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

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

Organization:	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**
	63A	2.1.2	8	578	The draft defines Process Assistants here, but provides little to no requirements or guidance on their use, training, or informational needs in section 3.	Consider adding normative requirements around what information and/or training must be made available to Process Assistants, especially in the context of Process Assistants provided by CSPs.
	63A	2.1.2	8	583-584	GSA suggests NIST clarify whether CSPs must provide the training and support resources on its own, or if it may require and confirm that such training and support is provided (for example, requiring such training in a contract or agreement with a third-party service provider).	Change "SHALL provide training..." to "SHALL provide training and support resources, or ensure such training and resources are provided, consistent with the...".
	63A	2.1.3	8	611	The draft states that "CSPs that offer IAL1 & IAL2 services SHALL provide a Remote Unattended identity proofing process and SHALL offer at-least one attended identity proofing process option. CSPs that offer IAL1 & IAL2 services SHOULD support identity proofing processes that allow for the applicant to transition between proofing types in the event an applicant is unsuccessful with one type (e.g., allow an applicant who fails remote unattended to transition to remote attended)." It is unclear whether CSPs are required to provide an attended proofing process that covers all aspects of the identity proofing process (as described earlier in this section), or if a hybrid process (as described later in the draft) suffices as the required alternative option. GSA strongly recommends that CSPs to have flexibility in meeting this requirement through hybrid processes instead of conducting the entire process in the presence of a proofing agent. For example, CSPs may opt to collect and validate evidence (identity resolution) through unattended review prior to a video session, and CSPs offering in-person proofing may need to collect and validate self-asserted attributes (either via unattended or attended processes) prior to the onsite attended session.	On line 596, change "...resolution, validation, and verification steps..." to "...resolution, validation, or verification steps..." On line 604-605, change "...completes the entire identity proofing process - to include resolution, validation, and verification..." to "...completes resolution, validation, or verification steps..." On line 611, change "CSPs that offer IAL1 & IAL2 services SHALL provide a Remote Unattended identity proofing process and SHALL offer at-least one attended identity proofing process option." to "CSPs that offer IAL1 & IAL2 services SHALL provide a Remote Unattended identity proofing process and SHALL offer at-least one partially attended identity proofing process option."
	63A	2.4.1.1	11	681	The draft's Fair Evidence Requirements state that "the information on the evidence is able to be validated by an authoritative or credible source." Some information on valid FAIR evidence (i.e. a student ID number on a student ID) may not be able to be validated by an authoritative or credible source, or necessary to accomplish identity proofing. Section 4.1.5 requires that core attributes be validated, not all attributes.	Change "The information on the evidence is" to "The core attributes on the evidence are"
	63A	2.4.1.1	11	683	This line uses the word "verified" but points to Sec. 2.4.2.2, Evidence Validation Methods.	Change "verified" to "validated" to match linked section and STRONG evidence requirements.
	63A	2.4.1.1	11	676, 679-680	GSA suggests clarification on whether a evidence must contain 1) the name of the claimed identity or 2) physical or digital security features. In practice, CSPs have used self-asserted and validated phone numbers as "FAIR" evidence.	Clearly state whether it is possible for self-asserted information - such as a phone number - to meet these FAIR evidence criteria despite that information not containing a name or physical/digital security features.
	63A	2.4.1.2	11	703	validated by an authoritative or credible source." Some information on valid STRONG evidence may not be current (i.e. physical address) and some information may not be necessary to accomplish identity proofing (i.e. gender, physical characteristics). Section 4.1.5 requires that core attributes be validated,	Change "The information on the evidence is" to "The core attributes on the evidence are"
	63A	2.4.1.3	12	731	This line uses the word "verified" but points to Sec. 2.4.2.2, Evidence Validation Methods.	Change "verified" to "validated" to match linked section and STRONG evidence requirements.
	63A	2.4.2.2	13	749	The use of the word "include" implies that there are additional methods that MAY be used to validate evidence.	Add additional evidence validation methods that are acceptable, if any.
	63A	3.1.1	16	848-850	If a CSP does not offer an alternative identity proofing flow for applicants without the required identity evidence (e.g., without Drivers Licenses), may it meet this practice statement criteria by simply stating that there is no alternative?	Change to "Alternative processes, if any, for the CSP to complete..."
	63A	3.1.1	17	852-854	This sentence seems to unintentionally expand upon the definition of "core attributes" by adding in in the list after "Core attributes include".	Change sentence to "CSPs should include the core attributes, as well as any additional attributes that the CSP collects for purposes of fraud mitigation, complying with laws or legal process, or conveying to relying parties (RPs) through attribute assertions."
	63A	3.1.11	28	1264	The draft states that CSPs SHALL "expeditiously" provide redress in situations where disparate negative impacts occur for different demographic groups and does not provide criteria on how to meet the requirement of "expeditiously". In order for RPs to compare the services of CSPs fairly, more guidance is required.	Consider adding specific requirements/guidance on redress timelines similar to guidance issued for handling data breaches (i.e., disclosure w/in X days, mitigation, long-term solution implementation, and communication of resolution.)
	63A	3.1.11	28	1249	The draft states that CSPs SHALL meet the following minimum performance thresholds for biometric usage in verification scenarios: False match rate: 1:10,000 or better; and False non-match rate: 1:100 or better. Using total rates leaves potential to over index marginalized groups while maintaining the minimum standard required. The same section (line 1259) separately states "CSPs SHALL employ biometric technologies that provide similar performance characteristics for applicants of different demographic groups (age, race, sex, etc.)"	Consider combining the two requirements or adding context to the minimum performance standards to include standard performance across demographic groups.
	63A	3.1.11	27	1219	Do the requirements for biometrics apply when it is only behavioral characteristics (typing cadence, mouse movements) monitored to differentiate between a human and a non-human as a fraud prevention measure?	Clarify whether the "use of biometrics" only applies to fraud detection when used to identify a specific individual, or if it also applies to the mere monitoring of behavioral characteristics todistinguish between human and non-human applicants.

	63A	3.1.12	29	1295	The draft states that "CSPs SHALL implement live capture of documents during the validation process." GSA supports the best practice of using live capture for document validation, but has concerns around a shift to SHALL due to: (1) accessibility and the (2) effectiveness of control (2) Accessibility: As the technology around document authentication under real world conditions is still developing, document authentication can be a friction point for legitimate users. This requirement will essentially require a user to have a smartphone to complete remote identity proofing, since it is difficult to take acceptable photos of an ID using a desktop computer. The requirement places a disproportionate burden on users who do not have smartphones (for example, users who access the internet and digital services at the library). (3) Effectiveness: It is also unclear whether this requirement would actually meaningfully improve security, as bad actors can connect a virtual camera to feed in images, and whether "live capture" refers to photos taken in real-time or videos.	Change SHALL to SHOULD.
	63A	3.1.13.1	32	1364	The CSP SHALL provide notification to the public about trusted referee services, but no language is included to specify how an Applicant may determine and verify that a Trusted Referee is associated and/or certified with the CSP. This is key to 1) preventing malicious actors from defrauding users and 2) building trust with RPs and the public.	Add requirements or guidance on what agent-specific information must be disclosed, when that information must be shared, and where that information can be accessed by the applicant.
	63A	3.1.13.1	32	1368	The draft states that the CSP "SHALL train and certify its trusted referees" and conduct "annual recertification". But no there is no language that defines what constitutes certification or how that certification should be verified. The lack of guidance will create a wild west of "certification" standards and make it difficult for RPs to accurately compare trusted referee services across CSPs.	Add requirements for documenting and verifying a trusted referee's certification.
	63A	3.1.13.1	32	1380	The draft states that the CSP SHALL record any proofing session involving a trusted referee, but does not require any information about the trusted referee to be included in the record. Without this information, conducting trust-preserving fraud investigations involving a trusted referee will be difficult.	Add a requirement to include at least the verifiable identifier and provider of the trusted referee within the record of the proofing session.
	63A	3.1.13.2	33	1400	The draft states that "CSPs SHOULD offer trusted referee services for failures in completing automated validation processes", but lists three requirements below it (a-d). It is unclear if these are always required, or if they are only required in the event that the CSP offers trusted referee services for failures such as mismatched core attributes or the absence of an applicant in a record source.	Add: "If trusted referee services are offered for failures in completing automated validation processes, the following requirements apply:", followed by the list of conditional requirements (a-d).
	63A	3.1.13.3	33	1419	The draft states that "The following requirements apply to the use of applicant references at IAL1 or IAL2:", and lists five requirements below it (1-5). It is unclear if these are always required, or if they are only required in the event that the CSP offers applicant references.	Change "The following requirements apply to the user of applicant references at IAL1 and IAL2:" to "If applicant references are offered at IAL1 or IAL2, the following requirements apply:", followed by the list of conditional requirements (1-5).
	63A	3.1.13.5	34	1461	This section's requirements apply "where such steps are deemed necessary by a risk assessment", suggesting that requesting evidence of an applicant reference's relationship to the applicant is not required. This could be more clear with the addition of a MAY statement in this section.	Change "In many cases, there will be business, legal, or fraud prevention reasons to confirm the relationship between the applicant and an applicant reference. Where such steps are deemed necessary by a risk assessment, the following requirements SHALL apply:" to "The CSP MAY confirm the relationship between the applicant and an applicant reference for business, legal, or fraud prevention reasons. If such steps are deemed necessary, the following requirements apply:"
	63A	3.1.13.6	35	1475	"Minors" is not defined. Is it any person under the age of 18?	Add a definition of "minor" in Appendix A, or define it here in a sentence: "A minor is a person under the age of 18."
	63A	3.1.2.1	19	932	The draft states that CSPs MAY use KBV as part of its fraud management program. This contradicts the requirement of disallowing the use of KBV during initial identity verification, which may introduce confusion amongst implementers and lead to gaps in implementation.	Consider changing this requirement to "SHALL NOT" for Federal CSPs and RPs.
	63A	3.1.2.1	18	901	The draft states that CSPs SHALL conduct a date of death check against a credible authoritative source. However, many sources of date of death flags contain inaccuracies or outdated data which may falsely flag users as deceased or fail to flag use of a deceased identity.	Consider replacing SHALL with SHOULD.
	63A	3.1.2.1	19	936-938	GSA suggests NIST clarify whether CSPs must provide the training and tools on its own, or if it may require and confirm that such training and tools are provided (for example, requiring such training and tools in a contract or agreement with a third-party service provider).	Change to "For attended proofing processes, CSPs SHALL train proofing agents to detect indicators of fraud and SHALL provide proofing agents and trusted referees with tools to flag suspected fraudulent events for further treatment and investigation, or must otherwise ensure that such training and tools are provided."
	63A	3.1.3.2	35	1033-1035	GSA suggests NIST clarify whether CSPs must provide the privacy training on its own, or if it may require and confirm that such training is provided (for example, requiring such training in a contract or agreement with a third-party service provider).	Change to "The CSP SHALL provide privacy training, or ensure that it is provided, to all personnel and any third-party service providers who have access to sensitive information associated with the CSP’s identity service.
	63A	3.1.3.2	22	1041-1042	GSA suggests even further clarification of whether an SSN is sufficient to act as identity evidence, even when it undergoes substantial validation in combination with other identity attributes from other evidence.	If SSN is in no circumstances acceptable as FAIR evidnece, state, "Knowledge of an SSN, regardless of any subsequent validation or verification conducted on the SSN, is not sufficient to act as evidence of identity nor is it considered an acceptable method..."
	63A	4.1.6	37	1549	Table A.1, Fair Evidence Examples lists Credit or Debit Card, Snap Card, or Social Security Card as FAIR evidence, but also says that they "must be presented with other evidence containing a photo." It is unclear how to verify ownership of a form of FAIR evidence that does not have a photo or address from the processes listed in 4.1.6 Verification Requirements.	If physical FAIR evidence without a photo or address (credit or debit card, Snap card, or Social Security card) is acceptable evidence to verify at IAL1, then outline a verification process for those forms of evidence.
	63A	4.2.2	41	1666	The new IAL2 requires CSPs to collect one piece of FAIR evidence and one piece of STRONG evidence (if the applicant does not have SUPERIOR evidence, like a passport). For CSPs that serve the general population, STRONG evidence (i.e. a driver's license) is the most common form of ID. If the CSP cannot verify a phone or connect to a financial account for an applicant in addition to their STRONG evidence (driver's license), then the applicant would need to provide a second form of physical FAIR evidence to verify at IAL2. Given the new requirements to verify ownership of FAIR evidence in 4.2.6.1, the applicant's only options are a second photo ID or a second ID that contains an address. Examples of eligible photo IDs listed in the Appendix -- corporate IDs, student IDs, Veteran Health IDs -- serve specific audiences and are not widely available. These additional FAIR evidence requirements may be too high a burden, as many legitimate applicants in the general population will only have one photo ID.	Ensure that more common physical FAIR evidence types (credit or debit card, Snap card, or Social Security card) are accepted at IAL2. Allow applicants to provide physical FAIR evidence without a photo or address -- or given the difficulty verifying ownership of some forms of FAIR evidence, require verification for only the strongest form of evidence. See other comments on sections 4.1.6, 4.2.6.1, and Appendix. Alternatively, consider "1 piece of SUPERIOR or STRONG evidence, or 2 pieces of FAIR evidence" to meet IAL2 verification.

	63A	4.2.6.1	42	1716	Table A.1, Fair Evidence Examples lists Credit or Debit Card, Snap Card, or Social Security Card as FAIR evidence, but also says that they "must be presented with other evidence containing a photo." It is unclear how to verify ownership of a form of FAIR evidence that does not have a photo or address from the processes listed in 4.2.6.1.	Add a requirement that allows applicants to provide physical FAIR evidence without a photo or address as their second form of evidence. Suggestion: "(c) If the FAIR evidence has neither a validated address nor a facial portrait, then confirm that the FAIR evidence is valid (according to 4.2.4) and that the core attributes on the FAIR evidence match the core attributes on the applicant's STRONG or SUPERIOR evidence." Alternatively, given the difficulty verifying ownership of some forms of FAIR evidence, verification pathways could be required for only the strongest form of evidence.
	63A	4.4	49	1920	Table 1 lists the requirements for each IAL. Section 4.1.4 and section 4.2.4 state that each piece of evidence shall be validated with one of the techniques listed in the table. Using "or" statements will be helpful here to clarify that only one of the listed validation techniques is needed for validating each piece of FAIR and STRONG evidence at IAL1 and IAL2.	Add: "or" between evidence validation list items when applicable.
	63A	4.4	49	1920	Table 1, Evidence Validation lists automated doc auth and visual inspection as methods for validating physical evidence. It should also include "- physical/tactile inspection" to match Section 4.1.4, Evidence Validation (at IAL1).	Add: "- physical/tactile inspection" to physical evidence validation list items.
	63A	4.4	49	1920	Table 1, Attribute Validation lists the methods for validating attributes. Using "or" statements will be helpful here to clarify that only one of the listed techniques is required for validating attributes at IAL2 and IAL3, depending on the evidence strength.	Change: "Confirmation of core attributes against authoritative or credible sources. Confirmation of digitally signed attributes through signature verification." to "FAIR and STRONG evidence: Confirmation of core attributes against authoritative or credible sources, or SUPERIOR evidence: Confirmation of digitally signed attributes through signature verification."
	63A	6	53	1991	The draft states there are three categories of threats to the identity proofing process including Impersonation, False or Fraudulent Representation, and Infrastructure. Scams or Social Engineering are a seperate and distinct threat to the identity proofing process not covered under the three categories outlined.	Consider adding Scams/Social Engineering as a distinct 4th category of threat where an attacker misleads or manipulates an individual to verify an identity on an account on the CSP's platform that the attacker controls.
	63A	8.2	63	2266	The guidance suggests to provide users with "... Information on whether the user's enrollment session will be in-person or in-person over remote channels, and whether a user can choose." Suggest clarifying this to "over in-person or remote channels".	Change "in-person or in-person over remote channels" to "over in-person or remote channels".
	63A	A.1	79	2728	Table A.1, Fair Evidence Examples lists Veteran Health ID Card as a form of FAIR evidence, but it is also included in Table A.2 Strong Evidence Examples. If the Veteran Health ID Card qualifies as STRONG evidence, it should not be listed in the FAIR evidence table.	Remove "Veteran Health ID Card" option from FAIR evidence table and keep in STRONG evidence table.
	63A	A.1	79	2728	Table A.1, Fair Evidence Examples lists credit or debit card, Snap card, or Social Security card as FAIR evidence, but also says that they "must be presented with other evidence containing a photo." It is unclear how to verify the ownership of these forms of evidence, because "physical or visual inspection of the card" is not one of the verification methods listed in Sections 4.1.6 (for IAL1) and 4.2.6.1 (for IAL2). It is then also unclear what the user benefit is to providing these cards if additional form(s) of evidence are still required.	Create a path in the normative requirements (Sections 4.1.6 and 4.2.6.1) to verify physical FAIR evidence without a photo at IAL1 and IAL2 (i.e. by comparing attributes on the FAIR evidence to stronger evidence), or require verification of ownership of the strongest form of evidence, allowing for physical FAIR evidence without a photo as secondary documents. Remove "must be presented with other evidence containing a photo" from the FAIR evidence table or clarify how this works in the normative requirements.
	63A	A.1 Fair Evidence Ex	78	2728	The "Financial Account" Verification example states "User input of a micro deposit event of sufficient entropy" but it is not clear where that entropy requirement is described.	
	63B	4.6	47	1840 - 1860	Mandatory notifications could be problematic, especially without delivery guarantee. Maintaining currency of addresses through regular validation needs to be considered. If official agency addresses are preferred, then responsibility can be placed on agencies but the language in 63B should more clearly address these or call for support rather.	
	63B	3.1.2.1	16	823	In describing that look-up secrets should be shared securely with subscribers, a few examples are provided, including "via a session authenticated by the subscriber at AAL2 or higher". It is unclear whether this is stating that, if shared online, look up secrets must be bound during a session authenticated by the subscriber at AAL2 or higher. Please clarify whether the level of "AAL2 or higher" is a requirement.	If not a requirement, remove "at AAL2 or higher". If a requirement, clarify in the following paragraph.
	63B	3.1.7.4	28	1193	In the guidelines, syncable authenticators seem to be permitted as either single-factor or multifactor, but the overview of syncable authenticators references multifactor cryptographic authenticators, which may confuse readers and assessors as to whether the requirements also allow for single-factor syncable authenticators. "Some multifactor cryptographic authenticators allow the subscriber to copy (clone) the authentication secret to additional devices..."	Remove the word "multifactor" in this sentence.
	63B	3.2.10	36	1473	This requirement may be difficult or impossible to prove as it is determined by the provider/manufacturer of the authenticators. Even if most providers/manufacturers of a particular kind	Change SHALL to SHOULD.
	63B	3.2.2	28	1216	GSA suggests clarification on what the CSP should do once the 100 rate limit is reached. Should the account be suspended for a certain duration? Should the authenticator rate limit never be reset until a certain event, such as redress?	Add a sentence to the end of this paragraph explaining what action must occur after the claimant reaches 100 unsuccessful consecutive attempts of a certain authentication method.
	63B	3.2.5.1 and 3.2.5.2	33		GSA agrees with the inclusion of the descriptions for Channel Binding and Verifier Name Binding. The addition of Sections 3.2.5.1 and 3.2.5.2, with examples, helps clarify the terms and the implementation models for federal agencies.	No change.
	63B	4.2	42	1692	The overview section states, "Since account recovery is rarely expected to be invoked..." Resetting a password is fairly common, and the guidelines elsewhere treat resetting a password differently from using other authenticators (sec 4.2.2.3): "One notable exception is a password that has been forgotten without other indications of having been compromised, such as having been obtained by an attacker." Please clarify if the account recovery requirements apply to recovering solely a lost/forgotten passwords as well as recovering other types of authenticators.	If resetting passwords is not subject to the requirements in 4.2, add clarifying content saying such. Otherwise, rephrase the "rarely expected to be invoked" phrase to account for the fact that password reset is fairly common.
	63B	4.6	47	1850	The section on Account Notifications requires supporting "at least two notification addresses per subscriber account, and at least one SHALL be validated during the identity proofing process..." This guidance does not account for subscribers who do not undergo identity proofing, and the rationale for why two addresses are needed is unclear given other requirements around account recovery.	Add content speaking to the rationale for requiring multiple notification addresses, and clarify what requirements apply to subscribers who do not go through identity proofing (authentication-only subscribers).
	63B	Appendix B	87	2900	This requirement may be difficult or impossible to prove as it is determined by passkey providers and attestation is not available. Even though most passkey providers do meet this guidance, if a CSP is held to a strict interpretation of this requirement (e.g. during an assessment) it may be unable to prove that it meets it and may be deterred from offering passkeys.	Change SHALL to SHOULD: 2900 Private keys stored in cloud-based accounts ~~SHALL~~ SHOULD be protected by access control 2901 mechanisms such that only the authenticated user can access their private keys in 2902 the sync fabric.

	63B	Appendix B	87	2903	This requirement may be difficult or impossible to prove as it is determined by passkey providers and attestation is not available. Even though most passkey providers do meet this guidance, if a CSP is held to a strict interpretation of this requirement (e.g. during an assessment) it may be unable to prove that it meets it and may be deterred from offering passkeys.	Change SHALL to SHOULD: 2903 User access to private keys in the sync fabric ~~SHALL~~ SHOULD be protected by AAL2- 2904 equivalent MFA to preserve the integrity of the authentication protocols using the 2905 synced keys.
	63B	Appendix B	88	2912 - 2915	For the federal enterprise passkeys requirements: Because of the variety of platforms and lack of support in many agencies, the MDM requirement should be a "should".	Change SHALL to SHOULD: 2912 Devices (e.g., mobile phones, laptops, tablets) that generate, store, and sync 2913 authenticators containing federal enterprise private keys ~~SHALL~~ SHOULD be protected by 2914 mobile device management software or other device configuration controls that 2915 prevent the syncing or sharing of keys to unauthorized devices or sync fabrics.
	63C	2.1	4	503-507	GSA suggests NIST removes the requirement that RPs (relying parties) shall employ appropriately tailored security controls from the MODERATE baseline security controls. GSA and other federal agencies have digital services assessed at LOW for baseline security controls; and these digital services are integrated with IdPs.	Strike "and RPs" from: 503 IdPs ~~and RPs~~ SHALL employ appropriately tailored security controls from the moderate 504 baseline security controls defined in [SP800-53] or an equivalent federal (e.g., 505 [FEDRAMP]) or industry standard that the organization has determined for the 506 information systems, applications, and online services that these guidelines are used 507 to protect.
	63C	3.10		1286-1292	GSA suggests NIST removes the requirement that RPs (relying parties) shall employ appropriately tailored security controls from the MODERATE baseline security controls. GSA and other federal agencies have digital services assessed at LOW for baseline security controls; and these digital services are integrated with IdPs.	Strike the "and RP" from: 1287 The IdP ~~and RP~~ SHALL employ appropriately tailored security controls from the 1288 moderate baseline security controls defined in [SP800-53] or equivalent federal 1289 (e.g., [FEDRAMP]) or industry standard that the organization has determined for the 1290 information systems, applications, and online services that these guidelines are used 1291 to protect.
	63C	3.10.1. Protection from Injection Attacks		1293-1336	GSA agrees with the Injection Attack recommendations. The addition of the common best practices are warranted including the recommendation to prohibit IdP initiated transactions. This section is a good addition.	None.
	63C	3.3.1.1	15	843	The draft states when "PPIs are used alongside identifying attributes, privacy policies SHALL be established to prevent correlation of subscriber data[...]". It is unclear to which federation member(s) the requirement applies. If it only applies to the IdP, it would be very difficult to maintain subscribers' privacy and prevent RPs from tracking them across services, especially given how the account resolution process is defined in 3.7.2. Additionally, the use of the term "policies" instead of "controls" or "measures" implies that this a privacy practice in name only.	Please clarify if this applies only to the IdP or all of members of the federation and consider having the requirement apply to all members. Additionally, consider changing "privacy policies" to "privacy controls".
	63C	3.4	17	897	On the role of authoritative and credible sources in the context of federation trust agreements and the goal of process transparency: The draft states “the trust agreement SHALL disclose details of the proofing process used at the CSP, including any compensating controls and handling exceptions” and it "SHALL be made available to subscribers upon request" (Sect. 4.3.1, p.47, L1807). The proofing process may involve transmitting evidence digitally to an Authoritative or Credible Source or a 3rd Party service that handles discrete portions of the proofing process (no name for this type of actor), which may or may not function within the same security domain or legal context as the CSP, in order to confirm the supplied evidence's veracity and the attributes being asserted against that evidence. However, none of these actors: Authoritative Source, Credible Source, Issuing Source, undefined 3rd Party service — are described as participating in the federation since the CSP is “no longer an active participant in the federation process” (Section 4.1, p.43, L1724) once the IdP provisions the subscriber account. Yet, the IdP must disclose these non-federation actors’ processes as part of the trust agreement, which may be difficult or impossible, especially if they operate externally and independently of the CSP. This ambiguity in how the IdP should detail the CSP’s (and its supporting actors') processes within the strictures of the trust agreement suggests more refinement is needed within the draft on the expectations and requirements of these “non-federation” actors within the federation context and their inclusion within the trust agreement document.	Consider either: 1) concretely defining the role(s) and requirements of authoritative, credible, and issuing sources within the context of the federation and how the IdP should disclose these various “trust agreements” to the subscriber. Additionally define terminology and assessment criteria for 3rd party services that may be contracted to handle pieces of the identity proofing workflow. or 2) limit the disclosure requirement to only those steps within the proofing process the IdP and/or CSP directly controls.
	63C	3.5.3	23	1085	Software and device attestations SHALL be verified when required by the "trust agreement or [...] federated protocol" request. However, given the limited and variable implementation of attestation, RPs may be setting themselves up for unrecoverable failure if this is demanded in situations where it is not required.	Consider adding a RP-directed "SHALL NOT" requirement(s) that restricts RPs from requiring attestation unnecessarily in public-facing applications. Additional language that clarifies the invasiveness of requiring attestation and the limited, high-risk contexts in which it should be used would also help contextualize the recommended change. Even though the draft goes into depth on this topic in 63B Appendix B, the language used there seems more directed towards the makers of syncable authenticators (Sect. B.3, p.89, L2976) or does not specify how agencies (i.e., federal CSPs and RPs) should handle absent, incomplete, or inconsistent attestations (Sect. B.3, p.89, L2984).
	63C	8.2.1	89	3042	All of the factors listed with respect to usability are insightful and could have metrics assigned to measure how successfully an RP or IdP is delivering its service to its end users.	Consider adding performance metrics for this section (see the US Web Design System's work on accessibility and Digital.gov's work on analytics) and making it normative.
	63C	All	All	All	The expansion and updates for Volume C contain clearly described patterns sufficient to support real-world implementations. GSA recommends NIST consider either changing the security, usability and privacy sections from Informative to Normative; or consider maintaining a best practices NIST IR with the usability and privacy recommendations. The usability and privacy recommendations deserve to be highlighted for both the U.S. commercial and U.S. government technologies, platforms and implementators.	GSA recommends NIST consider either changing the security, usability and privacy sections from Informative to Normative; or consider maintaining a best practices NIST IR with the usability and privacy recommendations. The usability and privacy recommendations deserve to be highlighted for both the U.S. commercial and U.S. government technologies, platforms and implementators.

	Base	3	24	982	The draft states that CSPs are required to complete the DIRM process and create a DIAS statement for each offering available to RPs. The current draft could potentially be construed to require a CSP to provide individual DIAS for each RP, and CSPs can serve dozens or hundreds of RPs, each with multiple user groups and types of online transactions. If this is the intent, it would be infeasible for CSPs to conduct this level of effort due to both scope and lack of visibility into the underlying data for each RP. GSA assumes the intent is for CSPs to instead create one DIAS per service offering, and strongly encourages NIST to ensure the corresponding DIRM process requirements support this intent. Some of the DIRM requirements will be difficult for CSPs to document because they are not the RP. The guidance should ensure CSPs support RPs by providing applicable information about their xAL offerings, so that RPs can then complete DIRM and DIAS statements for their user groups. This section should clarify that the CSP's cannot assess user populations and accepting risk for RPs.	Change "All CSPs SHALL implement the DIRM process for the services they offer and SHALL make a Digital Identity Acceptance Statement (DIAS) for each offering available to all current or potential RPs. CSPs MAY base their assessment on anticipated or representative digital identity services they wish to support. In creating this risk assessment, CSPs SHOULD seek input from real-world RPs on their user populations and their anticipated context." to "All CSPs SHALL implement the DIRM process for the services they offer and SHALL make a single Digital Identity Acceptance Statement (DIAS) for each offering available to all current or potential RPs. CSPs MAY base their assessment on anticipated or representative digital identity services they wish to support. In creating this risk assessment, CSPs SHOULD seek input from real-world RPs on their user populations and their anticipated context." In addition, review of the DIRM process should be completed to assess whether any requirements are not applicable to CSPs and are better left to RPs. Those requirements should be clarified and waived for CSPs as part of their DIRM process.
	Base	3	24	1003	Throughout section 3, the word "organization" is used, but it is not clear whether these steps apply to CSPs, RPs, or both.	Change "organization" to "RP" throughout Section 3, unless specific action is needed from the CSP.
	Base	3.5.1	45	1703	The draft states that organizations SHALL document their evaluation inputs to ensure that expectations are appropriately communicated to partners and vendors, but does not specify what sufficient documentation would look like. CSPs may look to other parts of the spec for guidance and language such as requiring privacy risk assessment summaries to be in "sufficient detail [...] to do due diligence investigation" (63A, Sect. 3.1.3.1, p.22, L1024) introduces ambiguity as "due diligence" isn't defined anywhere. Without further explanation on the level of detail needed here, RPs will find it difficult to compare prospective CSP services and their responsiveness to a changing information security landscape.	Consider adding additional guidance or requirements on what would constitute sufficient documentation for each minimum evaluation input that would "appropriately communicate" expectations to partners and vendors.
	Base	3.5.2	46	1715	Table 4 defines recommended performance metrics that organizations SHOULD capture as part of its continuous evaluation program, but the table does not include any language as to the purpose and context of each metric. By including this table, NIST is implicitly providing formal evaluation criteria for members in a federated context without providing a framework for *why* a metric should be captured and, for example, how an RP may use that information to assess an IdP, CSP, etc.	Consider either adding the purpose and evaluation criteria for each metric or moving this table to an implementation guide or appendix.
	Base	All	All	All	**NIST Question**: Is the updated risk management process sufficiently well-defined to support an effective, repeatable, real-world process for organizations seeking to implement digital identity system solutions to protect online services and systems?	**GSA Response**: With the exception of our comments on the DIRMs for CSPs, GSA agrees with the updated risk management processes outlined. These additions specifically are welcomed and address common challenges encountered with the previous processes: 1) Separating the user types and transactions for risk modeling 2) Identifying harms to individuals in addition to harms to an organization or impacted entities 3) Tailoring for disproportionate impact on underserved populations (example).