492	Consider adding "trustworthiness" (to include robustness to fraud, which is related to but separate from information security).	

	63-Base	2.3	7	501-503	"They may also consider partitioning the functionality of a digital service to allow less sensitive functions to be available at a lower level of assurance." Consider adding reasons for why this a good idea to the end of the sentence, such as "in order to improve equity and access without compromising security or to balance access with security concerns."	
	63-Base	2.3.2	8	542-44	DOJ's website only currently provides the 2020 Edition.	We are unable to locate the 2010 Edition in order to identify whether the items referenced here are in the 2020 Edition. We recommend updating based on the current, available Edition.
	63-Base	2.3.4	9	587	Does NIST intend for usability to be considered distinct from customer experience (CX), specifically the guidance in EO 14058 for federal agencies?	
	63-Base	2.3.4	9	597	Without a qualifier it's too easy to design a study around a 'typical' or 'average' user who has good internet connectivity and an up to date smart phone while excluding users who may be more challenging to support.	add 'demographically', so it reads 'with demographically representative users'.
	63-Base	4.1	11	614	The guidance needs to account for IAL0/AALx credentials	recommend changing to: "Applicant - the subject applying for a credential; for IAL1 and above, the subject to be identity proofed"
	63-Base	4.1	11	614-17	As defined, the terms Applicant, Subscriber, and Claimant are difficult to comprehend.	We recommend including additional examples or an infographic to clarify and simplify these terms in the DI context.
	63-Base	4.1	11	636	Recommendation: Change 'The usual' to "One possible" or similar.	
	63-Base	4.1	14	689-690	This sentence seems unclear; it can be construed to mean the attribute types or attribute values. Is the requirement that RPs must identify to the CSP or IdP the attributes it requires from the CSP/IdP following successful identity proofing or authentication?	
	63-Base	4.2	14	701	"IAL0" This is the only reference to IAL0 in this document. Is this intentional?	
	63-Base	4.2	15	713	"CSPs generally limit the lifetime of a subscriber account and any associated authenticators in order to ensure some level of accuracy and currency of attributes associated with a subscriber." Does NIST offer guidance for the valid lifetime of a subscriber account and the valid lifetime of specific authenticators?	
	63-Base	4.2	14	717	Suggest changing to "authenticators may be unbound, invalidated, or destroyed according to..."	
	63-Base	4.2	14	718	Typo: Change "CSPs" to "CSP's"	
	63-Base	4.2	14	719	Change "have a duty to maintain control" to "have a duty to maintain exclusive control"	
	63-Base	4.2	14	721-722	Change "In order to request issuance of a new authenticator, typically the subscriber authenticates to the CSP using their existing, unexpired authenticators." to "In order to request issuance of a new authenticator or binding of an additional existing authenticator, typically the subscriber authenticates to the CSP using their existing, unexpired authenticators.	
	63-Base	4.2	14	724	What standards does NIST specify for this abbreviated identity proofing process? 63A does have any references to an abbreviated identity proofing process.	
	63-Base	4.3.1	17	730	Given the importance of phishing-resistant authenticators, as described in OMB M-22-09, we suggest introducing this topic in the base volume, within this section, with further details to follow in Part B.	
	63-Base	4.3.1	17	733	While passwords are traditionally 'something you know', the increased use of password managers as a best practice moving passwords into 'something you have' territory. Perhaps change to "memorized password or PIN"?	
	63-Base	5	23	923	Due to the complexity of this process and the lack of clarity on implementing the requirements, consider relabeling this as informative.	
	63-Base	5	23	930	function' seems to refer to 'digital identity function'. Perhaps 'digital identity function' would be more clear than 'function in the identity system'?	
	63-Base	5	23	932	The first step for agencies needs to be fully defining and tailoring impact categories to provide concrete thresholds and examples for 'Limited/Low', 'Moderate', and 'High' for each category. This is non-trivial and should be an organized effort that includes business owners, cybersecurity, privacy & fraud experts, and enterprise risk management executives. Once clearly defined impact thresholds are established then an agency can conduct assessments that are meaningful, repeatable, and fully reflect that risk appetite of the agency. Ideally, this should precede conducting impact assessments. Otherwise, assessments will vary widely depending on the way an individual analyst interprets the term 'limited' or 'serious' on a particular day. Furthermore, this should be an iterative process - when confronted with an application-specific impact not initially considered the decision made should be documented in the impact criteria used as an assessment reference. Team composition is also important - and agencies need guidance on the skill sets and knowledge required to conduct thorough assessments.	
	63-Base	5	23	933	Change 'and associated impact levels' to 'and associated impact levels for each transaction.' Also, guidance needs to be included to define transactions and explain how to decompose services into transactions, as well as why it's important to do so. Providing analysis at the transaction level not only provides greater confidence in the overall risk score, but it identifies and calls out higher risk transactions that an organization may want to monitor or add controls to in order to reduce the associated risk.	
	63-Base	5	23	937	Change 'for each applicable xAL.' to 'for each applicable xAL and transaction.'	

	63-Base	5	23	939	for equity, usability - Will detailed guidance be provided on how to conduct 'detailed equity and usability assessments' and how to measure 'equity'? These are wonderful goals, but it will be difficult to achieve meaningful results without such guidance. Will agencies decide individually which equity parameters they will measure for their performance metrics, then decide on individual targets for improvement? There are many potential equity parameters - as partially enumerated in section 2.3.3 . Also, it will be challenging to balance privacy principals such as data minimization with efforts to improve equity and usability. It is not possible to measure all the equity impacts of a system without capturing information about users that some may see as overly intrusive, so we may need an 'opt out' or 'opt in' requirement so individuals being identity proofed can provide demographics voluntarily. Also, additional funding will likely be required. These are complex and expensive endeavors that may require applications to be updated so they can provide the necessary data for these assessments to occur.	provide guidance
	63-Base	5	23	939	threat assessments' Will guidance be provided on how to conduct threat assessments? With the shortage of cyber and DI expertise in the government, explicit guidance will be needed for this to be implemented well at many agencies.	provide guidance
	63-Base	5	23	945	This step is definitely needed, however agencies will need concrete guidance on how to do this. If that guidance is provided in a subsequent section in this document, it should be referenced here.	provide guidance
	63-Base	5	23	945	information is collected' Agencies will need guidance on what information to collect and how to evaluate/analyze it. This is non-trivial. Many applications are not designed in a way to make the right information easy to collect, and it may need to be supplemented with demographic or other information for analysis.	provide guidance
	63-Base	5	23	946	"performance of the identity system " Metrics for performance must be carefully designed, and agencies will also need concrete guidance on how to do this as well. For example, a common metric for identity proofing success is 'pass rate', so teams become incentivized to maximize 'pass rate'. Unfortunately, 'pass rate' is a completely meaningless metric where a perfect score can be achieved by removing all security. Better metrics are 1. What is the (approximate) pass rate for legitimate users and 2. What is the (approximate) fail rate for bad actors. This is more difficult to measure, but the results will be meaningful and actionable.	
	63-Base	5	23	949	Monitoring for unintended harms is something to aspire to, but is complex. It is challenging to distinguish bad actors from legitimate users in an operational environment.	Explicit guidance will need to be provided.
	63-Base	5	23	958	How will the typical analyst conducting risk assessments know about the changes to the threat environment that are relevant to them? We're not aware of any government resources that can give analysts the information they need to do this well. CISA's current resources are not a good match for this need.	
	63-Base	5	24	962	SHALL's should only be placed before clearly defined requirements. This type of ambiguous SHALL could lead to compliance challenges for agencies.	revise
	63-Base	5.1	24	971	An additional step is required - bad actors need to be explicitly and carefully considered. Who may be motivated to gain access to a particular transaction? What may they gain by obtaining information they shouldn't have access to or by providing false information? What are their incentives/motivations? Different categories of bad actor should be considered separately - for example, primarily politically vs economically motivated & bad actors who know the individual whose identity they are attempting to fraudulently utilize vs bad actors who do not know their victims. (This is not a comprehensive list.)	Include the additional step.
	63-Base	5.1	24	979	High, Moderate, or Low Given the inherent subjectivity in making impact assessments, as well as the equity and operational considerations that must be taken into consideration when implementation decisions are made, it is useful to understand whether an impact is assessed as a 'very low Low' or a 'Low, but borderline Moderate', and whether a Moderate is closer to Low/Limited or High.	Add the option to use a more granular scoring system, especially for agencies with a wide variety of user types and applications. SSA is using a 0-9 scheme where 0 is N/A, 1-3 is Limited, 4-6 is Moderate, and 7-9 is high.
	63-Base	5.1.2	25	998	Recommend changing 'potential impact' to 'expected potential impact' or similar. Otherwise, some risk assessors may take a 'butterfly flapping their wings sets off a hurricane' approach to risk assessment, conjuring highly unlikely worst-case scenarios.	
	63-Base	5.1.2	25	999-1000	The new wording for these categories improves clarity.	
	63-Base	5.1.2	25	1001	Why was 'unauthorized release of' replaced by 'loss of'? 'Loss' implies that the information may have been destroyed.	Perhaps rename this category 'Loss or unauthorized release of information', which would clearly cover both cases of inappropriately shared information and information that is deleted or destroyed by a bad actor, which is a risk with an authenticator error to a service where the legitimate user has previously provided information. Further suggest expanding the title to "Unauthorized release, verification, or loss of information". When information such as someone's SSN is verified by a bad actor it becomes more likely to be used for identity theft. Verified information is more valuable on the black market than unverified information, so government verification services pose a risk as well.

	63-Base	5.1.2	25	1002	Did NIST intentionally remove agency liability from consideration entirely? Also, organizations and wealthier individuals can sustain sometimes very large economic losses without losing 'economic stability'. Was the intent to only consider losses that have truly dire impacts? Isn't that the purpose of the 'Low', 'Moderate', and 'High' thresholds?	If that was not the intent revert back to the prior language which is clear and comprehensive "Financial Loss/Agency Liability".
	63-Base	5.1.2	25	1003	Recommend using the term 'physical safety and health'. Without the 'physical' qualifier this may be interpreted in too broad a fashion to include mental health. 'Reputation' sufficiently encompasses impacts that would commonly be expected to infringe upon mental health.	
	63-Base	5.1.2	25	1003	Consideration for the environment is a welcome inclusion in this DRAFT, however environmental damage that can lead to safety and health issues is not necessarily the same as environmental 'stability'.	Recommend removing 'environmental stability' from the title of this category and instead provide an example in the explanation that reminds readers that environmental damage may lead to health or safety impacts. If the intent is to address other impacts on the environment that may not directly impact human health or safety, a separate category could be created for those agencies where that category is relevant.
	63-Base	5.1.2	25	1004	This change in wording from 63-3 is appreciated - it is more comprehensive and adds clarity.	
	63-Base	5.1.2	25	1006 - 1007	Agencies will need more guidance on this.	Provide guidance
	63-Base	5.1.2	25	1014	It would be helpful to provide examples of harms to businesses or external organizations for those agencies that provide services to other organizations, such as SSA, IRS, FDA, USDA, etc.	include business in addition to citizen examples
	63-Base	5.1.2	25	1027	The unauthorized verification of PII can also lead to harms. The value of stolen PII increases when it has been verified by an authoritative source, and increases the likelihood that the PII will be used for identity theft.	Change 'loss of PII' to 'unauthorized release or verification of PII'
	63-Base	5.1.2	26	1,033	"Damage to or loss of economic stability:" See above comments. Recommend that NIST revert to the previous definition.	
	63-Base	5.1.2	26	1034-1036	"Harms to individuals may include debts incurred or assets lost as a result of fraud or other harm, damage to or loss of credit, actual or potential employment, or sources of income, and/or other financial loss." When these impacts not direct but instead are the results of impacts in other categories it may make sense to account for them in the primary impact category. This category should then be scoped so that it deals with direct financial loss only, such as when a check is rerouted from a beneficiary to a bad actor.	consider rescoping
	63-Base	5.1.2	26	1037-1038	If these harms arise from loss of sensitive information, damage to trust/reputation, or other impact categories, they can be addressed there.	consider scoping this to only direct financial loses.
	63-Base	5.1.2	26	1039	environmental stability Per earlier comments, recommend removing this from the health/safety category title and consider creating an Environmental Stability/Damage category to be used by agencies whose services or programs could have direct environmental impacts.	
	63-Base	5.1.2	26	1040	Suggest removing 'mental and emotional well-being' from this category and instead keep it focused on clear physical harm. Impacts to mental and emotional well-being are secondary rather than primary impacts and can therefore be fully accounted for in the appropriate primary impact category. For example, financial loss or unauthorized release of sensitive information can both result in distress. That distress is best accounted for within the precipitating category. It's important to not dilute this category which can paradoxically result in it being given less weight than it deserves.	remove mental, or emotional well-being from the physical safety category
	63-Base	5.1.2	26	1041-1042	"or loss of accessible, affordable housing." This impact should be covered within the financial harms category. Counting the same impact in multiple categories could reduce the readability and usability (and therefore the import) of a risk assessment.	
	63-Base	5.1.2	26	1041	This impact should be covered within the financial harms category. Counting the same impact in multiple categories could reduce the readability (and therefore the import) of a risk assessment.	move category
	63-Base	5.1.2	26	1043-1045	Is this a realistic primary consequence of a DI error in a service provided to the public? What is an example of this? And wouldn't the organization's inability to operate fall more appropriately in the damage to mission delivery category?	Reconsider this example
	63-Base	5.1.2	26	1046	What type of risk impacts are envisioned by the “Noncompliance with laws, regulations, and/or contractual obligations” category?	Please provide more guidance, including examples of laws and regulations that are typically involved in DI impacts
	63-Base	5.1.2	26	1047-1049	These are all secondary impacts that are covered by the other impact categories. The only primary impact for this category is to the agency/organization providing a service. SSA is rating the impact to the public for this category as N/A. The other categories such as damage to mission delivery already cover these impacts to the public.	Recommendation: Do not repeat impacts across categories without careful consideration. Instead, try to make them as focused and atomic as possible. In this case, the recommendation is to focus on the impact to the agency/organization if they violate laws/regulations/contractual obligations.
	63-Base	5.1.3	26	1055	Agencies need to be aware that they MUST concretely and unambiguously define what 'limited vs serious vs severe' looks like for their agency for each category, which is a non-trivial effort. Otherwise, assessments will be based on what 'feels' limited or serious to the individual tasked with doing the analysis that day (an individual who may very likely not have a strong risk assessment or DI or cyber background).	consider adding language making this a requirement
	63-Base	5.1.3	27	1066	While IAL, AAL, & FAL need to be considered separately, formally evaluating them separately typically leads to a repetitive copy-paste effort in DIRAs. In the vast majority of cases the impact will be the same regardless of the source of the error whenever there is identity proofing. --- In many cases, organizations can reapply an evaluation to multiple xALs. For instance, the harms from an impostor invoking a transaction on another's behalf can be expected to be the same irrespective of whether the impostor completed identity verification using a false identity or appropriated a valid credential - in that case, the organization can reapply the impact analysis for determining IAL to AAL.	Change 'evaluated' to 'considered', or consider adding the language: "; however, organizations MAY apply a single impact assessment to more than one xAL."

	63-Base	5.1.3	27	1071	"slight", "insignificant", and similar terms are nebulous. Under FIPS199, LOW means limited, not inconsequential., and 63A/B/C technical guidance requires a reasonably-high technical standards even at the xAL1 level.)	Recommend removing the word 'slight' to align this explanation better with the FIPS 199 definition of 'Low'.
	63-Base	5.1.3	27	1071	"disparities" The inclusion of disparity here creates a curiosity when we apply the high-water mark. In practice, increasing the xAL also increases the effect of disparity since it shifts the equity-trust trade-off in the direction of higher trust. Also, how can an identity proofing, authentication, or federation error in itself result in disparities? Certainly, IdP/auth/federation mechanisms can result in disparities, but the impact analysis examines the transaction, not the technical mechanism. -------- Disparities in access are independent of the impact categories and instead correlate with the implemented controls (which are chosen based on the impact category ratings.) So, the higher the rating in an impact category due to inappropriate access being granted, the higher the controls will be, and the greater the disparities. Impacts from disparities in appropriate access that arise from the implementation of controls simply can't be considered at the same time as impacts that arise from granting inappropriate access.	As part of the DIRA process, separately document the expected disparities in pass/success rates for legitimate users that may arise from the different IAL, AAL, & FAL implementations. (And remove it from this section.) For example, at IAL1 x% of legitimate individuals below the poverty line are expected to pass remote identity proofing, and at IAL2 only x-20%, etc. (Although this will be challenging to measure and implement. See previous comments).
	63-Base	5.1.3	27	1085 - 1088	Outcome disparities due to DI errors can be eliminated by removing all controls. The impacts arising from inappropriately granting access cannot be assessed in the same category as the impacts that arise from inappropriately denying someone access (due to the controls intended to prevent the first type of impact).	Recommendation: As part of the DIRA process, separately document the expected disparities in pass/success rates for legitimate users that may arise from the different IAL, AAL, & FAL implementations. (And remove it from this section.) For example, at IAL1 x% of legitimate individuals below the poverty line are expected to pass remote identity proofing, and at IAL2 only x-20%, etc. (Although this will be challenging to measure and implement. See previous comments).
	63-Base	5.1.3	27	1093	Inconvenience' is both a secondary effect and categorically different from damage to trust or reputation.	Recommendation: Remove 'inconvenience' from this category. It will arise naturally from other impacts such as damage to mission delivery and financial loss, so should usually be accounted for in those primary categories. Or, move it to a separate category in case it is a primary impact for certain applications. (SSA has taken this approach and evaluates inconvenience in its own category, considering it at the end of each assessment.)
	63-Base	5.1.3	28	1100	The title is missing: 'Unauthorized Release of Sensitive Information'	Add title
	63-Base	5.1.3	28	1110	Recommend that this category only be used for direct financial loss (for example, payments are redirected to the wrong account). Indirect losses that occur as a result of impacts in other categories can be accounted for in those primary categories.	rescope category
	63-Base	5.1.3	28	1111	"Low: at worst, an insignificant or inconsequential financial loss to any party." is not aligned with FIPS 199	Recommend changing to: "Low: at worst, a limited financial loss to any party."
	63-Base	5.1.3	28	1116	Mental health impacts are secondary to other impact categories so can be handled in the primary category, such as damage to reputation, loss/exposure of sensitive information, and financial loss. Also, mental health is far too subjective and variable to assess on its own. An event that traumatizes one individual may not even be noticed or remembered by another individual, and that is especially true across cultures. Agencies would need both social anthropologists and psychologists on staff to assess this separately.	consider removing mental health from this category
	63-Base	5.1.3	28	1116 - 1117	environmental impact - Remove from this category and create a separate category, or clarify to indicate that this is environmental impact that is expected to have impacts on the health of individuals (such as increased lead levels in water).	adjust structure according to comment (remove or clarify)
	63-Base	5.1.3	28	1127	edit wording	an insignificant or inconsequential --> limited
	63-Base	5.1.4	29	1133	This section is where the tension between strength of controls and demographic disparities that may arise from the implementation of those controls could be discussed. For example, IAL2 may cause an in increase in legitimate users being denied access to a service, which may lead to economic harm, whereas IAL1 may lower the access disparities but increase the risk of fraud (which may also lead to economic harm).	
	63-Base	5.1.4	29	1139	"Risk" combines impact and likelihood. It is a longstanding issue in the NIST guidance to use the terms "risk" and "impact" interchangeably. Risk considers the impact together with the likelihood (considering the threat environment); whereas impact does not. The guidance here requires agencies to "assess the risk" but only use the assessed impact to determine xALs.	Since we aren't discussing likelihood, recommend changing 'risk' to 'impact'
	63-Base	5.1.4	29	1139	"identify measures to minimize their impact." The intent of risk management is to effectively manage, not minimize, risks. If organizations' objectives were simply to minimize the adverse impact from a digital service, they could do so by simply not deploying the service.	Change to: ""identify measures to manage their impact."
	63-Base	5.1.4	29	1140	"SHALL assess" Strongly recommend changing this from 'assess' to 'consider'. The word 'consider' leads to readable risk assessments where the risks are easy to discern, and any differences in identity and authentication errors can be made clear. The word 'assess' results in unreadable copy-paste exercises where the same impact is typically repeated three times for each of the seven categories which drowns out the actual impacts in a lot of noise.	Change "SHALL assess" to "SHALL consider".
	63-Base	5.1.4	29	1140	"SHALL assess the risk" Per the above comments, either change 'risk' to 'impact' or add guidance on assessing likelihood and determining risk based on both likelihood and impact. (If likelihood is used, consider discussing confidence in the likelihood, which can be challenging to determine, furthermore most agencies may not be gathering the data and doing the analysis required to determine likelihood accurately.)	See comment

	63-Base	5.1.4	29	1141	"separately" See earlier comment re. reapplication of assessments.	
	63-Base	5.1.4	29	1150-1151	How can this possibly be known in the impact assessment stage, where we have not identified any technical mechanisms? We can't assess barriers that arise due to identity proofing controls until after we've decided on what those controls will be (based on the impact of granting inappropriate access).	remove from this section and consider elsewhere
	63-Base	5.1.4	29	1161	"digital identity system." Is the unit of assessment the digital service or the function of the digital service?	
	63-Base	5.2.2.1	31	1197	A reference to IAL0 should be included. Some agencies will have IAL0 for some of their credentials, and its absence here may lead to over-use of identity proofing when it's not required or, at the very least, inconsistent terminology (which has impacts in a federated environment).	reference IAL0
	63-Base	5.2.2.1	31	1198	This description understates the IAL1 assurance requirement. Like IAL2, IAL1 is supported by strong evidence validated against authoritative sources. The principal differentiator between IAL1 and IAL2 as written rests in verification requirements. IAL1, as written, provides reasonably strong assurance.	
	63-Base	5.2.2.1	31	1198-99	Section 5.6 in NIST SP 800-63A-4 refers to Table 1, which indicates that IAL1 requires 1 piece of superior or 1 piece of strong plus 1 piece of fair evidence. Why is this not referenced in this statement in NIST SP 800-63-4. As written here, it appears that IAL1 has no evidence requirements.	
	63-Base	5.2.2.2	31	1212	grammar: "the claimant controls authenticator registered"	Change to: "the claimant controls authenticators registered"
	63-Base	5.2.3	32	1238	"initial selections are primarily based on cybersecurity risk" This statement is not supported by the evaluation criteria earlier in this section. Initial selections are not based on risks at all, but rather potential impacts. Those potential impacts are primarily non-cybersecurity oriented, affording great weight to fraud, privacy, and personal harms that can result from an identity error.	Change 'primarily based on cybersecurity risk' to 'primarily based on the impacts arising from digital identity errors'. (specifically, false positive identity errors)
	63-Base	5.2.3	32	1241	A 'failure' to identity proof someone or to authenticate someone could mean that it is working as designed - such as when an impersonator/ bad actor is prevented from gaining access to a system.	Change 'failures' to 'errors'.
		5.2.3.1	33	1259	Change "are not applicable to the system." to "are not applicable to the system and the organization SHALL NOT assign an IAL (or SHALL assign an IAL of IAL0)."	see comment
	63-Base	5.2.3.1	33	1267	Strongly recommend replacing 'worst-case' with 'highest assessed impact'.	see comment
	63-Base	5.2.3.1	33	1267-1268	Organizations should not need to concoct worst-case scenarios and attach an IAL to that worst-case scenario. Standard practice is to assess reasonably-foreseeable harms and determine controls conforming to those harms. Consider an identity failure where a person would need to visit an in-person office. A person can suffer a fatal injury in an automobile crash while on transit to the physical site. Clearly, assessors should need to consider that a DI error could result in loss of life should that worst-case chain of events occur.	
	63-Base	5.2.3.1	33-34	1287-1289	More detailed guidance is required for how, exactly, agencies should consider the balance between equity and required security controls, as underserved communities may be more impacted by the requirements for higher level identity proofing and authentication.	
	63-Base	5.2.3.2	34	1308	Strongly recommend replacing 'worst-case' with 'highest assessed impact'.	see comment
	63-Base	5.2.3.2	34	1315 - 1318	Rather than taking this approach, it's recommended to assess the impact to mission delivery caused by false positive DI errors along with the other categories. Do not wait and evaluate it and then try to combine the impacts of errors caused by false positives with the impacts of the controls. Instead, evaluate the potential impacts of false negatives separately.	consider recommendation
	63-Base	5.2.3.2	34	1321	It is likely that low-impact (e.g., IAL1) systems will be AAL2 under the requirement that any service involving personal information use MFA. It may be beneficial to break out the requirement: Low impact (no personal information): AAL1 Low impact (involving personal information): AAL2 Moderate impact: AAL2 High impact: AAL3	see comment
	63-Base	5.2.3.3	35	1351	Change 'worst-case' to 'highest impact'	see comment
	63-Base	5.3	36	1375	This section is a very helpful addition to the guidance!	N/A

	63-Base	5.3.1	37	1398	As proposed in the guidance, the selected technology is both an outcome of and input to the xAL selection. How can it be both simultaneously? Until an xAL is selected, the technology is unknown (in fact, the RP may not have even selected a CSP at that point) – how can agencies assess the "barriers, including biases" of a technology that has not been selected yet? Section 5.3.1 requires agencies to "conduct detailed assessments of the controls defined at the assurance level to determine potential impacts". How is this possible when (1) the organization may not have made a CSP selection yet and therefore will not know the specific controls, and (2) CSPs have flexibility in their control implementation and can adjust their controls to ensure continued performance. Does adding a new CSP require a new DIRA because the new CSP may have different controls? CSPs are already required to consider equity in their service offerings (see 800-63A section 5.1.3), and document measures it takes "to mitigate the possibility of inequitable access, treatment, and outcomes". If equity of service is a requirement of CSP implementations, what is the added value of conducting a separate study at the DIRA phase? What weight should RPs place on the CSP assessments, and to what extent should RPs conduct their own? What level of effort does NIST anticipate here? There is not a great deal of basic research in this general realm, and it is not realistic for RPs to be expected to conduct basic research to complete each DIRA.	
	63-Base	5.3.1	37	1398	Is the intent by NIST to leverage existing assessments being performed (e.g., PTAs, PIAs, etc.) or is the intent to fold privacy, equity, usability, and threat assessments into agency Digital Identity Risk assessments for purposes of determining final xAL services for digital services? How, exactly, might equity, privacy, and usability impacts be integrated into the assurance level selection process and digital identity risk management model?	provide clarity/additional guidance
	63-Base	5.3.1	37	1404	"SHALL assess impacts" Should this be risks rather than impacts here?	
	63-Base	5.3.1	37	1406	"Privacy – to determine unintended consequences to the privacy..." Is this the same as a Privacy Impact Assessment? If it is different, how is it different?	
	63-Base	5.3.1	37	1411	Will there be guidance on which demographics and groups should, at a minimum be considered? Will it be left up to each agency? Will agencies also independently establish their on metrics and evaluation techniques?	add clarity to answer questions
	63-Base	5.3.1	37	1414 - 1416	This should not be left up to each individual agency. They don't have the expertise or resources, and doing this right is a significant effort.	Consider how to provide support, or remove expectation
	63-Base	5.3.2	37	1424	"to the greatest degree possible" - this language can offset the requirement later in the section to "demonstrate comparability of a chosen alternative or document residual risk incurred" by requiring organizations to minimize residual risk at the cost of other equities. The suggested change allows agencies to consider practicability factors, including service equity, in selecting compensating controls.	Change to "to the greatest degree practicable"
	63-Base	5.3.2	38	1438	Change "due to availability of evidence" to "due to the lack of availability of required evidence"	see comment
	63-Base	5.3.2	38	1440	Guidance is needed on how one can "demonstrate comparability." Describing the compensating controls is straightforward, but without data, how can comparability be assured?	
	63-Base	5.3.4	39	1474-75	This is an important artifact for agency Authorizing Officials to consider when reviewing authorization packages. Especially when there is a deviation between assessed vs. implemented assurance levels. As such, this should be required, not optional.	"Federal agencies SHALL include this information in the system authorization package described in [SP800-37]."
	63-Base	5.4	39	1481-83	Given the increased threat landscape in the DI space, and increased overlap amongst privacy, security, and fraud governance teams, such feedback loops should be considered a requirement versus optional to ensure DI solutions are stood up in a manner that support the interests of all groups involved in compliance, usability, and risk mitigation. Additionally, if intent here is to reference PIAs as defined in E-Gov and OMB M-03-22, "Privacy Impact Analysis" should be changed to "Privacy Impact Assessment".	"These programs SHALL consider feedback from application performance metrics, threat intelligence, fraud analytics, assessments of equity impacts, privacy impact analysis, and user inputs."
	63-Base	5.5	39	1486-89	Of equal importance when considering digital identity solutions is privacy, especially considering several of the controls in the new Identification and Authentication control family in NIST SP 800-53 r5 require full collaboration between information security and privacy programs per the FPC Collaboration Index for Security and Privacy Controls.	"Close coordination of identity functions with cybersecurity teams, threat intelligence teams, privacy teams, and program integrity teams can enable a more complete protection of business capabilities, while constantly improving identity solution capabilities."
	63-Base	5.5	39	1493	Recommend changing this to a SHALL. It's critical that this occur and should be relatively easy to implement.	increase requirement to SHALL
	63-Base	5.5	39	1496	Can NIST make a statement supporting cross-agency information sharing to combat fraud?	
	63-Base	A.1	43	1589	It's our understanding that only NIST SP 800-63-4 will contain definitions for terms used throughout the DI Guidelines (base volume + A-C)). As such, we recommend any terms that are used throughout be defined here. The following terms are used throughout the series but are not included in the current list of defined terms:	
	63-Base	A.1	43	1589	SAOP should be included as a definition.	Senior agency official who has agency-wide responsibility and accountability for ensuring compliance with applicable privacy requirements and managing privacy risks.
	63-Base	A.1	43	1589	PIA should be included as a definition	An analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis.

	63-Base	A.1	43	1589	Risk Assessment Definition	Given the consolidated control catalog for privacy and security in NIST SP 800-53 r5, this definition should also include a reference to "privacy". See revised statement below: "It is part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security and/or privacy controls planned or in place."
	63-Base	A.1	43	1589	Systems of Record Notice should be defined	A system of records notice (or "SORN") is published by a Federal agency in the Federal Register upon the establishment and/or modification of a system of records describing the existence and character of the system. A SORN identifies the system of records, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system.
	63-Base	A.1	43	1589	Phishing Resistant Authentication should be included as a definition	Authentication processes designed to detect and prevent disclosure of authentication secrets and outputs to a website or application masquerading as a legitimate system.
	63-Base	Requirements Notations and Conventions	43	1589	This section appears to have been removed from rev. 4. It was included in rev. 3 and contained helpful information regarding the terms "SHALL" "SHALL NOT", "SHOULD, "SHOULD NOT", "MAY", "NEED NOT", 'CAN", and "CAN NOT".	Please include this section from rev. 3 in rev. 4 to ensure readers understand these terms as they apply to various sections within the guidelines.

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

Please submit responses to dig-comments@nist.gov by March 24 April 14, 2023

Organization:	*SOCIAL SECURITY ADMINISTRATION*
Name of	*Jeffrey Walsh*
Email Address of	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
	63A	Questions	iii	199	"Are current testing programs for liveness detection and presentation attack detection sufficient for evaluating the performance of implementations and technologies?" They are not sufficient. Given the rapid evolution of deep fake technologies, the federal government really needs a lab dedicated to this - not only to detect and prevent the evolving threats to remote identity proofing and biometric-based authentication, but to be able to detect politically-motivated fakes that could destabilize our democracy.	N/A
	63A	Questions	iii	210	"What equity assessment methods, impact evaluation models, or metrics could we reference to better support organizations in preventing or detecting disparate impacts that could arise as a result of identity verification technologies or processes?" (Comment in Suggested Change column)	Guidelines are required that standardize which metrics should be captured during the identity proofing process along with guidance on how to do so, along with definitions for commonly used terms so relying parties and CSPs can meaningfully and accurately communicate results. For example, 'pass rates' for an IAL2 process may be used by a CSP to refer to the percent of individuals who succeed in eventually getting through the IAL2 processes, regardless of attempts (where only legitimate users start the process). One agency/RP may use 'pass rates' to mean the percentage of individuals who successfully get through the identity proofing process on a single attempt, without taking into account whether the user is legitimate or a bad actor. Another agency/RP may use the term 'pass rates' to mean the percentage of legitimate users who get through the process within 24 hours of starting. Terms such as 'pass rate' need to mean the same thing to everyone involved, and need to defined in a way that makes sense. It is also important to capture, to the extent possible, the reason for an identity proofing failure. Did someone fail because their ID was expired, and they need to get it renewed before they re-initiate the process? Did it fail because credit checks were used and the person has no credit history? Did it fail because they couldn't pass the selfie check, although they are a legitimate user? Did it fail because someone moved recently, or was using a mobile device that did not belong to them? Did they fail because they provided a synthetic SSN? Did someone simply stop the process and start again later, perhaps because they were interrupted? These differences matter and need to be captured and analyzed to improve identity proofing systems and understand equity impacts.
	63A	Questions	iv	217	"What applied research and measurement efforts would provide the greatest impact on the identity market and advancement of these guidelines?" (Comment in 'Suggested Change' column.)	We need to understand the true impact of identity proofing controls. Does a particular control reduce fraud by x% but reduce pass rates for legitimate users by y%? We have no idea what x or y is today; we are forced to guess because the studies haven't been done. What impact do controls have on particular user groups? Should we use some controls for some populations and other controls for other populations (such as financial checks)? Do certain combinations of controls work better than others? Without the proper data we do not have the information required to chose the best controls. Also, the individuals choosing which identity proofing controls to use need to understand how each control can be defeated and the level of effort involved. This is guidance that would need to be updated frequently since attack methods can evolve rapidly. For each control, is it something an average bad actor can bypass in an hour or less? (Such as creating synthetic FAIR evidence.) A day? A week? Does it require technical expertise or a nation-state level-actor?
	63A	2	3	375	federal agencies is capitalized inconsistently in the document	use consistent capitalization throughout the series
	63A	2	3	402	"Fraud Prevention" Suggest change to 'fraud mitigation'. Fraud controls can be preventative, detective, or responsive (see GAO report 15-593SP). A CSP's objective is not only to prevent fraud, but also to detect and effectively respond to (e.g., criminally prosecute) identity fraud that does occur. Suggested rewording: "Fraud mitigation: detect, respond to, and prevent access to benefits, services, data, or assets using a fraudulent identity."	
	63A	2.1	4	402	Five Expected Outcomes of Identity Proofing are listed	Consider adding a sixth outcome: 'Fraud Remediation: for high impact applications, capture and retain enough data to support the prosecution of individuals responsible for impersonation attempts.'

	63A	2.2	4	408	IAL0 is a useful level and should be treat it as such by changing the wording to reflect the rest of the list.	Remove the parenthesis from IAL0 and treat it like the other IALx's listed. IAL0: No Identity proofing. There is no.... IAL1: The identity proofing process...
	63A	2.2	4	409	consider using "real-world" and "real-life" consistently.	
	63A	2.2	4	410	"self-asserted" attributes are, by definition, neither validated nor verified.	Remove 'Self-asserted'
	63A	2.2	4	412	"supports the real-world existence" At IAL1, the identity proofing process provides some assurance not only in the real-world existence of the claimed identity, but also (through evidence validation and verification) that the subscriber is the individual they claim to be. Suggest change to: "The identity proofing process provides baseline assurance that the applicant is the real-world identity they claim to be."	
	63A	2.2	4	414	"credible sources" This is a very useful addition to the guidance It can be impossible to validate against authoritative sources. However, distinctions between the two types of sources should be made along with guidance as to when to use each.	Keep "credible sources" but explain how they are different from authoritative sources. Indicate that credible sources should be used only when it is impractical or impossible to use an authoritative source. Also, to prevent the market responding to this change by standing up sources labeled as credible that are not reliable, there should be requirements for credible sources, such as organizations subject to regulatory oversight.
				416-417	"IAL2 adds additional rigor to the identity proofing process by requiring the collection of stronger types of evidence" The evidence collected in IAL1 and 2 are the same. ---------- The statement that IAL2 requires "stronger types of evidence" relative to IAL1 is directly inconsistent with the technical guidance. Both IAL1 and IAL2 require the same evidence (1 piece of SUPERIOR or 1 piece of STRONG + 1 piece of FAIR).	The evidence collected in IAL1 and 2 are the same, so remove this phrase.
	63A	2.2	4	416	IAL2 - We are not aware of any proven equivalent alternative for the non-repudiation capabilities of biometrics (with liveness checks, timestamps, meta-data analysis, etc.). There is no way to effectively strongly bind a claimed identity to the identity of a human organism without the use of biometrics, particularly for individuals who have a limited credit history, do not own a home, and may not own the devices that they are using for remote identity proofing.	For alternatives to biometric controls, guidance should be provided on which controls have been proven to be as nearly as effective as biometrics, and how effective those controls are compared to biometrics, expressed as a percentage, such as controls x, y, and z in combination are 94% as effective as biometric verification.
	63A	2.2	4	417	"a more rigorous process for validating" This statement is also inconsistent with the guidelines. The validation requirements at IAL2 are no different from the validation requirements at IAL1	Since validation is the same, remove this statement
	63A	4	6	427	Typo: "This section provides and overview"	Change to: "This section provides an overview"
	63A	4	6	438	Word choice: "SHOULD enable optionality"	For clarity, change to: "SHOULD provide options" or similar
	63A	4	6	440	"At a minimum, this SHOULD include accepting..." These items, particularly "supporting multiple data validation sources", can implicate additional fraud vectors. Consider adding the sentence, "Since such optionality can result in greater exposure to fraud by providing attackers with a broader set of attack vectors, CSPs SHOULD evaluate fraud exposure for each option and implement mitigating fraud controls where warranted. At a minimum, CSPs SHOULD ensure that each option provides, in aggregate, comparable assurance to other available options."	
	63A	4.1	6	451	Grammar: "To ensure, to a stated level of certainty, the applicant is who they claim to be"	Change to: "To ensure, to a stated level of certainty, that the applicant is who they claim to be"
	63A	4.1	6	461	"minimum necessary....Home address" Many agencies, including SSA, need to provide services for individuals who do not have a fixed home address or who move frequently.	Consider acknowledging the challenges homelessness can create for the identity proofing process and providing recommendations for when there is no home address (or credit history).
	63A	4.1.1	8	466	In figure 1, collection of evidence is in the resolution step; however, in section 4.3, collection of evidence is described as the first step of validation.	Make the figure consistent with the text

	63A	4.1.1	8	472	"The CSP also collects" See comment for line 466 re. whether collection of evidence is a function of resolution or validation.	Consider relabeling "Resolution" as "Resolution and collection" here and in figure 1.
	63A	4.1.1	8	481	Typo?: "The CSP compares the pictures on the license and the passport to the photo of the live applicant's photo"	For an IAL2 example, this should be changed to: "The CSP compares the pictures on the license or the passport to the photo of the live applicant's photo"
	63A	4.1.1	9	485	Typo: "verifying they the applicant"	Change to: "verifying that the applicant"
	63A	4.2	9	494	Word choice: "a complete and successful identity proofing transaction." This paragraph is describing an identity proofing process, not a single transaction.	Change to: "a complete and successful identity proofing process."
	63A	4.3	9	495	Suggest changing the title to "Identity Evidence Collection and Validation" to reflect order of events	see comment
	63A	4.3	9	495	It would be helpful if NIST were to publish and maintain a list of acceptable forms of identity evidence and their respective strengths, along with authoritative and credible sources and suggested core attributes for each piece of evidence. As additional evidence becomes available, such as mobile driver's licenses, the list can be updated.	N/A
	63A	4.3	9	497	grammar: "determine it is authentic"	Change to: "determine whether it is authentic"
	63A	4.3	9	497-498	" current, and unexpired." What is the difference between "current" and "unexpired"? Does ensuring that a document is current also ensure that it is unexpired?	
	63A	4.3	9	500	"key data contained on the identity evidence" It would be very helpful if NIST were to provide a wiki that contains example evidence, the strength of that evidence, and the 'key data' for each piece of evidence.	
	63A	4.3.2	10	526	An additional characteristic of acceptable digital evidence is needed: the digital evidence must be cryptographically protected from alteration and must be strongly bound to the issuer so fake evidence cannot be easily created.	Add a seventh criteria: "The digital evidence must be cryptographically protected from alteration and must be digital signed by the issuer."
	63A	4.3.2	10	539	Typo: "accessible to intended person""	Change to: "accessible to the intended person"
	63A	4.3.2	10	541	"the presented digital evidence can be verified through authentication at an AAL or FAL commensurate with the assessed IAL." Which AAL is 'commensurate' with which IAL? Accepting digital evidence at AAL1 for an IAL1 identity may not be sufficient. Perhaps AAL2 should be the minimum. In practice, AAL2/FAL2 may also be the only available options for authenticating to digital evidence for IAL3 identity proofing, so perhaps that should be the maximum required as well.	Change to: "the presented digital evidence can be verified through authentication at AAL2 or FAL2, or higher."
	63A	4.3.3.1	11	551	Fair Evidence: "The issuing source of the evidence confirmed the claimed identity through an identity proofing process." Identity proofing? Or identity resolution? In previous guidance a utility account statement is listed as FAIR evidence, but no identity proofing process is typically required when setting up utilities - only identity resolution and perhaps attribute validation.	Either change to: "The issuing source of the evidence used an identity resolution process prior to issuing the evidence." Or provide requirements for the steps fair evidence issuers must follow to meet NIST's identity proofing requirements, along with concrete examples of fair evidence where identity proofing is done in a way that meets those requirements.
	63A	4.3.3.1	11	555-556	This section suggests that a reference number is not required if the document includes a facial portrait or sufficient attributes to resolve an identity. However, 4.3.1(2) and 4.3.2(2) would not permit a facial portrait in place of a reference number.	
	63A	4.3.3.1	11	557	There are several references in this draft to ensuring documents are unexpired, e.g., section 2.1 provides that validation includes "confirming that all supplied evidence is...unexpired". However, this section indicates that that recently-expired evidence is acceptable as evidence under some circumstances.	
	63A	4.3.3.2	11	570	"There is a high likelihood that the evidence issuing process would result in the delivery of the evidence to the person to whom it relates." High likelihood implies that enough information is known about the issuing process for every issuer that the statistical probability of issuance to the correct individual can be known. Since this isn't possible in practice, change 'high likelihood' to 'reasonable belief'.	Change to: "There is a reasonable belief that the evidence issuing process would result in the delivery of the evidence to the person to whom it relates."
	63A	4.3.3.2	11	570	What is meant by "There is a high likelihood that the evidence issuing process would result in the delivery of the evidence to the person to whom it relates"?	Provide additional clarification
	63A	4.3.3.2	11	576; 595	"The evidence includes physical security features that make it difficult to copy or reproduce" presumes a physical form of evidence which precludes digital evidence such as an mDL and does not address the alteration of evidence.	Change to: "The evidence includes physical or cryptographic security features that make it difficult to copy, reproduce, alter, or otherwise misuse." The same comment applies to line 595.
	63A	4.3.3.3	11	594	"The evidence includes digital information that is cryptographically signed." Not all physical evidence will contain digital information.	If the comment is retained (see above), change to: "If the evidence includes digital information, it must be cryptographically signed."

	63A	4.3.3.3	12	599	This sentence is ambiguous. Does it mean "The CSP SHALL validate (all identity evidence to meet evidence collection requirements) and (all core attribute information required by the CSP identity service", or "The CSP SHALL validate all identity evidence to meet (evidence collection requirements) and (all core attribute information) required by the CSP identity service." Perhaps consider breaking into multiple sentences to clarify meaning.	
	63A	4.3.4	11	600	"and all core attribute information required by the CSP" Relying parties need to understand what the 'core' attributes are that have been validated.	Recommend providing the minimum core attribute set for all commonly used identity evidence, including the DL and Passport. Also, since there is going to be some discretion involved, recommend requiring the CSP to publish all attributes that they validate, and whether they use a credible or authoritative source for the validation.
	63A	4.3.4.1	11	606	Typo: "and that it as not been"	Change to: "and that it has not been""
	63A	4.3.4.1	11	608-609	1. This does not account for the allowance for FAIR evidence to be acceptable up to 6 months post-expiration 2. An ambiguity arose during COVID-19 where several jurisdictions extended the expiration of documents through administrative or executive order. In these cases, the expiration date printed on the evidence was superseded by administrative order, and the document continued to be valid past its printed expiration date. To clarify the ambiguity in favor of giving weight to jurisdictional orders, there may be value in adding "Where the issuing source administratively modifies the expiration date of previously-issued evidence, such as in emergency situations where renewal is not available for an extended period of time, CSPs SHOULD apply the issuing source's policy rather than the printed expiration date in determining whether the evidence is expired."	
	63A	4.3.4.3	13	625	"or credible source" Who defines a 'credible' source? Some guidance will be required otherwise vendors may simply label themselves as credible when they may not be.	
	63A	4.3.4.4	13	630-632	This provision can be problematic. FAIR evidence must be collected at IAL1/IAL2 but has no security features, allowing the attributes printed on the evidence to be trivially fabricated. This provision would allow such attributes to be considered validated without additional verification. This provision should be limited to apply when the evidence is self-validating (e.g., an address printed on a driver's license that is validated at the STRONG level for authenticity does not require further validation; however, an address printed on a utility bill on plain paper must be validated against another source.) That said, Sections 5.3.3 and 5.4.3 suggest that FAIR evidence must be validated.	Reconsider all uses of FAIR evidence
	63A	4.3.4.4	13	645-646	This allowance seems to severely stretches the commonly-understood meaning of "authoritative source", which is a source that is authoritative. A source that merely has access to evidence traceable to an issuing source would not itself be considered authoritative under the common meaning, although it may nonetheless be credible.	
	63A	4.3.4.4	14	647 - 654	This paragraph provides what appears to be non-normative guidance on what constitutes a credible source. This should be changed to normative guidance and include additional requirements that strengthen the confidence in the ability of the source to accurately validate the evidence.	Modify to state: "A CSP SHALL only consider a source to be credible if it:"
	63A	4.3.4.4	14	654	Wording: "checked for data correlation for accuracy"	Change to: "checked using data correlation for accuracy"
	63A	4.4.1	14	663	The enrollment code verification guidance as specified in Sec. 5.1.6. is not sufficient. It needs to be expanded for use with identity verification.	When enrollment codes are used for identity verification, the address needs to be strongly associated with an individual in an authoritative or credible source. For identity verification, postal address should be preferred and email address should be disallowed.
	63A	4.4.1	14	669-670	"comparison of the facial portrait presented on identity evidence to the facial image of the applicant" Would this provision allow the CSP to use an image from the issuing source in place of the image presented on the identity evidence? A limitation of current remote issuance processes is that the image printed on the document cannot always be captured in high resolution. If the image can be obtained from the issuing jurisdiction rather than the presented evidence, certain classes of attack could be curtailed; however, it is not clear if the guidance would allow for this approach.	Allow the use of a facial portrait that is obtained from the authoritative source, such as being able to use AAMVA as the source for the driver's license portrait. This could both increase pass rates for legitimate users and reduce fraud.
	63A	4.4.1.	15	684	"Control of a digital account" What types of digital accounts would be acceptable? More information is needed.	
	63A	4.4.1	15	686	"An individual is able to demonstrate control of a ... signed digital assertion (e.g., verifiable credentials)" A 'verifiable credential' may lack necessary security features. All security considerations in the specification are non-normative: https://www.w3.org/TR/vc-data-model/#cryptography-suites-and-libraries	Recommend removing verifiable credentials as an example or qualifying it, such as by stating: (e.g., verifiable credentials with security and issuance features equivalent to a derived PIV credential)
	63A	5.1	16	697	Change "performing identity proofing at any IAL." to "performing identity proofing at any IAL (not including IAL0)."	see comment

	63A	5.1.1	16	701	Consider adding: - The CSP's policy and process for validating and verifying identity evidence, including training and qualification requirements for personnel who have validation and verification responsibilities, as well as specific technologies the CSP employs for evidence validation and verification. - If the CSP allows verification requirements to be satisfied by demonstrating association with a digital account, the CSP's policies and procedures for accepting association with a digital account for verification.	see comment
	63A	5.1.1		708-712	It would be useful if NIST or some other central organization could provide data analysis correlating past attributes used for validation to incidents of fraud so that CSPs could assess which attributes are the most or least reliable.	
	63A	5.1.1	16	713	The phrase "dealing with" is quite informal. Consider replacing with "resolving".	see comment
	63A	5.1.1	16	713	Change "dealing with identity proofing errors" to "resolving potential or alleged identity proofing errors"	see comment
	63A	5.1.1	16	714	communicating Communication is one element of a broader remediation process, which can also include revoking the credential and investigating the fraudulent act.	Consider requiring the policy and process to extend to all remediation activities, and not only communication to affected parties.
	63A	5.1.1.1	17	731	"the CSP SHALL be responsible for fully disposing of or destroying all sensitive data." Many methods of disposing of or destroying data are insufficient.	Require conformity with NIST SP 800-88
	63A	5.1.1.2	17	737	Change "In the event the CSP uses fraud mitigation measures" to "If the CSP uses fraud mitigation measures"	see comment
	63A	5.1.2	17	744	"The following privacy requirements apply to all CSPs providing identity services at any IAL." IAL0 is an IAL, so recommend changing it to 'at any IAL where identity proofing is conducted', or similar.	Change to: "The following privacy requirements apply to all CSPs providing identity services at any IAL where identity proofing is conducted."
	63A	5.1.2.1	18	762	"the CSP SHALL consult the NIST Privacy Framework" SHALL follow makes sense, but what does SHALL consult mean from a compliance perspective?	Change to: "the CSP SHALL follow the NIST Privacy Framework"
	63A	5.1.2.1	18	773-775	This statement would not appear to allow processing for purposes of fraud detection and mitigation.	Please consider adding "mitigate fraud risks" to the list of permissible functions.
	63A	5.1.2.1	18	773-775	"Processing of PII SHALL be limited to the minimum necessary to validate the existence of the claimed identity, associate the claimed identity with the applicant, and provide RPs with attributes they may use to make authorization decisions." Won't CSPs need the option to collect additional PII in order to assess equity?	Change to: "Processing of PII SHALL be limited to the minimum necessary to validate the existence of the claimed identity, associate the claimed identity with the applicant, provide RPs with attributes they may use to make authorization decisions, and, with appropriate opt in/out functionality provided to the individual, assess equitable outcomes." Per comment 61 in 63base rev.4, opt in/out requirements will likely be needed when collecting information for assessing equity.
	63A	5.1.2.2	18	776-780	"The CSP MAY collect the Social Security Number (SSN) as an attribute ...CSPs SHALL implement privacy protective techniques (e.g., transmitting and accepting derived attribute values rather than full attribute values themselves)" Derived values works well for things like deriving age from DOB, but how does this apply to SSN? The SSN is never used to derive attributes. It is only useful when the complete SSN is transmitted.	Recommend removing this sentence from the SSN paragraph and mentioning attribute derivation techniques in a place that's more appropriate in the guidance.
	63A	5.1.2.2	18	778	Making this requirement a SHALL rather than a SHOULD is impractical, as there are legitimate reasons for the CSP to collect the full attribute value (e.g., verifying against data exchanges that require the full value.).	

	63A	5.1.2.2	19	790-791	"These mechanisms SHALL be easy for applicants to find and use." How would one measure how 'easy' something is to verify compliance?	Recommend either changing this to a SHOULD or pointing to something with solid requirements. (Perhaps EO 13166?)
	63A	5.1.3	19	795-797	"SHALL....identify processes or technologies that can possibly result in inequitable access..." Will each agency and CSP independently determine which equity factors to consider for access? Or will there be guidance?	
	63A	5.1.6	21	864	"Enrollment codes are used to confirm an applicant has access to a validated address." Does validated address mean that the address exists? Or that the person is strongly associated with the address in a credible record? In some cases the former is what will be needed (when providing contact information) and in some cases the later (identity verification & notice of an identity proofing event).	
	63A	5.1.6	21	869	"Enrollment codes SHALL be sent to a validated address (e.g., postal address, telephone number, or email address)." Is validated being used in the sense that the addressed is checked to make sure it exists?	
	63A	5.1.6	21	869-870	"The applicant SHALL present a valid enrollment code to complete the identity proofing process." Shouldn't there be a requirement that the enrollment code only be sent to an address that is strongly associated with the applicant in a credible or authoritative source? And if that is the case, is email appropriate given its lack of security?	Change to: ""The applicant SHALL present a valid enrollment code to complete the identity proofing process. The enrollment code SHALL be sent to an address of record for the individual that has been provided by an authoritative or credible source. The address MAY be a postal address or a mobile phone number. Email SHALL NOT be used to complete an identity proofing process for IAL2 and above."
	63A	5.1.6	21	874-875	"A random six digit number generated by an approved random number generator with at least 20 bits of entropy;" Does this have to be a number? Or can it be an alphanumeric code? If it's alphanumeric 4 digits is sufficient to obtain 20 bits of entropy. Also, a random 6 digit number has slightly less than 20 bits of entropy: 6 log2(10) = 19.93 So, if the goal is at least 20 bits of entropy, 7 digits is required, or a 4 char alphanumeric code. If the goal is to use 6 digits, and alphanumeric is to be prohibited, perhaps the entropy statement can be dropped.	Consider changing to: "Enrollment codes SHALL be generated by an approved random number generator and comprise of the following: - A random sequence of at least 6 digits or alternative secret that contains at least 20 bits of entropy,"
	63A	5.1.6	21	874-875	The requirement to use an approved RNG only applies to (a), but (b) and (c) also require a random secret. Should this requirement also apply to (b) and (c)?	
	63A	5.1.6	21	875	"an approved random number generator with at least 20 bits of entropy" Does this apply to the secret or to the RNG itself?	Restructure the sentence so it's clear that the entropy applies to the generated code
	63A	5.1.6	21	880	For SMS and email, enrollment codes used as authenticators to bridge sessions will need longer valid times than enrollment codes used to confirm control of an address.	
	63A	5.1.6	21	885-886	"valid for at most...10 minutes, when sent to a validated telephone number (SMS or voice); or...24 hours, when sent to a validated email address." These times are far too short if the code is used for bridging an enrollment session. For that use case they must be significantly longer. However, they may also be unnecessarily short when used to confirm that someone has access to an address provided. What is the security justification for these particular restrictions? Why was 10 minutes chosen for phone? In rural areas or places with poor connectivity, delivery of SMS can take longer than 10 minutes which creates equity issues.	Recommend that these guidelines be lengthened considerably, using evidence-based justifications for the times given, or change the SHALL to a SHOULD.
	63A	5.1.6	21	887	"The enrollment code SHALL NOT be used as an authentication factor." Isn't the enrollment code being used as an authenticator when it's used to bridge two enrollment sessions (864-867)?	Remove this requirement or separate the different uses of the enrollment codes into discrete sections since the requirements are different for each use case.
	63A	5.1.7	22	894-896	"Notifications of proofing: ...SHALL be sent to a validated address (e.g., postal address, telephone number, or email address) of record" Is validated intended to mean that there is strong reason to believe that the address or phone number are strongly associated with that individual? Or that they are postal addresses and phone numbers that actually exist? I would suggest rewording to require that it is sent to a validated address that is linked to the applicant in an authoritative or credible source. Note: 'of record' can be used to indicated that a CSP or RP has recorded the information provided by an applicant, it does not necessarily mean that the address was linked in a credible source.	

	63A	5.1.7	22	896	""Notifications of proofing: ...SHALL be sent to a validated address (e.g., postal address, telephone number, or email address) of record" There is no authoritative source mapping individuals to email addresses in the united states, and most are protected by a passwords only which may not even meet AAL1 standards.	Remove email address as an option.
	63A	5.1.7	22	898	"SHALL include details about the identity proofing event, such as the name of the identity service" Providing the name of the identity proofing service should not be optional	Change to: ""SHALL include details about the identity proofing event, including the name of the identity service"
	63A	5.1.7	22	901	"in the case the recipient repudiates the identity proofing event." Repudiation is an indicator that the individual's PII has been stolen and is being used to try to gain access to services. Shouldn't the CSP be required to record cases of repudiation, and share that information with RPs as a fraud indicator?	
	63A	5.1.7	22	902-904	"SHOULD provide additional information, such as how the organization or CSP protects the security and privacy of the information it collects and any responsibilities the recipient has as a subscriber of the identity service." This makes it optional for the applicant/recipient to be informed of any responsibilities that they may have. Is that the intent?	Change to: "SHALL provide additional information, such as...."
	63A	5.1.8	22	917	What is the difference between "biometric mechanisms" and "biometric characteristics"?	Please provide definitions for both
	63A	5.1.7	23	928-929	"CSPs SHALL allow individuals to request deletion of their biometric information at any time, except where otherwise restricted by regulation, law, or statute." Bad actors could use this requirement to remove evidence of fraud.	Change this requirement to make it clear that while a request can be made, the CSP should not be obligated to comply with it when the biometric is used for fraud detection or prosecution. Also, this requirement should be limited to IAL 1 & 2 only.
	63A	5.1.7	23	928-929	1. Does the requirement allowing individuals to request deletion extend to requiring CSPs to honor that request? (e.g., if a fraudulent actor requests deletion of a biometric that could likely used against them in a criminal preceding, must the CSP comply?) 2. In no case should this requirement apply to IAL3, which requires collection of a biometric for nonrepudiation. Allowing a subscriber to delete their biometric information after enrolling at IAL3 would weaken the assurance to RPs that the IAL3 credential is robust to future nonrepudiation claims.	
	63A	5.1.7	23	930-931	CSPs SHALL have all biometric algorithms tested by an independent entity (e.g., accredited laboratory or research institution) for performance Recommend requiring that the entity must be an independent accredited laboratory or research institution. Otherwise 'independent entities' without such qualifications will invariably crop up to conducting testing in a way that will allow any algorithms to pass.	Change to: "CSPs SHALL have all biometric algorithms tested by an accredited laboratory or research institution for performance"
	63A	5.1.8	23	932	Which demographic groups? This needs to be standardized. Without standardization no comparison is possible and compliance could be obtained by using demographic measurements that defy the intent of this requirement	Consider referencing the FRVT List and/or DHS demographic data/definitions.
	63A	5.1.8	23	935-937	While NIST specified FMR for biometric algorithms, it does not set performance requirements for Presentation Attack Detection. There are existing performance standards defined by independent third parties such as FIDO Alliance or ISO 30107.	NIST should include Imposter Attack Presentation Attack Rate of PAD level 1 and Level 2 as specified by ISO or FIDO Alliance in addition to FMR.
	63A	5.1.8	23	938-940	CSPs SHALL employ biometric technologies that provide similar performance characteristics for applicants of different demographic groups (racial background, gender, ethnicity, etc.).	Change to: "CSPs SHALL employ biometric technologies that provide similar performance characteristics for applicants of different demographic groups. Specifically, performance should be similar regardless of sex or skin tone (measured using the Fitzpatrick skin types).", or similar.
	63A	5.1.8	23	943	"CSPs SHALL make all performance and operational test results publicly available." Recommend that the performance and operational test results include demographics and device information. There may be a stronger correlation between device age and camera quality and pass rates then between sex or skin tone and pass rates.	Change to: "CSPs SHALL make all performance and operational test results publicly available. Those results SHALL include all captured demographic indicators as well as information about the device used for the biometric capture."
	63A	5.1.8	23	946	"user base of the system" Will this include the range of devices found in the user base, since those may have a greater impact on the results than other demographic factors?	Change to: "CSPs SHALL assess the performance and demographic impacts of employed biometric technologies in conditions substantially similar to the operational environment and user base of the system. The user base is defined by both the demographic characteristics of the expected users as well as the devices they are expected to use."
	63A	5.1.8	23	948	Line 948 is a duplication of line 943.	Remove

	63A	5.1.8	23	951-952	"CSP SHALL collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject" 'Ensures' is not realistic. Recommend changing to 'provides strong confidence' or similar.	Change to: "CSP SHALL collect biometrics in such a way that provides reasonable assurance that the biometric is collected from the applicant, and not another subject"
	63A	5.1.8	23	954	"liveness detection capabilities to confirm the genuine presence of a live human" NIST will need to test liveness detection capabilities and provide guidance on adequacy. There will likely be a huge range of capabilities in vendor products, and CSPs will have no way of knowing which products actually work against common attacks. As deep fake capabilities develop, this need for testing and the publication of results will continue to grow.	
	63A	5.1.9	24	986-987	"the applicant reference is identity proofed to the same or higher IAL as the applicant." This is a role that, while needed, is vulnerable to abuse. To reduce the risk of fraud the applicant reference should therefore be identity proofed an IAL2 or above, with biometric verification required.	Change to: "the applicant reference must be identity proofed at IAL2 or above."
	63A	5.1.9.1	24	993	"Requirements for Trusted Referees" Trusted Referees are needed to achieve equity, however there is always a chance that the ability to bypass evidentiary requirements will lead to fraud and abuse, including through bribery. To mitigate this it is important to maintaining an association between the Trusted Referee and the applicant in the CSPs records.	Add a further requirement that the CSP maintain a link between the Trusted Referee and the applicant in their records.
	63A	5.1.9.2	25	1004	"CSPs SHOULD allow the use of applicant references." A SHALL would improve equity for citizen services.	Change to: "CSPs SHALL allow the use of applicant references"
	63A	5.1.9.2	25	1008	"The CSP SHALL identity proof an applicant reference to the same or higher IAL intended for the applicant" Recommend that all applicant references be identity proofed at IAL2 or higher, with biometric verification, and that the CSP associate the applicant with the applicant reference in their records, and maintain that association. Otherwise the use of applicant references could become an avenue for fraud.	Change to: "The CSP SHALL identity proof an applicant reference to IAL2 or higher"
	63A	5.2	26	1030	While SRIP is allowed at IAL3, the method is also allowable for other IALs. Also, if this section describes a generic supervised remote process, "supervised remote identity proofing" need not be capitalized.	Change to: "A supervised remote identity proofing process."
				1037-1038	"detect the presentation of fraudulent identities" Suggest replacement with "fraudulent presentation of identities". It is the presentation that is fraudulent, not necessarily the identity itself.	see comment
	63A	5.3	26	1039	Typo: "and application departures"	Change to: "and applicant departures "
	63A	5.3	26	1043	"risks outweigh security considerations" Instead of 'outweigh', consider "or where the security benefit from higher assurance levels is outweighed by privacy and equity considerations." This language frames the trade-off between security and equity/privacy less adversarially.	
	63A	5.3	26	1044	"requirements apply to all CSPs providing identity proofing and enrollment services" Remove the term "CSPs providing". It isn't needed and all services may not be provided by the CSP.	Change to: "requirements apply to all identity proofing and enrollment services"
	63A	5.3.1	26	1049	"behavioral analytics" Does NIST distinguish between behavioral analytics and behavioral biometrics? This distinction is important given the specific requirements that apply to biometrics in this guidance.	
	63A	5.3.2.1	26	1056	"One piece of STRONG evidence and one piece of FAIR evidence" Fair evidence, as stipulated in this guidance, offers zero value in identity proofing. Fair evidence, such as utility bill. does not include any security features and customizable templates are readily available online. Validation of fair evidence requires only visual inspection, which cannot differentiate between genuine and non-genuine documents. At the same time, fair evidence requires a person to obtain copies of such documents, representing a likely source application departures. ---------- Is there any study showing that requiring a piece of FAIR evidence in addition to STRONG evidence actually reduces fraud? It would seem likely that adding a FAIR evidence requirement when STRONG evidence has already been provided has no impact on false positives and may very well increase false negatives. After all, it's much harder to steal or forge a driver's license than a school ID or Utility account statement, and FAIR evidence typically can't be verified.	"For IAL1, remove the requirement for FAIR evidence completely. Doing so will not weaken the total assurance as stipulated in the guidance, while avoiding unnecessary fallout. For IAL2, simple visual examination of FAIR evidence, absent corroboration from an issuing or credible source, should not be acceptable unless the evidence includes security features that prevent presentation of a counterfeit document. (see comment for 5.4.3)"
	63A	5.3.3	27	1061	Core attributes needs to be defined, preferably for each type of common evidence encountered, such as for driver's licenses and passports.	
	63A	5.3.3	27	1064	Consider changing to: "Inspection by qualified personnel of visible, tactile, or other physical security features using appropriate technologies."	see comment

	63A	5.3.3	27	1068 - 1069	"The CSP SHALL validate the genuineness of each piece of FAIR evidence by visual inspection by trained personnel" There is no way to "validate the genuineness" of FAIR evidence. This requirement cannot be met and will increase both the expense and inconvenience of identity proofing with no commensurate increase in security.	Recommend removing this requirement.
	63A	5.3.3	27	1071	"Validating the accuracy of attributes (such as account or reference number" How does one validate the accuracy of account or reference numbers for FAIR evidence, when there is no credible source for the majority of those numbers? How are the account numbers on utility bills going to be validated? There are about 1600 electrical utilities in the United States (https://www.statista.com/topics/2597/electric-utilities/#topicOverview). What about school ID's? There are about 27K high schools and 4k colleges/universities in the US. How will those ID's be validated? Recommend all FAIR evidence requirements be dropped unless it's proven to be worthwhile. FAIR evidence cannot be validated. Forgeries are simple to create. Yet, they create very real inconvenience and likely barriers for legitimate users.	Remove the FAIR evidence validation requirements since it isn't possible to meet them.
	63A	5.3.3	27	1073	Consider adding: "or that are included on STRONG or SUPERIOR evidence" Rationale: Consider an applicant who recently moved and received a new DL on which the new address is printed. At IAL1, the language would allow the attributes on the new DL to be considered validated without the need for separate confirmation. Since the individual moved, authoritative and credible sources are likely to not yet have the applicant's new address.	see comment
	63A	5.3.3	27	1074-1074	"Validating the accuracy of self-asserted attributes by comparison with authoritative or credible sources." There are no authoritative or credible sources most pieces of fair evidence. This requirement cannot be met for FAIR evidence.	Remove this requirement since meeting it isn't possible.
	63A	5.3.3	27	1084	The current sentence precludes the use of AAL2 and FAL2	Add 'and higher' or 'at least' to both the AAL and FAL requirements
	63A	5.3.3	27	1084	Theoretically, this allows an IAL1 system (which can contain PII) to be accessed with a single authentication factor, which is not permissible under EO13681. More practically, this allowance allows an attacker who gains access to an individual's banking credential (e.g., through a phishing attack) to amplify the impact of the breach by also gaining access to government services. Suggestion: "Demonstrated association with a digital account through a multifactor AAL1 authentication or a multifactor AAL1 and FAL1 federation protocol or equivalent, as documented in its practice statement."	
	63A	5.3.3	27	1084	No requirement for IAL is required. As written, a Gmail account would be acceptable.	Add the requirement that the digital account be at both 'IAL1/AAL1' or higher'.
	63A	5.3.4	27	1086	When used for identity verification, the enrollment code needs to be sent to a physical address controlled by the applicant.	Add a requirement that the enrollment code is sent to either a postal address or phone number strongly associated with the applicant, through an authoritative or credible source.
	63A	5.3.4	27	1086	typo "code Sec. 5.1.6"	Change to "code, see Sec 5.1.6"
	63A	5.3.4	27	1089	"to a validated address for the applicant, as specified in Sec. 5.1.7." Section 5.1.7 does not require that the address needs to be linked to the applicant in an authoritative source. To improve security, that requirement needs to be added.	
	63A	5.4	28	1092-1093	Suggest: "in order to provide increased mitigation against impersonation attacks and other identity proofing errors relative to IAL1 while remaining accessible."	
	63A	5.4.2.1	28	1106	"One piece of STRONG evidence and one piece of FAIR evidence" See earlier comment on FAIR evidence. The document does not specify how FAIR evidence is to be validated at IAL2. ---------- FAIR evidence is easy to forge and cannot be validated, so is unlikely to improve confidence in an identity. At the same time, it is likely to cause user inconvenience and increase the cost of identity proofing. Recommend removing FAIR evidence as a requirement when STRONG evidence is presented.	Change to requiring the collection of One piece of SUPERIOR or STRONG evidence
	63A	5.4.3	28	1114	see comment for IAL1	
	63A	5.4.3	28	1118	Unlike IAL1, the document does not indicate how FAIR evidence is to be validated. Consider: "The CSP SHALL validate the genuineness of FAIR evidence by one of the following: - if the evidence includes security features, inspection by trained personnel, or - confirming attributes as valid by comparison with the issuing source or authoritative source(s), or - If present, confirming the integrity of digital security features"	

	63A	5.4.3	28	1119	Account or reference numbers for FAIR evidence cannot be reliably validated. There are about 1600 electrical utilities in the United States (https://www.statista.com/topics/2597/electric-utilities/#topicOverview). What about school ID's? There are about 27K high schools and 4k colleges/universities in the US. How will those ID's be validated? There is no credible source for either.	Remove FAIR evidence validation requirements from Unsupervised Proofing. For this line, remove the validation of account and reference numbers.
	63A	5.4.4.1	29	1128	The return of the enrollment code is important requirement of IAL2 in the current guidance, which provides defense against an imposter who has access to genuine identity evidence.	Consider adding: "The CSP SHALL additionally require verification of the applicant's return of a valid enrollment code."
	63A	5.4.4.1	29	1133	This requirement could be met with a Gmail account that has MFA enabled.	Change to "Demonstrate association with an IAL2 or higher digital account..."
	63A	5.4.5	29	1141	To reduce fraud, notification of proofing should be sent to a postal address that is strongly associated with the purported applicant in an authoritative source.	Add that requirement.
	63A	5.5.3.1	30	1166-1168	In the interest of service equity, suggest considering a provision that does not require verifying the integrity of cryptographic security features if not present (e.g., REAL-ID-compliant identity documents)	
	63A	5.5.4	31	1186	See comment on requiring enrollment code.	
	63A	5.5.4	31	1190	IAL3 should provide a very high confidence in the identity of the applicant so should require biometric comparison. Demonstrated association with a digital account is not equivalent to biometric verification, especially in this case where a Gmail account with MFA turned would meet the requirements.	Remove option 2.
	63A	5.5.5	31	1194	Section 5.1.7 does not require that the address is strongly associated with the applicant in a credible or higher source, which is needed for this step to be meaningful.	Add the requirement
	63A	5.5.8	32	1232	Are there any minimum security requirements for this channel?	Add clear requirements
	63A	5.6	33	Table 1	Evidence - Remove the additional requirement of FAIR evidence requirements where STRONG evidence is provided	see comment
	63A	5.6	33	Table 1	Verification - IAL1: change to at IAL1 or higher and AAL1 or FAL1 or higher IAL2: See previous comments regarding biometrics Also, change 'at AAL2 or FAL2' to 'at IAL2 or higher, and AAL2 or FAL2, or higher' IAL3: Require Biometric comparison	see comment
	63A	6.1	34	1244-1255	"At a minimum the CSP SHALL include the following information in each subscriber account..." Add a requirement that if a trusted referee or applicant reference was used that the identifier of the individual who acted in that role is linked to the subscriber account.	see comment
	63A	6.2	35	1270-1271	Prior to effectuating any update, the CSP SHALL require validation of updates to core attributes consistent with the requirements for the highest IAL associated with the subscriber account.	see comment
	63A	6.3.2	35	1294	Add "and its practice statement" to the end of the sentence.	see comment
	63A	7	36	1307	typo: Change "CSPs" to "CSP's"	see comment
	63A	7	37	Table 2	Typo: "another individuals identity" -> "another individual's identity"	see comment
	63A	7	37	Table 2	Table 2 - typo "in order claim"	Change to "in order to claim"
	63A	7	37	Table 2	"An individual claims benefits from a state in which they do not reside." What is claimed is the identity attribute (state of residence) rather the benefit itself (which is a programmatic decision separate from identity). As worded, the example may run afoul of the requirement that "Identity proofing is not conducted to determine suitability or entitlement to benefits."	Consider changing to: "An individual falsely claims residence in a state in order to obtain a benefit that is available only to state residents."
	63A	7.1	38	Table3	Table 3 - typos "technology.CSP", "indications or malicious traffic", "Death Master File).CSP"	Change: ""technology. CSP" and "indications of malicious traffic", "Death Master File). CSP"
	63A	8.4	42	1420	There may be value in making this a normative requirement, e.g., including a requirement in Section 5.1.4 such as: "The CSP SHALL ensure that information provided to unsuccessful applicants does not disclose or allow the applicant to infer the consistency of any self-asserted information with authoritative or credible sources."	
	63A	8.4	42	1421	A SHALL would provide greater protection against fraud. If this isn't implemented bad actors could use identity proofing as a validation service.	Change "but should not inform the applicant" to "but SHALL NOT inform the applicant"
	63A	9.3	47	1655	Change "users that" to "users who"	see comment
	63A	10.1	51	1731	Change "determine" to "determining"	see comment

	63A	10.1	51	1734	Add a third mitigation: 3. Providing flexibility in the Practice Statement to accept name variations where reasonable for service equity (for example, to allow for differences in name order, multiple surnames, and recent name changes).	see comment
	63A	10.1	52	1742	Note: EO 13988 may also apply here as it relates to verification of gender as an attribute.	
	63A	10.2	52	1759	Add a third mitigation: 3. Ensuring that the selected IAL is not higher than necessary to be commensurate with the risk of the digital service offering.	see comment
	63A	10.3	53	1802	An additional mitigation would be to fail over to a second algorithm, ideally one that performs better than the primary algorithm for certain populations.	Add that suggestion.
	63A	10.3	54	1812	Another mitigation is to have the biometric verification done algorithmically when in person has failed, since the best algorithms perform better than people.	Add that suggestion.
	63A	10.3	54	1815	Grammar: Remove the 'of'	see comment

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

Please submit responses to dig-comments@nist.gov by March 24 April 14, 2023

Organization:	*SOCIAL SECURITY ADMINISTRATION*
Name of Submitter/POC:	*Jeffrey Walsh*
Email Address of Submitt	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
	63B	2	3	386-387	Would this be better presented as "AAL1 provides some resistance to subversion of the authentication process." (replace "some" with "strong" and "very strong" for AAL2/3 respectively). The claimant will always control the authenticator to successfully authenticate; the difference in AALs is the resistance of the authentication protocol to subversion (as described in previous paragraph, lines 380-382.)	
	63B	4	6	439	This requirement means that almost all publicly facing applications will require AAL2, from a low/limited impact service where a single individual checks the status of their benefits application, to a service where a DI error could lead to serious consequences, such as an attorney managing multiple beneficiary claims. Yet, the authentication control for both would be AAL2. To meet the needs of the general population, and to implement controls commensurate with the risk, phishing resistant MFA cannot be required for Low/Limited impact applications, however for applications where a DI error has more serious consequences, phishing resistance should be required.	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. 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	4	6	439-440	"Therefore" does not necessarily hold here. EO13681 requires that services that involve PII require multiple factors of authentication. A multifactor credential can be AAL1 and therefore suitable for PII disclosure under EO13681 (for instance, a multifactor credential that does not require reauthentication every 12 hours would not meet AAL2 requirements but would still be suitable for PII disclosure under EO13681.)	
	63B	4	6	440	"personal" information excludes many types of sensitive and valuable information, such as proprietary business data and financials	Change 'personal' to 'sensitive' or 'highly sensitive'
	63B	4.1.1	6	450	The term "memorized secret" to describe a password seems outdated. Best practice is that passwords not be memorized, but rather use password managers (which are explicitly allowed later in the document).	Consider renaming to "Password" in the guidance to reflect that there is no longer any expectation of memorization.
	63B	4.1.2.	7	460	"SHALL use approved cryptography" lacks specificity. Approved by whom?	Change to "cryptography approved for use in the Federal Government by NIST" for clarity.
	63B	4.4	12	631-	Is there an intersection between digital identity risk and OMB M-17-12, 'Preparing for and Responding to a Breach of Personally Identifiable Information?'	
	63B	4.5	13	Table 1	Phishing resistance, AAL1 - Not Required Under M-22-09, phishing resistance must be provided as an option if an MFA is offered.	Recommend that this be divided into 'Recommended' and 'Required' options for AAL2 so agencies will be able to mandate phishing resistance for some services/applications.
	63B	5.1.1	14	667	The memorization component is no longer true; users cannot be relied on to memorize large numbers of passwords. "recorded or memorized by" would be more accurate.	Change 'memorized by' to 'memorized or recorded by'
	63B	5.1.1.1.	14	678	"If the CSP disallows" allows the CSP to allow commonly used and expected passwords and still declare itself AAL2 compliant.	Recommend that this be made into a requirement 'The CSP SHALL disallow the use of memorized secrets that are commonly used, expected, or known to be compromised.'
	63B	5.1.1.2.	16	729-731	Along these lines, should verifiers implement automated attack prevention techniques, as the draft guidance requires for IDP?	
	63B	5.1.1.2.	16	733	"Verifiers SHALL NOT...prohibiting consecutively repeated characters". This is effectively mandating that such insecure passwords as '88888888' be allowed.	Remove "or prohibiting consecutively repeated characters" as an example.
	63B	5.1.1.2.	16	766 & 811	"The salt SHALL be ... chosen arbitrarily" allows for the use of predictable salt values.	Recommend changing this to 'the salt SHALL...be generated by a NIST-approved RNG [SP800-90A]'.
	63B	5.1.2.1	17	793	Consider "at least 20 bits or 6 decimal digits of entropy" to allow 6-digit numbers (which provide about 19.93 bits). This language is used in 5.2.12.	
	63B	5.1.3	18	819	This section does not include any 'SHALL' statements so reads as informative, yet is not labeled as such.	Recommend making any requirements clear by using explicitly 'SHALL' statements, or by clearly marking the section as informative.
	63B	5.1.3.1.	21	854	"SHALL be encrypted" - are there any requirements for the encryption?	Make the encryption requirements explicit
	63B	5.1.3.1.	21	864	"Suitably secure" is quite vague.	Recommend making a clear requirement for the security.
	63B	5.1.3.1.	21	866	To clarify, is NIST no longer permitting sending the OOB over a PSTN (e.g., landline) network?	
	63B	5.1.3.1.	21	869-870	"device SHOULD NOT display the authentication secret while it is locked by the owner". In the case of SMS messages, this may be under the control of the device owner rather than the verifier.	Consider adding "to the extent practical" to recognize that the capabilities of the parties may be limited in certain circumstances.
	63B	5.1.3.1.	21	882	Does an application need to meet certain requirements to be considered 'secure'?	
	63B	5.1.3.2.	22	903	Per earlier comment, consider "at lease 20 bits or 6 decimal digits of entropy"	see comment
	63B	5.1.3.2.	22	907	Sec 5.2.2.2 limits to 100 consecutive failed attempts. Does NIST envision the throttle resetting when a new secret is generated?	
	63B	5.1.3.3.	23	918-920	Does NIST envision particular methods here, such as an LRN query or MNO service?	
	63B	5.1.4.1.	24	969 & 1024	"If a subscriber needs to change the device used for a software-based OTP authenticator, they SHOULD bind the authenticator application on the new device to their subscriber account". This is a device-based authenticator, so when the device is changed rebinding needs to occur.	Recommend changing this to a 'SHALL'
	63B			1100 & 1186	Although this implies that the key was generated on the device, that should be made explicit.	Change to 'that SHALL be generated on the device and SHALL NOT be exportable'.
	63B			1103	What, exactly, makes a processor 'suitably secure'?	Provide requirements.
	63B	5.1.8.1	29	1157	Typo: 'requirements'	Correct.

	63B		30	1202	Grammar: Change "(TEE), trusted" to "(TEE), or trusted"	see comment
	63B	5.2.2	31	1233-1235	How does a subscriber who is locked out as a result of rate limiting regain access?	Consider adding: "The CSP SHOULD provide a mechanism to reset the limit of consecutive failed authentication attempts. If implemented, this mechanism SHALL incorporate mechanisms to reduce the likelihood that an attacker will use the
	63B	5.2.2	31	1235	100 consecutive failed authentication attempts on a single subscriber account seems to be way too permissive and poses a risk to the subscriber. Why is this number not a lot less? Closer to 10 seems more appropriate.	Change to 10 consecutive
	63B	5.2.2	31	1238	Consider adding an additional example: "Implementing automated attack detection as described in 800-63A-4 Section 5.3.1."	see comment
	63B	5.2.2	32	1249	"the verifier SHOULD disregard" The impact of this requirement is unclear. What does it mean to "disregard any previous failed attempts for that user from the same IP address"? Since the rate limiting guidance limits the number of failed authentications, is it not the case that all previous failed attempts (regardless of IP address) are disregarded?	
	63B	5.2.3		1259	The biometric False Match Rate (FMR) does not provide confidence in the authentication of the subscriber by itself. In addition, FMR does not account for spoofing attacks. Recommend changing to 'does not provide sufficient confidence'	see comment
	63B			1303	"Certification by an approved accreditation authority" - Approved by who?	Clarity is needed
	63B	5.2.10.	38	1463	What is the organization being referred to here (e.g., CSP, Verifier, or RP)?	Clarity is needed
	63B	5.2.10.	38	1465-1466	In evaluating risk, an organization can typically choose to accept, mitigate, transfer, or reject the risk. This statement frames the only options as accept/reject. Mitigation could be a reasonable option for restricted authenticators (e.g., for SMS, to use MNO-operated sources to evaluate risk).	Consider: "If at any time the organization determines that the risk to any party is unacceptable, then the organization SHALL remediate the risk, for example, by incorporating compensating controls or not accepting the authenticator.
	63B	5.2.10.	38	1476	Add "risk to subscribers and relying parties"	see comment
	63B	5.2.10.	38	1479	From the perspective of the RP, the authentication assertion may not indicate that a given authentication was made using a restricted authenticator. The following language would provide the RP additional tools to measure and manage risks arising from their use: "To allow for situations where an RP determines that the risk of accepting a restricted authenticator is unacceptable, the CSP SHALL provide a mechanism that prevents the restricted authenticator from being used to authenticate to that RP. The CSP SHALL also include an indicator in authentication assertions that indicates whether the subscriber used a restricted authenticator."	see comment
	63B	6.1	41	1581	Is the limitation to only unsuccessful intentional, or should the record also contain information about the source of successful authentications?	
	63B	6.1	41	1583	"the associated keys " Not all authenticators utilize keys	Change to "any associated keys"
	63B	6.1.1.	42	1602	The term "primary authenticator" is not defined. Which authenticator does NIST consider to be "primary", and what are the implications (if any) of an authenticator being so designated?	clarify
	63B	6.1.1.	42	1622-1623	Should it be required that the device is issued in-person, or only the long-term secret? For instance, consider a TOTP secret that an applicant loads in-person into an authenticator application on a smartphone. Even though the smartphone is not issued in person, should this be allowed?	
	63B	6.1.2.1.	43	1635	Change "at the AAL" to "at the highest AAL"	see comment
	63B	6.1.2.3.	44	1669	"accounts that have not been identity proofed (i.e., without IAL)". This is IAL0.	Update to include the term IAL0
	63B	6.1.2.3.	44	1673	In addition to the case of a forgotten password, is this the process to be followed if there is evidence of compromise of the memorized secret as described in 5.1.1.2 ("verifiers SHALL force a change if there is evidence of compromise of the authenticator.")	
	63B	6.1.2.3.	44	1678-1683	(major) Please consider one physical authenticator rather than two at AAL1/AAL2, e.g., subscriber must prove ownership of a previously-registered address and control of a previously-registered second factor. Requiring a second physical authenticator adds a significant usability cost that will prevent successful recovery in this extremely common use case. (moderate) Would NIST consider reusing the enrollment code allowances in 63A, Section 5.1.6? That section allows codes to be generated through a secure optical label or secure link, which is not allowed here. It is not clear why a QR code would be acceptable for an enrollment code but not acceptable for account recovery. (minor) For UX purposes, consider the standard 20-bits of entropy instead of a random alphanumeric code. Random alphanumeric codes are difficult to convey by telephone and commonly mis-entered	
	63B	6.1.2.3.	44	1688	10 minutes may not be sufficient in areas with poor cell service.	
	63B	6.1.2.3.	44	1689	Recommend that email not be allowed for AAL2 or above. Email addresses may not be sufficiently protected and demonstrate no physical control or access requirement, unlike phones & physical mailboxes.	Remove email for AAL2 and AAL3
	63B	6.1.3.	46	1746	This represents a point-in-time assurance, but would not in itself prevent the subscriber from later reverting to a weaker authenticator.	Suggest replacing "able to establish that the stronger authenticator is in fact being used" with "able to establish confidence that the stronger authenticator is in continuous use and that reverting to a weaker authenticator will
	63B	6.2.	46	1763	Recommend changing this to a SHALL. Why wouldn't this be done?	
	63B	6.2.	46	1764	Suggest changing to 'following detection of compromise" for clarity.	
	63B	6.2.	47	1773	Recommend that email should NOT be used as an 'address of record'. It's often an IAL1/AAL1 account, or less.	Remove email

	63B	6.4.	47	1788	Consider adding: CSPs SHALL allow subscribers to unbind specific authenticators previously bound to the subscriber account where doing so would not reduce the AAL below the minimum level permitted by the CSP. Before unbinding the new authenticator, the CSP SHALL require the subscriber to authenticate at AAL1. Where the unbinding would result in reducing the highest attainable AAL or IAL of the subscriber account, the CSP SHOULD warn the subscriber prior to unbinding the authenticator. The CSP SHOULD send a notification of the event to the subscriber.	see comment
	63B	7.1.1	50	1870	Should this be SHALL NOT? Are there circumstances where including cleartext PII in a session cookie is acceptable? (CWE-315)	Recommend changing this to 'SHALL NOT' to protect PII.
	63B	8.1	52	1928	As the security situation around LastPass has illustrated, a password manager, if used, opens numerous other vulnerabilities (compromise of the vault cyphertext, master password, or vulnerabilities in pre-entry (https://bugs.chromium.org/p/project-zero/issues/detail?id=1930)). These types of threats may be worthwhile to note.	
	63B	8.2	57	1945	Another vector is attacks against support functions, including insider threats involving CSP agents. CSPs need to ensure that customer support representatives are properly trained and that the organization employs effective internal controls to guard against attacks that use customer support services as a vector.	

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

Please submit responses to dig-comments@nist.gov by March 24 April 14, 2023

Organization:	*SOCIAL SECURITY ADMINISTRATION*
Name of Submitter/POC:	*Jeffrey Walsh*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
	63C	2	3	338-339	"In a federation scenario, the CSP provides a service known as an identity provider, or IdP." The CSP may or may not be the IdP. For example, GSA's USAccess may act as a CSP and issue a PIV to a second agency. That second agency may federate with a third agency, acting as the IdP while using a USAccess-issued PIV for user authentication, and may also provide additional attributes.	correct the sentence
	63C	2	4	386 & 930	This use of 'subscriber' here is confusing. The person is a subscriber to the CSP/IdP, not to the RP.	Recommendation: change from 'RP subscriber account' to 'RP user account' or 'Provisioned RP account'.
	63C	4.2	9	513	"Government-operated IdPs asserting authentication at FAL2 SHALL protect keys. " Strongly recommend dropping the 'government-operated' qualifier so that all IdPs accepted by government RPs have the same baseline security.	see comment
	63C	4.4	9	545	" or an indication that no IAL claim is being made" This is IAL0 - recommend that IAL0 be asserted in this case.	see comment
	63C	4.4	10	547	"or an indication that no AAL claim is being made" For consistency, recommend an AAL0 level be added to the guidance and then asserted here.	see comment
	63C	4.4	10	560	""IAL1", the lowest numbered IAL described in this suite" Isn't IAL0 the lowest numbered IAL?	Fix this so IAL0 is used
	63C	5	13	618	"identity attributes" The IdP may also provide roles used for authorization	remove the 'identity' qualifier and just say 'attributes'.
	63C	5.2.1	19	784	"Protocols requiring the transfer of keying information SHALL use a secure method" What are the minimum requirements for a 'secure method'?	provide requirements
	63C	5.2.1	19	786	"shared secrets or public keys. Any" What are the cryptographic requirements for the keys?	provide requirements
	63C	5.3	21	829	"A subscriber's attributes SHALL be transmitted between IdP and RP only for identity federation transactions or support functions such as identification of compromised subscriber accounts as discussed in Sec. 5.5. A subscriber's attributes are not to be transmitted for any other purposes" IdPs need to be able to send attributes needed for authorization in addition to identity attributes. This statement seems to prohibit that.	Recommend changing this from for "identity federation transactions" to for "identity or authorization federation transactions".
	63C	5.4	24	930	"RP Subscriber Accounts" Since a user subscribes to an IdP, another term should be used for that individual's account at an RP, since they are not subscribed to the RP.	Suggestion: Change "RP Subscriber Accounts" to "RP User Accounts" or "Provisioned RP Accounts".
	63C	5.4.2.	27	1011	Typo - change "from with each other" to "from each other"	see comment
	63C	5.4.2.	28	1023	"The IdP SHOULD signal downstream RPs when a subscriber account is terminated, or when the subscriber account's access to an RP is revoked. " I would add a requirement to provide a reason for the termination or revocation in the case of suspected fraud/account compromise. This can alert the RP to review prior transactions to look for suspicious activity.	see comment
	63C	5.4.2.	28	027, 1062, 1068, 1126	"Upon receiving such a signal, the RP SHALL terminate the RP subscriber account and remove all personal information associated with the RP subscriber account" Suggest removing this statement for IAL1 and above accounts. If an individual has an account at a federal agency which offers the option to access a service using Login.gov or ID.me, for example, it is not uncommon for someone to have both credentials and then cancel one. Their account at the RP shouldn't then be deleted. Even if the user terminated all of their federated credentials, their information with the agency shouldn't be deleted - it should be retained so they can get a new credential and access their information in the future. In many cases, the account at the RP should be independent of the IdP.	see comment
		5.4.5.	29	1083	"the RP SHOULD employ a time-based mechanism to identify RP subscriber accounts for termination that have not been accessed after a period of time, for example, 120 days since last access." What is the rationale for doing this? Many government services are only accessed annually, or even every few years.	Remove this 120 day example
	63C	5.5	30	1118	"An IdP MAY disclose information on subscriber activities to RPs for security purposes" Recommend changing this to a SHOULD, or even a SHALL.	see comment
CC	63C	5.5	30	1120-1121	"An RP MAY disclose information on subscriber activities to IdPs for security purposes" Recommend changing this to a SHOULD or a SHALL in the case of a compromised or fraudulent account.	see comment
	63C	5.7	32	1203& 1210	"The IdP/RP MAY send a signal regarding...The account is suspected of being compromised." Strongly recommend changing this to a SHALL. It is irresponsible for account compromise to be detected without sharing that knowledge across the federation.	see comment

	63C	6	34	1243	"Digital signature or message authentication code (MAC)" Should there be a requirement that NIST-approved crypto be used for these?	
	63C	6	34	1248	" or an indication that no IAL is asserted." This is IAL0, so this statement is not needed.	remove statement
	63C	6	35	1266	"All metadata within the assertion SHALL be validated" There may be metadata that does not require validation. Recommend changing to: "The following metadata...SHALL be validated:"	see comment
	63C	6.1	36	1301-1305	This section reads like a definition rather than a requirement. If it is a definition/informative, it would be helpful to explicitly label it as such. If it is a requirement, it needs to be rewritten so that any requirements contained in the section are clearly stated.	clarify
	63C	6.1.2.1	37	1353	"The RP would then prompt the subscriber to present the certificate from their smart card in order to reach FAL3." The presentation of the certificate does not, by itself, achieve FAL3.	I would state the additional steps required, or rephrase to something like "The RP then prompts the subscriber to authenticate using their smart card certificate in order to reach FAL3."
	63C	6.2.5.	44	1481	"A pairwise pseudonymous identifier (PPI) allows an IdP to provide..." Should this be stated as a requirement, such as "A pairwise pseudonymous identifier (PPI) MAY be used by an IdP to provide multiple..."	
	63C	6.2.5.1	44	1501	grammar: "between the IdP and the federation proxy itself. The proxy, acting as an IdP, can itself provide pairwise" Editorial comment: Remove both instances of the word 'itself'.	see comment
	63C	6.3.	46	1558	"The IdP can indicate in the assertion when the last time the subscriber's attributes have been updated in the subscriber account"	Consider making this a SHOULD to improve data quality.
	63C	7.1	48	1621	"SHOULD have a lifetime of no more than a small number of minutes in length." "a small number of minutes in length" may mean 2 minutes to one developer and 120 minutes to another. How is the maximum amount of time required for the lifetime of the assertion reference determined? Please provide a more concrete requirement that is evidence-based.	see comment
	63C	7.2	52	1666-1669	"Though it is possible to intentionally create an assertion designed to be presented to multiple RPs, this method can lead to lax audience restriction of the assertion itself, which in turn could lead to privacy and security breaches for the subscriber across these RPs. Such multiRP use is not recommended." Why not just prohibit this? Is there any reason this is needed in the federal government?	
	63C	7.3	52	1680	"authenticated protected channel." Are the minimum security requirements for creating an authenticated protected channel referenced anywhere?	Provide or reference requirements
	63C	8	53	1698	"including the CSP which now acts as an IdP" The CSP and IdP may not be the same entity.	update