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

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

Organization:	***General Services Administration***
Name of Submitter/POC:	***General Services Administration***
Email Address of Submitter/POC:	

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	Overall	Does the guidance sufficiently address privacy?	NA	NA	GSA assesses that the guidance does sufficiently address privacy risk management via reference to the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management. In addition, the General Privacy Requirements and Additional Requirements for Federal Agencies appear to sufficiently address privacy standards for federal agencies, regardless of whether they operate their own identity service or use an external CSP as part of their identity service.	
2	Overall	General	NA	NA	The four volumes in the aggregate are complicated and require expert analysis. Recommend working with CISO Council to update the Digital Identity Risk Acceptance (DIRA) template to derive required AAL, IAL, and FAL levels for Federal systems. This will ensure consistent and more accurate determinations for required auth, identity, and federation levels.	Updated DIRA for IAL AAL and FAL determination.
3	Overall	General	NA	NA	Align NIST 800-63 and M-22-09 requirements to NIST 800-53 requirement set more specifically.	800-53 R5 should more specifically align to 800-63 vs the current general reference to the guideline.
4	Overall	General	NA	NA	The security of identity validation sources and verification providers (particulary commerical sources) is challenging as few align with Federal cybersecurity requirements (e.g., FedRAMP, NIST 171, traditional A&A, etc) and have proven to themselves lack good security (e.g., MFA, good cyber hygiene, end of life software, etc). While this is beyond the scope of NIST 800-63, it requires a broader effort including OMB to define security requirements (e.g., FISMA broadly) before they can be used. What level of security compliance (e.g., SOC, ISO, PCI, 171, FedRAMP, traditional A&A, etc) is required before for a Federal system to integrate with a commercial solution that acts as an validaiton source or provider?	NIST and OMB (GSA can help) should work to define compliance requirements for Federal usage and integration with Federal and commerical validation source and verification providers.
5	Overall	How are session management thresholds and reauthentication requirements implemented by agencies and organizations? Should NIST provide thresholds or leave session lengths to agencies based on applications, users, and mission needs?	NA	NA	GSA recommends NIST remove most of Section 7.1.* in Volume B, and Section 5.6 in Volume C, related to session management and reauthentication. Applications, users and types of users impact the session management thresholds. For example, there has been confusion for 800-63 Version 3 and the session management clauses introduced. While the clauses attempt to separate the "relying party" responsibilities from the CSP or IDP responsibilities, the separation is not clearly understood across teams nor aligned with modern system architectures including mobile use cases, single page applications, and SaaS applications used across the enterprise user focused use cases.	Remove most of Section 7.1.* in volume B related to session management. Applications, users and types of users impact the session management thresholds.
6	63C	How are session management thresholds and reauthentication requirements implemented by agencies and organizations? Should NIST provide thresholds or leave session lengths to agencies based on applications, users, and mission needs?	NA	NA	GSA recommends simplifying and clarifying the distinctions between CSP (Volume B) and IDP (Volume C). There are overlapping sections and requirements for Reauthentication and Session Requirements. GSA applauds the attempt in separating Volume B and Volume C requirements. Volume C attempts to explain a few versions of the styles of approaches to identity federation frameworks. However, the attempt is possibly introducing more confusion for implementing controls for a CSP that is also an IDP. For example, Volume C Section 5.6 references "See [SP800-63B], Sec. 7 for more information about session management requirements for both IdPs and RPs". However, there are conflicting requirements. Similar to Volume B Section 7.1.*; GSA recommends removing the Volume C Section 5.6 Reauthentication and Session Requirements or moving this sub-section to a Informative only section.	Similar to Volume B Section 7.1.*; GSA recommends removing the Volume C Section 5.6 Reauthentication and Session Requirements or moving this sub-section to a Informative only section.
7	Overall	Is any language in the guidance confusing or hard to understand? Should we add definitions or additional context to any language?	NA	NA	GSA recommends the Informative sections in all volumes be updated for plain language. Informative sections are useful for business teams to review for high level use cases and examples. Since informative sections do not contain normative requirements, a plain language approach benefits additional teams and readers without sacrificing the standards development organization language needed for the normative sections.	GSA recommends the Informative sections in all volumes be updated for plain language.
8	Overall	What applied research and measurement efforts would provide the greatest impact on the identity market and advancement of these guidelines?	NA	NA	The Trusted Referee concept is incredibly important to providing an avenue for all individuals access to online government services and GSA supports its continued development. Because of this importance, GSA recommends the trusted referee concept would benefit from a separate volume for a special publication after more detailed research, measurements, and data analysis and modeling. This additional research - based on real world data available - will inform, and continue to benefit, the development of this concept for real use cases (such as for disaster relief, undocumented people, unbanked people, etc). As it stands currently, the special publication section requiring ALL CSPs to define and implement a trusted referee process will result in numerous different unaligned practices, depending on CSP and agency goals. Each CSP will separately define what risk-based decisions are sufficient to establish a trusted referee process and then define their own policies and procedures with minimal input or insight into a broad set of challenges and changing landscapes across the different agencies, services, and use cases. Additionally, based on historical approaches, algorithms developed by closed source communities and offered for services may also be proprietary. A clear set of metrics is needed to measure and compare the effectiveness of algorithms.	Based on the talents and expertise of Commerce and NIST for data science, machine learning, and measuring - a new volume or special publication after detailed research and analysis for Trusted Referee would be assumed as within scope. Agencies and CSPs would benefit from this new volume or special publication including examples of factors to consider for each type of risk-based assessment for each use case and guidance on how proofing these individuals may vary at different IAL levels/
9	63-Base	2	3	357	A digital identity need not be unique in the context of a digital service. Take, for instance, a service that uses claims to determine certain characteristics (e.g., is a legal adult) but need not require any other information. The digital identity need not be unique in the context of that service.	Change: "always unique" to "typically unique"
10	63-Base	2	3	370	Consider drawing a parallel between risks associated with digital identity and risks associated with identity in general (e.g., verifying a customer's identity by phone)	Add: "Like all risks involving identity, risks associated with digital identity stretch beyond..."

11	63-Base	2	3	390	"Is the same subject that previously accessed the service" -- in some situations, a digital service may require confidence that the same subject previously accessed a different digital service. (e.g., Service 1 = submit a form, Service 2 = check form status. Service 2 would need confidence that the subject accessing the service for the first time is the same person who previously accessed Service 1.)	Change "the service" to "a given service"
12	63-Base	2	3	395	Consider adding "usable" to this list to align with the four considerations in the rest of the spec.	Add: "deploying secure, private, usable, and equitable..."
13	63-Base	2	4	399	The sentence on lines 399-403 is difficult to parse. Conside restructuring for clarity.	Change to: "Additionally, this publication provides instruction for credential service providers (CSPs), verifiers, and relying parties (RPs) that supplement the NIST Risk Management Framework [NISTRMF] and its component special publications. The publication describes the risk management processes that organizations should follow for implementing digital identity services."
14	63-Base	2	4	407	The statement refers to authentication but discusses digital identity more broadly.	Change "While digital authentication supports" to "While digital identity supports"
15	63-Base	2.2	5	447	The statement "for non-federated systems" suggests that IAL and AAL are not required for federated systems.	Change "For non-federated systems" to "For both federated and non-federated systems"
16	63-Base	2.2	5	447	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 not assigning an IAL at all to transactions that do not require evidence in a real-world identity, (AAL can also be optional under the guidance in 800-63A, Section 6.1, line 1238, which allows identity proofing without provisioning a subscriber account and therefore does not require authentication.	Add or change to: "Agencies will accept up to three components referred to Identity Assurance Level (IAL), Authentication Assurance Level (AAL), and Federation Assurance Level (FAL). Not all components will be applicable to every system; for instance, Federation Assurance Level is not required for non-federated services."
17	63-Base	2.2	6	490	The draft states, "Effective enterprise risk management is multidisciplinary by default...". The term "by default" implies a lack of conscious choice rather than intentional design.	Change "by default" to "by design"
18	63-Base	4.1	11	614	The draft states that an applicant is "the subject to be identity proofed". The definition does not include a person in the process of obtaining an IAL0 credential.	Change to: "Applicant - the subject to be identity proofed or credentialed"
19	63-Base	4.1	11	636	The guidance refers to "the usual sequence of interactions". However, for a number of reasons, it is often more practical to begin by establishing authenticators, and then complete identity proofing. Following proofing, the identity is bound to the existing credential. This approach ensures that a user who is not able to complete authenticators will not need to restart the entire identity proofing process.	Change "The usual sequence" to "A common sequence"
20	63-Base	4.2	14	717	The draft states, "Alternatively, the authenticators may be invalidated and destroyed...". CSPs can unbind an authenticator from a subscriber account without invalidating and destroying the actual authenticator.	Change to: "Alternatively, the authenticators may be unbound, invalidated, or destroyed..."
21	63-Base	4.2	15	719	The draft states, "Subscribers have a duty to maintain control of their authenticators." Subscribers must not only retain control, but must obtain exclusive control (e.g., must not intentionally share the credential).	Change "maintain control" to "maintain exclusive control"
22	63-Base	4.2	15	724	NIST 800-63-4 and 800-63A-4 do not appear to refer to an abbreviated proofing process, other than the provision in63B § 6.1.2.3, ll. 1659-1660. Is this the "abbreviated" process referred to here?	Clarify whether the abbreviated process is solely used for account recovery as outlined in 800-63B-4, section 6.1.2.3.
23	63-Base	5	23	924	The opening paragraph of Section 5 can be more explicit on the actors and actions involved in assessing digital identity risks.	Change to: "This section provides details on the methodology that RPs use to assess digital identity risks for digital services and assess xALs."
24	63-Base	5	23	928	A digital service may comprise several functions, each with their own risk. The guidance does not specifically state whether the unit of assessment is the digital service as a whole or the transaction, although line 502 suggests that partitioning is permissible. Suggesting language would clarify to assessors.	Add: "Organizations may choose to evaluate a digital service as a single entity or partition the functionality of a digital service into discrete transactions and evaluate each transaction separately."
25	63-Base	5.1	24	967	Section 5.1 outlines the process for conducting initial impact assessments and identifying risks specific to an RP application or service. What is the CSP's or IDP's role in conducting impact assessments, if any? Would an organization create a single impact assessment, or would they work with customers to develop impact assessments for each use case and user population?	Clarify the role and responsibilities of a CSP or IDP in assessing and analyzing adverse impacts of failures in identity proofing, authentication, and federation. (e.g., on line 924, change "This section provides details on the methodology for assessing digital identity risks for each xAL" to "This section provides details on the methodology for RPs to assess digital identity risks for each xAL")
26	63-Base	5.3	36	1381	Section 5.3 states that "organizations SHALL establish and document an xAL tailoring process... in the Digital Identity Acceptance Statement."	Define the word "organization" and clarify the use of tailoring for CSPs and IDPs, and the role and responsibilities of drafting a Digital Identity Acceptance Statement.
27	63-Base	5.5	39	1496	What does continuous improvement look like for a CSP that serves many RPs? Any continuous improvement that an IDP or CSP does to their service offerings needs to be either: deemed as an acceptable risk and adopted by all partners at the given xAL, or requires a user to provide additional information if they sign in to an RP with stricter requirements. See also Section 5.3.2.	Consider clarifying the process of continuous improvement for CSPs that serve many RPs and use cases, and in federated models.
28	63-Base	4.*	All	All	The informative sections - including Section 4 descriptions in 800-63 base volume - contain statements using the "should" qualifier. Use of "should" or "must" in a descriptive and informative only section can be confused with Normative sections and requirements.	Remove and replace all uses of "should" or "must" in the Informative sections of all 800-63 volumes.
29	63-Base	4.3.1	18	791	For item 2, a more common example could be pairing "something you have" and "something you know". For example, a smartphone using a passcode or Face or Touch Unlock to enable WebAuthn?	Consider an additional or alternative example to avoid implying that hardware with a cryptographic key is necessary to fulfill item 2.
30	63-Base	5.1.2	25	998	Consider clarifying that organizations need only consider proximate harms, i.e., organizations must consider all reasonably-foreseeable direct and indirect impacts, but do not need to consider chains of events that could result in a non-promixate adverse impact.	Change "potential impact of" to "expected potential impact of"
31	63-Base	5.1.3	27	1065	The draft states, "Each assurance level, IAL, AAL, and FAL (if accepting or asserting a federated identity) SHALL be evaluated separately." This guidance caveats FAL as conditional, but IAL and AAL can also be non-applicable/IAL0. If there is no identity proofing, IAL0 is automatic and there is no need to assess. If there is no identity proofing, there is no risk of identity proofing errors.	Change to "Each applicable assurance level (IAL, AAL, and FAL) SHALL be evaluated separately."
32	63-Base	5.1.3	28	1071	In 800-63-4, "Low" corresponds to limited harms (as opposed to serious and catastrophic). We are concerned that organizations will reserve IAL1 for extremely low-risk scenarios instead of mainstream use. The term "limited" should be applied consistently to describe LOW risk (consistent with FIPS 199).	Replace terms such as "insignificant" and "inconsequential" consistently with the word "limited", just as the word "serious" is consistently associated with "Moderate" impact. Include more language that makes it clear that IAL1 is not only for extremely low-risk scenarios. "slight" -> "limited" (line 1071); "limited, short-term" -> "limited" (line 1095), "an insignificant or inconsequential" -> "a limited" (line 1111); "an insignificant or inconsequential" -> "a limited" (line 1127)
33	63-Base	5.1.3	27	1071	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. At the point of evaluation, the RP may not know the technical mechanism or the disparities such a mechanism may introduce.	Revert to 800-63-3 language and keep "Impact of harm to agency programs or public interests" category.
34	63-Base	5.1.3	27	1099	Impact levels and damage to trust and reputation should have more clarity and examples.	GSA recommends revising to be more specific.
35	63-Base	5.1.4	29	1139	The terms "risk" and "impact" should not be used 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.	Review use of "risk" and "impact" throughout section 5 to ensure consistency with other risk management framework documents.
36	63-Base	5.1.4	29	1139	The draft states, "... organizations SHALL assess the potential risks and 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 "minimize their impact" to "manage their impact and likelihood"

37	63-Base	5.1.4	29	1150	The draft states that entities should consider the impact of specific modes of failures for identity proofing, like "The impact of not providing service to an eligible subject due to barriers, including biases, faced by the subject throughout the process of identity proofing." At the time of the assessment, the RP may not have selected a CSP and therefore not know the technical mechanisms. How can the RP evaluate "biases faced by the subject throughout the process of identity proofing" at this stage?	Change to: "To the extent known, the impact of not providing service..."
38	63-Base	5.1.4	29	1166	Editorial: "digital service" intended in place of "digital identity system"	Change "digital identity system" to "digital service"
39	63-Base	5.2.2	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.	Make IAL1 definition in the base spec consistent with the 63A definition (comment below). IAL1 should not be presented as having weaker evidence validation and verification requirements relative to IAL2 where it does not.
40	63-Base	5.2.2.1	31	1197	Section 5.2.3.1 Selecting Initial IAL contains an important distinction for digital identity risk assessments. "Not all RP applications will require identity proofing. If the RP application does not require any personal information to execute any digital transactions, the system can operate without identity proofing users of the RP application. " Volume A also includes the IAL0 designation. Not requiring any personal information and also not requiring identity proofing is important for anonymous transactions and protecting a person's privacy. This scenario was covered in 800-63-3 using self-asserted health information for drug trial tests as an example. Another scenario was/is when the business transaction itself contains an identity proofing process (govt example: immigration processes, asylum seekers). Adding the IAL0 to the 5.2.2.1. Identity Assurance Level section will help emphasize that IAL0 is an option and outcome for risk assessments. Currently (800-63-3), this option is often misunderstood and lacking in the federal agency digital identity risk assessment processes (documentation).	Option: Add IAL0 to Section 5.2.2.1 to align with 800-63A volume. Alternative Option: see additional GSA comments and suggestions to remove IAL0 since FAL and AAL do not also have an "0" option explicitly defined. Just as FAL is not required for a service that does not use federation, so too is IAL not required for a service that does not require identity proofing. GSA recommends consistency for all. Choose one or the other, to maintain and promote consistency.
41	63-Base	5.2.3	32	1238	The draft states, "These 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, but rather potential impacts. Those potential impacts are primarily non-cybersecurity oriented, affording great weight to fraud, privacy, environmental, and personal harms that can result from an identity error.	Change to: "These initial selections are based on a number of factors, including security. These impacts will be tailored..."
42	63-Base	5.2.3.1	33	1267, 1308, 1351	The guidance requires organizations to consider “potential impact” and encourages identifying a “worst case”. Requiring organizations to attach an IAL to an envisioned worst-case scenario will result in over-assessment since the worst-case downstream scenario for even the most benign transaction can be catastrophic. Instead, consider reasonably-foreseeable harms and determine controls conforming to those harms. Example: A person can suffer a fatal injury en route to the physical site for in-person identity proofing. It would not be practical for assessors to consider that an identity error could result in loss of life should that worst-case chain of events occur.	Replace “worst-case” with “expected worst-case”
43	63-Base	5.2.3.1	33	1280	The language in the draft recommends initially selecting IAL1 if the overall risk (as shown in Table 1) is "Low". However, high risks to the individual -- including loss of economic stability, safety, health, or environmental stability as a result of being unable to access services -- could result in a "High" combined impact level. In those cases, IAL1 may be the best solution, even though the spec would suggest a higher IAL because of the combined risk level calculated in Table 1. This is mentioned briefly (Lines 1284-1289) but could be more strongly emphasized.	Consider updates to the impact analysis that address the conflict between "high risk" mission delivery and impact scenarios to the individual, and selecting a lower xAL level. Consider calling out the risk of fraud/identity theft to both the individual and the organization vs. the ability to access services, such as the extent a malicious actor can immediately engage in fraud directly through the application.
44	63-Base	5.2.3.2	34	1231	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:	Replace list as follows: Low impact (no personal information): AAL1 Low impact (involving personal information): AAL2 Moderate impact: AAL2 High impact: AAL3
45	63-Base	5.3.1	37	1404	Editorial: risks intended rather than impacts.	Change "assess impacts" to "assess risks"
46	63-Base	5.3.1	37	1417	The RP needs to both select a CSP or IDP and define an xAL. As written, the xAL depends on the CSP or IDP, but the CSP or IDP also depends on the xAL. This results in a circular dependency, and NIST should outline the order of events.	Review all volumes for circular dependencies across RP, CSP, IDP and inconsistent language.
47	63-Base	5.3.2	37	1440	In order for RPs to make informed risk decisions, they must be provided with detail about deviations, and comparability determinations	Add: Where compensating controls are implemented, CSP/IDPs SHALL make avaiable the deviations, results of their assessment of comparability, residual risk, and justifications for departures to RPs.
48	63-Base	5.3.2	38	1445	What does tailoring look like for a CSP or IDP that serves many RPs with varying impacts and risks? Any tailoring that an IDP or CSP does to their service offerings needs to be either: deemed as an acceptable risk and adopted by all partners at the given xAL, or requires a user to provide additional information if they sign in to an RP with stricter requirements.	Consider clarifying the use of tailoring for CSPs that serve many RPs and use cases, and in federated models.
49	63-Base	General	NA	NA	There is a need for a FedRAMP like certification framework and qualified assessors regime (FedRAMP 3PAO) to review and validate IDP AAL IAL and FAL claims.	NIST and OMB (GSA can help) to defined certification framework for verifying IDP IAL AAL and FAL claims and develop an independent qualified assessor regime similar to what is in place for FedRAMP 3PAOs.
50	63-Base		3	367	The lack of consistency between the terms "digital service", "online transactions", etc., has been a historical source of confusion in applying the guidance. For example, on line 419, a sentence uses "digital service" and "online transaction" in the same sentence. It is not clear anywhere in the guidance what the distinction is (or if NIST intended to draw a distinction). The term "digital service" is used in the guidance alongside similar terms like "digital transaction", "system", and "application". We recommend using these terms consistently and defining the terms in the glossary.	Change: "digital services" to "digital services, including services that issue and maintain digital identities, must be designed...: Define "digital service" in the glossary, and use consistently.
51	63-Base		38	1465	The draft states, "If at any time the organization determines that the risk to any party is unacceptable, then that authenticator SHALL NOT be used". 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). Therefore, a blanket statement that "that authenticator SHALL NOT be used" is overly simplistic.	Change to: "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."
52	63A	2.1	4	402	The draft states that the expected outcomes of identity proofing include "Fraud Prevention: mitigate attempts to gain fraudulent access to benefits, services, data, or assets." Fraud prevention is just one element of fraud mitigation. Fraud controls can be preventative, detective, or responsive (see GAO report 15-593SP). An organization'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.	Change to: "Fraud mitigation: detect, respond to, and prevent access to benefits, services, data, or assets using a fraudulent identity."
53	63A	2.2	4	410	The statement "Self-asserted attributes at IAL0 are neither validated nor verified" is repetitive. If the attributes are validated or verified, they are not self-asserted. More substantively, IAL0 can be removed completely. Just as FAL is not required for a service that does not implicate federation, so too is IAL not required for a service that does not require identity proofing. Just as we do not use FAL0 to describe the former, we do not need IAL0 to describe the latter.	Change to: "Attributes at IAL0 are self-asserted."; or remove designation entirely.

54	63A	2.2	4	412	IAL1 today means "no identity proofing", but the new IAL1 standard does verify the claimed identity against authoritative or credible sources and requires the same evidence as IAL2. This is likely to cause significant confusion for both CSPs and RPs, especially in making the transition from rev 3 to rev 4. Additionally, the rev 3 version of IAL1 meaning "no identity proofing" is likely to cause hesitancy from RPs to adopt rev 4 IAL1 as a viable identity proofing standard.	Rename rev 4 IAL1 to explicitly indicate that it is a new assurance level, distinct from the existing, rev 3 IAL1.
55	63A	2.2	4	412	The evidence required for IAL1 is identical to that of IAL2, and the difference is primarily between the verification of that evidence, which should lead organizations to have confidence in IAL1 as an acceptable standard for identity proofing.	Change to: "IAL1 requires the collection and validation of strong evidence and supports the real-world existance of a claimed identity. Core attributes are obtained from identity evidence or asserted by the applicant and are validated against authoritative or credible sources. Steps are taken to link the attributes to the person undergoing the identity proofing process."
56	63A	2.2	4	416	The draft states that "IAL2 adds additional rigor to the identity proofing process by requiring the collection of stronger types of evidence and a more rigorous process for validating the evidence", despite the validation and evidence requirements at IAL1 and IAL2 being identical.	Change to "IAL2 adds additional rigor to the identity proofing process by requiring verification using biometric comparison or demonstrated access to a digital account at AAL2."
57	63A	4	6	440	Re the requirement: "At a minimum, this SHOULD include accepting multiple types and combinations of identity evidence, supporting multiple data validation sources, enabling multiple methods for verifying identity (e.g., use of trusted referees), multiple channels for engagement (e.g., in-person, remote), and offering assistance mechanisms for applicants (e.g., applicant references)." These items, particularly "supporting multiple data validation sources", can implicate additional fraud vectors. It is important that any alternative capabilities be evaluated for fraud risks so as not to open vulnerabilities.	Add the sentence to the end of the paragraph: "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."
58	63A	4.3	9	497	The guidance refers to documents being "current, and unexpired". Does NIST intend to draw a distinction between "current" and "unexpired"?	Change to "authentic, accurate, and current" if no distinction is intended between "current" and "unexpired"; or explain the difference.
59	63A	5.1	16	696	The phrase "any IAL" appears to exclude IAL0.	If IAL0 terminology is kept, change "any IAL" to "IAL1 and above".
60	63A	5.3	26	1043	The draft states that automated comparison of a facial portrait at IAL1 is optional "where privacy and equity risks outweigh security considerations." This language frames privacy/equity and security adversarily.	Change to: "where the security benefit from higher assurance levels is outweighed by privacy and equity considerations."
61	63A	5.4	28	1092	The draft states that IAL2 identity proofing "allows for both remote and in-person identity proofing processes in order to maximize accessibility while still mitigating against impersonation attacks and other identity proofing errors." This suggests that IAL1 does not mitigate against impersonation attacks and other errors.	Change to "... in order to provide increased mitigation against impersonation attacks and other identity proofing errors relative to IAL1 while remaining accessible."
62	63A	5.6	33	1234	The Resolution row in Table 1 uses the language "Same as IAL1" for the IAL2 and IAL3 requirements. Should the Evidence row use the same terminology when the evidence for IAL1 and IAL2 is the same?	For the IAL2 Evidence cell in Table 1, change to "Same as IAL1" for clarity.
63	63A	7	37	1313	(Editorial)	Change "individuals" to "individual's" (possessive) in Table 2, Fraudulent Use of Identity (Identity Theft) description.
64	63A	7	37	1313	In Table 2, "False Claims", the example states, "An individual claims benefits from a state in which they do not reside." The example may run afoul of the requirement that "Identity proofing is not conducted to determine suitability or entitlement to benefits." What is claimed is the identity attribute (state of residence) rather the benefit itself (which is a programmatic decision separate from identity).	Change to: "An individual falsely claims residence in a state in order to obtain a benefit that is available only to state residents."
65	63A	9.3	51	1734	The CSP's practice statement can include language in its practice statement that allows the CSP to accept name variations as an equity mitigation.	Add: "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)."
66	63A	9.3	52	1759	It is important that RPs do not overassess services, as overassessment can result in more user populations not having the minimum evidence required.	Add: "3. RPs should ensure that the selected IAL is not higher than necessary to be commensurate with the risk of the digital service offering."
67	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 figure 1 and section 4.3 consistent with respect to where evidence is collected. (The reference to collection on line 472 is also potentially affected.)
68	63A	4.1.1	8	466	NIST does not prescribe a specific order for identity proofing and enrollment, so it should be clear that alternative flows are allowable.	Change "Figure 1 outlines the basic flow" to "Figure 1 outlines a basic flow" or "Figure 1 outlines the conventional flow"
69	63A	4.3.3.1	11	555	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.	Change to "The evidence contains a facial portrait or sufficient attributes to uniquely identify the person to whom it relates." (The reference number is required of all evidence.)
70	63A	4.3.3.1	11	557	There are several references in the 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.	Change "unexpired" to "current". By doing so, fair evidence can be considered current for 6 months beyond its expiration without conflicting with other sections in the draft.
71	63A	4.3.3.3	12	594	Under REAL-ID implementation guidelines, there is no requirement for a digital signature. See 73 Fed. Reg. 5271 (Jan. 29, 2008). Such documents therefore cannot meet the requirements for SUPERIOR under this section, although documents that meet REAL-ID standards satisfy the remaining requirements. Under the implementation guide, the only documents that are acceptable at the SUPERIOR level are: US Passports, foreign e-passports, PIV/CAC/TWIC cards, permanent resident card, and Native American Enhanced Tribal Cards. Of these, only the US Passport is generally available to US Citizens (at a cost of $130.) The implication is that most individuals who require an IAL3 credential will need a passport. Requiring a passport for an IAL3 credential would implicate service substantial equitability concerns.	Remove requirement (6)
72	63A	4.3.4	12	599	The draft states, "The CSP SHALL validate all identity evidence collected to meet evidence collection requirements and all core attribute information required by the CSP identity service." 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.	Change to: "The CSP SHALL validate both identity evidence and core attributes for authenticity, accuracy, and currency."
73	63A	4.3.4.1	12	608	The draft states, "The CSP SHALL validate that the evidence is current through confirmation that its expiration date has not passed..." This does not account for the allowance for FAIR evidence to be acceptable up to 6 months post-expiration. Additionally, an ambiguity arose during the COVID-19 pandemic where 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."	Change to: "The CSP SHALL validate that the evidence is current commensurate with its strength. 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, the CSP SHOULD apply the issuing source's policy in evaluating currency."

74	63A	4.3.4.4	13	630	The provision that "Core attributes that are contained on identity evidence that has been validated according to Sec. 4.3.4.1 can be considered validated" introduces a significant vulnerability. 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.)	Replace with: "A CSP MAY consider core attributes that are contained on identity evidence that has been validated at the STRONG level or higher according to Sec. 4.3 to be validated."
75	63A	4.4.1	14	669	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.	Add the sentence: "In performing the physical comparison, the CSP MAY obtain the facial portrait directly from an authoritative or credible source in place of the facial portrait on the evidence supplied by the applicant."
76	63A	4.4.1	15	684	Demonstrating "control of a digital account" is referenced. Earlier in the section, a single sentence is used as the introduction to the five bullet points which include "control of a digital account": "depending on the IAL identity verification requirements presented in Sec. 5." GSA recommends clarifying the "control of a digital account" and the relationship to Sec. 5. GSA assumes NIST is referencing a digital account that has been established at "a different" CSP or IDP and that digital account conforms to a particular IAL. GSA assumes NIST is referencing reuse and establishing a new digital account based on precedence and inheritance.	Clarify standards for demonstrating control of digital accounts as a method for identity verification.
77	63A	5.1.1	16	708	Do a CSP's "core attributes" need to be the same for all users and/or all RPs? For example, could an SSN be validated against one form of evidence for some users, but an address or phone number be used for other users to fulfill the same evidence requirement?	Expand on the definition of core attributes and how CSPs might determine their core attributes.
78	63A	5.1.1	16	713	The draft states that the practice statement should include, "The CSP's policy and process for dealing with identity proofing errors...". The term "dealing with" is informal.	Change to: "The CSP's policy and process for remediating suspected identity proofing errors, including both failing to identity proof a true applicant and erroneously identity proofing a false applicant.
79	63A	5.1.1	16	714	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.	Replace with "The CSP's policy and process for identifying and remediating suspected or confirmed fraudulent accounts, including communicating with RPs and affected individuals."
80	63A	5.1.2.2	18	773	This definition of "processing" would not include the processing of PII for purposes of fraud detection and mitigation.	Add: "mitigate fraud risks, and identify identity proofing errors"
81	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.).	Change to: "Additionally, CSPs SHALL, to the extent practical, implement privacy protective techniques (e.g., transmitting and accepting derived attribute values rather than full attribute values themselves) to limit the proliferation and retention of SSN data."
82	63A	5.1.6	18	871	Item 2 should be removed. It is not a property of enrollment codes, but a requirement of the broader process in which it operates.	Remove or move: "The applicant SHALL present a valid enrollment code to complete the identity proofing process."
83	63A	5.1.6	18	874	The requirement to use an approved random number generator only applies to (a), but (b) and (c) also require a random secret. Should this requirement also apply to (b) and (c)?	1. Replace 3(a) with "A random code containing at least 20 bits or 6 decimal digits of entropy:" or add the requirement, "Random codes SHALL be generated using an approved random number generator" (intended to apply to any enrollment code, not just a random 6-digit number)
84	63A	5.1.6	21	874	The draft states that 20 bits of entropy is required for enrollment codes, but 6 random numeric digits is only about 19.9 bits of entropy.	Change 63A to match 63B rev. 4 which more clearly states, "20 bits or 6 decimal digits of entropy".
85	63A	5.1.7	22	900	The draft states that notifications of proofing "SHALL provide clear instructions, including contact information, on actions to take in the case the recipient repudiates the identity proofing event." Is this in the event that the user wants to delete their account, decline to share their information, or if someone realizes that their information has been used by a malicious actor?	Clarify the use cases when CSPs are required to provide clear instructions and contact information in the event that they are contacted by the user.
86	63A	5.1.8	23	951	The draft states, "CSP SHALL collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject." "Ensures" is too strong a word; surety is never assured.	Change "ensures" to "provides reasonable assurance that"
87	63A	5.1.9	24	979	Do applicant references need to be authenticated separately from the subject of identity proofing? Or put another way, would an applicant reference have a separate CSP or IDP account, or would they "share" an account and enter information on behalf of the applicant on their account?	Clarify any authentication requirements for applicant references, and whether or not applicant refrences should be issued a separate credential by the CSP. A visual flow of how applicant references should be proofed in conjunction with the applicant's identity proofing process would be ideal.
88	63A	5.2.3.1	26	1056	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. Physical fair evidence also requires a person to obtain copies of such documents, representing a likely source application departures.	- For IAL1, consider removing the requirement for FAIR evidence. 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)
89	63A	5.3.1	26	1049	Does NIST distinguish between behavioral analytics and behavioral biometrics? This distinction is important given the specific requirements that apply to biometrics in this guidance.	Consider differentiating between behavioral analytics and behavioral biometrics in acceptable means to prevent automated attacks on the identity proofing process.
90	63A	5.3.2.1	26	1053	A plain reading of this is that the CSP must collect identity evidence directly from the applicant. However, it is commonplace in the industry to not collect FAIR evidence(e.g., utility bills or phone records) directly from applicants, but rather to infer such evidence by validating PII from the piece of STRONG evidence and certain self-asserted attributes.	Clarify whether evidence must be collected directly from applicants in all cases, or if certain types of evidence may be implicitly collected by running checks on self-asserted attributes during validation.
91	63A	5.3.3	27	1064, 1114	The draft states that the geniuneness of evidence should be validated by "Visual inspection by trained personnel." Genuineness of identity evidence can also be corroborated through non-visual inspection (e.g., tactile features such as raised lettering)	Change to: "Inspection by trained personnel of visible, tactile, or other physical security features."
92	63A	5.3.3	27	1068	The draft states, "The CSP SHALL validate the genuineness of each piece of FAIR evidence by visual inspection by trained personnel." What evidence validation methods could be used for unsupervised remote processes or for digital FAIR evidence where trained personnel may not be involved in inspecting evidence?	Add more options for validating FAIR evidence, especially digital FAIR evidence for unsupervised remote identity verification, as in the STRONG evidence requirements in rev 4 and in rev 3 (Table 5-2 Validating Identity Evidence).
93	63A	5.3.3	27	1070	On line 630, there is an allowance that core attributes can be considered validated if they appear on evidence that is verified, which is not reflected here.	Add: "or that are included on STRONG or SUPERIOR evidence".
94	63A	5.3.4	27	1084	The allowance of an AAL1 account is problematic when combined with the account recovery provision in 63B. The guidance here allows a subscriber to reset a password by repeating only the verification component of identity proofing. This could allow an attacker who compromises a 1FA account to use that password to compromise a MFA credential at IAL1.	Change to: "Demonstrated control of a multifactor digital account associated with the applicant, in accordance with the CSP's Practice Statement (Sec. 5.1.1)"

95	63A	5.4.2	28	1114	The guidance does not stipulate how FAIR evidence is to be evaluated at IAL2, unlike IAL1 (lines 1068-1069).	Add: "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 - confirming the integrity of digital security features"
96	63A	5.4.3	28		Suggest breaking out Validation of Evidence, and Validation of Attributes for both IAL2 like IAL3	Break out validation of evidence and validation of core attributes. These are two actions that are necessary but perform different functions in the flow. for IAL2 & IAL3, it is essential that the evidence is real.
97	63A	5.4.4.1	29	1130	Change "provided" to "validated" Clearly enumerate that the presented evidence has been validated. If a drivers license and a passport is uploaded, and the drivers license is validated, the passport cannot be used for the biometric comparison	Change "provided" to "validated"
98	63A	5.4.4.1	28	1128	The guidance no longer requires return of an enrollment code for remote proofing at IAL2. The return of an enrollment code provides defense against an imposter who has access to genuine identity evidence, especially in the absence of a biometric.	Consider guidance or requirements for use of enrollment codes at IAL2 when addresses (phone, email) are used as core attributes in identity proofing, while maintaining a path for binding an account with a biometric for individuals who don't have a stable phone or address.
99	63A	5.4.4.1	29	1130	The wording in regards to a biometric/facial comparison is slightly different between IAL1 and IAL2: IAL1 (line 1081): "Physical comparison of the applicant's face or biometric comparison of the facial image of the applicant to the facial portrait included on a piece of SUPERIOR or STRONG evidence..." IAL2 (line 1130): "Comparison of a collected biometric characteristic, such as a facial image, to the associated reference biometric contained on a piece of presented SUPERIOR or STRONG evidence" Is this intentional? If so, what is the difference between a "collected" biometric characteristic and a physical comparison? For remote proofing with supervision (video), would CSPs need to collect and store the user's facial image in some way?	Standardize wording across IAL1 and IAL2 if the biometric requirement is the same -- if not the same, clarify intention of the term "collected biometric characteristic" particularly for remote proofing with supervision.
100	63A	5.4.4.1	28	, A_a_IRL , A_a_AL}))	The draft states that the CSP can verify the binding of the applicant by "Demonstrated association with a digital account through an AAL2 authentication or an AAL2 and FAL2 federation protocol." The guidance does not indicate that the account must be associated with the applicant. Additionally, third-party providers such as banks may not conform with AAL2 requirements exactly; these should still be acceptable by the CSP if documented in the CSP.	Change to: "Demonstrated control of a digital account associated with the applicant through an AAL2 authentication protocol or equivalent, in accordance with the CSP's Practice Statement (Sec. 5.1.1)"
101	63A	5.4.4.1	29	1133	Consider account takeover notifications, and: 1) shared signals framework (SSE) 2) CAEP, 3) and RISC.	Consider providing guidance on: CSP or IDPs should be made aware of such a takeover, and should ensure that the associated identity should be minimially reviewed, and potentially revoked, or downgraded. Likewise, that CSP or IDP inform any other CSPs that depend on it for verification or identity services.
102	63A	5.5.3.1	30	1166	In interest of service equity (see comment on line 594), consider a provision for IAL3 that does not require verifying the integrity of cryptographic security features if not present (eg., REAL-ID-compliant identity documents).	Change to: "The CSP SHALL validate the genuiness of each piece of SUPERIOR evidence by: 1. Confirming the integrity of its cryptographic security features and validating any digital signatures, or 2. Confirming the document reference number and core attributes with an authoritative source."
103	63A	6.3.2	35	1270	The draft states, "The CSP SHALL provide the capability for subscribers to change or update the personal information contained in their subscriber account." The document does not provide a mechanism to ensure that subscribers cannot update their core attributes unless those attributes have been verified (example: allowing users to arbitrarily change their SSN or DOB).	Add: "Prior to effectuating any change or update, the CSP SHALL require validation of new core attributes consistent with the requirements for the highest IAL associated with the subscriber account."
104	63A	6.3.2	35	1294	The draft states, "The CSP SHALL delete any personal or sensitive information from the subscriber account records following account termination in accordance with the record retention and disposal requirements." Deletion must also be performed pursuant to the CSP's practice statement.	Add: "and its practice statement (Sec. 5.1.1)"
105	63B	6.1	42	1583	The draft states, "When any new authenticator is bound to a subscriber account, the CSP SHALL ensure that the binding protocol and the protocol for provisioning the associated keys...". Not all authenticators involve keys.	Change "the associated keys" to "any associated keys"
106	63B	6.4	47	1788	The guidance does not include an elective mechanism for a subscriber to remove an authenticator that was previously bound to an account.	Consider adding: "CSPs SHALL allow authenticated subscribers to unbind specific authenticators that were previously bound to the subscriber account, provided that removal would not have the effect of reduce the AAL below the minimum level permitted by the CSP. 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."
107	63B	8.1	55	1945	Consider the risk of insider fraud as a threat against CSP and authenticator operations. For instance, a customer support representative who has access to perform support functions could be bribed to reset a password on behalf of an attacker.	Add: "Fraud risk management manages risks of fraud within the system, including fraud perpetrated by insiders with privileged information and access to CSP functions."
108	63B	10.1	64	2180	The draft states, "Prompt users with adequate time (e.g., 1 hour) to save their work before the fixed periodic reauthentication event required regardless of user activity." The guidance here seems (at least initially) unclear because the terms "fixed periodic" don't appear elsewhere in the draft. The term "periodic" also applies only under certain conditions in the authentication lifecycle. This type of prompt, with the listed lead time, is reasonable to make under many circumstances not described by the guidance.	Expand guidance and remove the reference to the specific event so that the guidance is more clear and covers more situations where this is appropriate. Consider changing to: "Prompt users with adequate time (e.g., 1 hour) to save their work before a reauthentication event if the reauthentication event is required regardless of user activity."
109	63B	4.2.3	9	546	GSA recommends NIST remove most of Section 7.1.* in Volume B, and Section 5.6 in Volume C, related to session management and reauthentication. Applications, users and types of users impact the session management thresholds. Alternatively, if NIST continues to maintain, significant updates should be made to align with modern technology. At a minimum, requiring MFA after 30 minutes of inactivity has proven to be a detrimental user experience including for accessibility, mobile experiences, and public benefits. For example, some users seek to refresh a web-page several times over the course of one day to view the status of an public benefits application. The user is left being prompted excessively for MFA if 30 minutes have passed, and it does not appear that an optional session cookie (e.g., to remember a device) would be permissible in this framework.	Alternatively, if NIST continues to maintain, significant updates should be made to align with modern technology. At a minimum, NIST should consider permitting an optional "remember my device" cookie to allow a user to log in with one factor after 30 minutes of inactivity but before 12 hours have elapsed.
110	63B	5.1.1.2			While complexity has been removed; password length requirements remain at 8 characters resulting in disparate policies across the federal civilian executive branch, some at 8 characters, some at 12, FedRAMP at 14, some at 16. This could prove frustrating for share services solutions. Recommend revisiting.	Revisit the minimum 8 character password threshold and consider allowance of complexity for privileged/system accounts.

111	63B	5.1.1.2			Removal of complexity requirements is not tied to bad password checking capabilities; this has resulted in users being able to set the very weak passwords we aim to avoid ..e.g., passwordpassword. While not everyone will knowing set weak passwords, it has put the onus on security programs to kickstart password stregnth testing programs to seek them out and force change. Recommend action to work with Industry (most notably Microsoft) to build into it systems a bad password checking capability or facilitate development of marketplace solutions that easily integrate with MS AD.	Work with Industry to build in bad pw checking capability natively.
112	63B	5.1.3.1	21	859	Suggest removing statements or language that is too qualitative for a requirement statement. For example, the use of typically - "Email....and is typically accessed using only a memorized secret.". Incorporating qualitative language in a normative section and a normative requirement statement (i.e. "shall not") leads to confusion and unnecessary interpretations. For example, by the statement on line 859: If we have multi-factor on our email and can prove possession of a specific device - then we CAN use email for delivery of out-of-band authentication.	Clarify language throughout. For example, by the statement on line 859: If we have multi-factor on our email and can prove possession of a specific device - then we CAN use email for delivery of out-of-band authentication.
113	63B	5.1.3.1	21	859	Does NIST have a source that email is still "typically" accessed using only a memorized secret, given the push for MFA by many major providers in recent years? Also, consider "accessible" instead of "accessed", since email is often accessed through long-lived sessions rather than by entering a password.	Consider citing or change "typically" to "often". Change "accessed" to "accessible".
114	63B	5.1.3.1	21	870	The draft states, "If a secret is sent by the verifier to the out-of-band device, the device SHOULD NOT display the authentication secret while it is locked by the owner." Whether the device displays the authentication secret while locked may not be under the verifier's control.	Add: "To the extent practical, if a secret is sent..."
115	63B	5.1.3.2	22	793, 903, 1529	Other parts of the specification use language like "6 decimal digits (approximately 20 bits of entropy)". 6 decimal digits is not strictly sufficient to meet 20 bits of entropy. "20 bits or 6 decimal digits of entropy" would also be appropriate here and help with consistency.	Change to: "20 bits or 6 decimal digits of entropy" for accuracy and consistency elsewhere in the spec.
116	63B	5.2.10	38	1463	Language confusion, unclear if the Organization is the CSP or the RP.	Consider changing "organization" to "RP" to clarify the actor who is responsible for determining the acceptable level of risk for their systems.
117	63B	5.2.2	31	1233	How does a subscriber who is locked out as a result of rate limiting regain access? The guidance does not provide recourse for a person who has had 100 authentication attempts to regain control of the credential. (As an example - the subscriber might need to contact CSP's support, or the suspension might lift automatically after a given period of time elapses.)	Add: "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 mechanism to circumvent rate limiting." Or change "subscriber account" to "single secret" - see comment on line 907.
118	63B	5.2.2	32	1249	The draft states, "When the subscriber successfully authenticates, the verifier SHOULD disregard any previous failed attempts for that user from the same IP address." 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?	Consider clarifying how a verifier should disregard previous failed attempts for a user from the same IP address.
119	63B	5.3.1.2	16	729	63A requires automated attack prevention, but 63B does not. Given the requirement to implement a rate limiting mechanism, should authentication have language similar to Section 5.4.1 in 63A?	Add (paraphrased from 63A, Section 5.4.1): "Verifiers SHOULD implement a means to prevent automated attacks on the verification process. Acceptable means include, but are not limited to: bot detection, mitigation, and management solutions; behavioral analytics; web application firewall settings; and traffic analysis."
120	63B	6.1..1	42	1602	The term "primary authenticator" is used here for the first time. Until this point, authenticators in a MFA scheme are considered co-equal. Which authenticator does NIST consider to be "primary", and what are the implications (if any) of an authenticator being so designated?	Define the term "primary authenticator" or change "the subscriber's primary authenticator" to "a subscriber's authenticator"
121	63B	6.1.2.3			GSA recommends removing or revisiting the proposed requirements related to account recovery and subscriber accounts that have not been identity proofed (i.e. "without IAL"). Abandoning an account and having a subscriber establish a new account is not feasible at scale or possibly necessary for the use cases, risks and impacts. Since CSPs are currently defined to include standalone applications, including commonly used commercially sourced services for low or no risk use cases where anonymity is preferred by consumers, abandoning an account may increase frustration, decrease usability, and impede accessibility for a broad consumer base. GSA agrees that for subscribers that have been identity proofed, the commonly used account recovery procedures for public applications are not ideal. For the higher risk use cases, the account recovery processes defined in 6.1.2.3 should be updated to more clearly trace to the risks and impacts.	Recommend removing or revisiting the proposed requirements related to account recovery and subscriber accounts that have not been identity proofed (i.e. "without IAL"). For the higher risk use cases, the account recovery processes defined in 6.1.2.3 should be updated to more clearly trace to the risks and impacts.
122	63B	6.1.2.3			Suggest revisiting 6.1.2.3 in entirety. We agree the account recovery process is challenging. However, the options presented in Section 6.1.2.3 are too restrictive; may not scale; and should focus on the risk and patterns to prevent versus a prescriptive set of requirements. For example, the description of replacement of memorized secrets only provides options that include: Biometric, or Two physical authenticators In addition, for the subscriber accounts without IAL- abandoning the account is stated as the only option.	Suggest revisiting 6.1.2.3 in entirety and providing data driven, scalable options for agencies to consider.
123	63B	6.1.2.3	43	1659	Repeating only the verification portion of IdP is potentially problematic for IAL1, when a subscriber could perform verification using an AAL1 credential. A bad actor who has compromised an acceptable IAL1 credential (e.g., from a genuine subscriber's bank) could claim a loss of authenticators and successfully complete verification using the stolen password. This would defeat MFA.	Require return of an enrollment code at IAL1 and above for verification as discussed in other comments. This will limit the ability of an attacker who has control of an acceptable digital account to use that access to usurp an IAL/IAL2 account.
124	63B	6.1.2.3	43	1667,1678	Consider requiring a notification as added assurance that the person who recovered their account is the owner of the claimed account, following account recovery and binding a new memorized secret. See 63A, 5.1.7.	Consider including: ""When a CSP binds a new memorized secret as described in this section, the CSP SHALL send a notification to the subscriber. The notification SHALL provide clear instructions, including contact information, in the case the recipient repudiates the account recovery event."
125	63B	6.1.2.3	44	1673	In addition to the case of a forgotten password, is this 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.")	Change "(i.e., forgotten)" to "(e.g., forgotten or compromised)"
126	63B	6.1.2.3	44	1678	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 misentered.	"at least 6 random alphanumeric characters" -> "at least 20 bits or 6 decimal digits of entropy".
127	63B	6.1.2.3	44	1678	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.	Provide consistency between Section 6.1.2.3 and 63A Section 5.1.6. Change to: "The confirmation code SHALL conform to the same requirements as the enrollment code (800-63A, Section 5.1.6), and CSPs SHALL apply rate throttling to verification of confirmation codes (Section 5.2.2)."

128	63B	6.1.2.3	44	1678	The requirement for two physical authenticators adds a significant usability cost that will prevent successful recovery in this extremely common use case. GSA recommends that NIST review the definition of physical authenticators in Section 4.2.1 and develop a more robust set of requirements that represent equitable and accessible options for common use cases at low or no risk transactions.	Options: 1) Consider a confirmation code to a known address in conjunction with one additional physical authenticator to be sufficient to invoke the password reset process for AAL1 and AAL2. 2) Change ""two physical authentictors" to "one physical authenticator" 3) Perform research on common use cases and revisit the risk and impacts.
129	63B	6.1.2.3	44	1682	800-63A rev4 has reduced enrollment codes to 6 random numeric digits. Can confirmation codes for account recovery in 63B match?	Change to: "6 random numeric characters"
130	63B	6.1.3	44	1746	The draft states, "In situations where the authenticator strength is not self-evident (e.g., between single-factor and multi-factor authenticators of a given type), the CSP SHALL assume the use of the weaker authenticator unless it is able to establish that the stronger authenticator is in fact being used (e.g., by verification with the issuer or manufacturer of the authenticator)." This represents a point-in-time assurance, but would not in itself prevent the subscriber from later reverting to a weaker authenticator.	Change "able to establish that the stronger authenticator is in fact being used" to "able to establish confidence that the stronger authenticator is in continuous use and that reverting to a weaker authenticator will invalidate the binding."
131	63B	Overall			Volume 800-63B has some inconsistent language in informative sections which impacts how the standards are applied, including to standalone applications versus components of a federated identity system. Abstract: "The result of the authentication process may be used **locally by the system performing the authentication** or may be asserted elsewhere in a federated identity system" Purpose: "This document, SP 800-63B, provides requirements to credential service providers (CSPs) for remote user authentication..." Most requirements in normative sections are written for CSPs. GSA recommends NIST clarify clarify the definition of a CSP and clearly state that a CSP can be a standalone application. Conversely, review and clarify requirements in normative sections for applicability to standalone applications versus CSPs. As an example, review the account recovery sub-section. When reviewing, replace "CSP" with "IDP" or "application". Then determine if the requirements still apply; or clarify.	GSA recommends NIST clarify clarify the definition of a CSP and clearly state that a CSP can be a standalone application. Conversely, review and clarify requirements in normative sections for applicability to standalone applications versus CSPs. As an example, review the account recovery sub-section. When reviewing, replace "CSP" with "IDP" or "application". Then determine if the requirements still apply; or clarify.
132	63C	4.2	8	498	The draft states for FAL2: "If front channel presentation is used as discussed in Sec. 7.2, additional injection protections SHALL be implemented by the RP." Section 7.2 does not specify which injection protections are required, which creates ambiguity in how a CSP might meet FAL2.	
133	63C	5.1	13	13	This section on trust agreements should be removed or made informative. Example: "Establishment of a trust agreement is required for all federation transactions, even those in which the IdP and RP have a shared security domain or shared legal ownership. In such cases, the establishment of the trust agreement is an internal process that can be completed quickly." A trust agreement where the IDP and RP have a shared legal ownership is a common implementation for enterprise use cases leveraging federated protocols and implementations. In this scenario, the need for a separate or distinct and ambiguous trust agreement is superceded by enterprise risk management, organizational policies, security controls, interconnection agreements, and / or delegations of authority already present in other required items for a federal organization. Inclusion of a trust agreement as a "required" clause in Section 5.1 introduces additional unnecessary burden.	
134	63C	12.2			Throughout all four volumes of 800-63-4 draft, the volumes and sections switch context for the types of networks and use cases in scope. For example, "remote", "Internet", and "security domain". The inclusion of Kerberos further complicates the C volume and it's relationship to the base, volume a and volume b. The document doesn't explain that kerberos uses non-web based protocols and thus has different networking assumptions. Given a broader push to modernize federation protocols, it may be beneficial to reduce the section on kerberos or discuss some of the limitatons of kerberos given its reliance on non-web ports/protocols.	Given a broader push to modernize federation protocols, it may be beneficial to discuss some of the limitatons of kerberos given its reliance on non-web ports/protocols and sometimes use of obsolete cryptography.
135	63C	5.1.2	15		Recommend that multi-lateral trust agreements include if the attributes are validated, unvalidated or derived.	the set of attributes, and their validation status the idP can make available to the RP
136	63C	5.6			GSA recommends simplifying and clarifying the distinctions between CSP (Volume B) and IDP (Volume C). There are overlapping sections and requirements for Reauthentication and Session Requirements. GSA applauds the attempt in separating Volume B and Volume C requirements. Volume C attempts to explain a few versions of the styles of approaches to identity federation frameworks. However, the attempt is possibly introducing more confusion for implementing controls for a CSP that is also an IDP. For example, Volume C Section 5.6 references "See [SP800-63B], Sec. 7 for more information about session management requirements for both IdPs and RPs". However, there are conflicting requirements. Similar to Volume B Section 7.1.*; GSA recommends removing the Volume C Section 5.6 Reauthentication and Session Requirements or moving this sub-section to a Informative only section.	Similar to Volume B Section 7.1.*; GSA recommends removing the Volume C Section 5.6 Reauthentication and Session Requirements or moving this sub-section to a Informative only section.