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:	*InCommon Federation*
Name of Submitter/POC:	*Tom Barton*
Email Address of Submitter/PO	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63-Base	5.2.3.1		1252-54	If an RP does not process PII, it may still require identity proofing. Your subsequent example of managing operational infrastructure, like the electric grid, is spot on.	Omit statement.
2	63-Base	5.3.2		1427-29	Being “unable” is too constraining. Even the subsequent example shows this: an FBI background check compensates for an IALx identity proofing process, even if the CSP is able to implement one.	Modify wording to permit compensating controls when appropriate, not just when unable.
3	63A				This is a much clearer and more simply stated rendering of IAL requirements than 63A-3. Kudos.	
78	63A	2.2		417	This statement is false, although if you implement the suggestion in comment 17 below, it will become true.	
4	63A	4.3.2		538-41	Must the applicant present the digital evidence during identity proofing, or may CSP perform the online access to applicant's digital evidence? Ie, need the applicant even be aware of digital evidence being created for them that is used for identity proofing? Example, MNO records used as digital evidence that are not necessarily accessible to their customers.	Add clarifying statements.
5	63A	5.1.1		716-17	Notifying RPs of changes to the internal processes by which the CSP performs identity proofing does not mitigate any risk to the identity proofing process.	Omit this requirement.
6	63A	5.1.2.1		761-63	Overly prescriptive if the CSP does not operate within the US Federal government or is not obligated to follow these specific sources under contract.	Rephrase to permit other privacy and/or security frameworks.
7	63A	5.1.2.1		769-71	Unclear wording.	Clarify that "organizations that use its services" refers to clients of their services and does not refer to any RPs that rely on authentications or claims issued by the CSP.
8	63A	5.1.3			The goal of ensuring equitability by US Federal agencies and others is laudable. However, private sector organizations that operate their own CSP as an enterprise service, not provided as a general CSP service to people outside of those belonging to the organization (employees, and perhaps students or other affiliates), may have their own equitability goals and means of achieving them. Any equity issues they have are more likely to do with the nature of the organization’s culture and mission; their identity proofing process isn’t at issue.	Apply equitability requirements only to CSPs that provide their services outside of a single enterprise context.
9	63A	5.1.4		828-30	Organizations that are not federal agencies may use worthy risk management methodologies other than NIST's.	Broaden the statement to permit other risk management frameworks.
10	63A	5.1.6			Throughout volumes A, B, and C, various terms are used in lieu of "validated address" as defined in 63A section 4.3.4.	Use "validated address" for this construct consistently throughout 800-63. Make a glossary entry for "validated address", replacing that for "address of record". Alternative: standardize on "address of record", update its glossary entry to refer to 63A section 4.3.4, and amend 4.3.4 to restate there that "address of record" refers to an address validated by one of these methods.
11	63A	5.1.6		874-75	What random number generators are approved?	Cite reference, perhaps to an additional term in the glossary.
12	63A	5.1.6		876-77	What is "a uniquely identified address" and what is "an appropriately constructed" session ID?	Define these terms.

13	63A	5.1.9.1			Trusted referees are specifically trained "agents" of CSPs, which need not imply anything else about their relationship with the CSP. They should be identity proofed to mitigate one avenue for potential fraud.	Add "CSPs providing trusted referees SHALL identity proof each trusted referee to the same or higher IAL intended for the applicant" in this section.
14	63A	5.1.9.1		994-95	This requirement is not suited to CSPs that provide enterprise IAM services, ie, only to employees, students, etc. Such organizations may choose means outside of the credentialing process to address access and equity issues.	Demote to "MAY" and add a SHALL requirement specific to federal agencies (who will pass it on in their contracts to commercial CSPs), or tighten to "CSPs providing services to the public SHALL ...".
15	63A	5.1.9.1		997-100	Further follow up on Comment #14 above	In each numbered requirement, replace "CSPs" with "CSPs providing trusted referees".
16	63A	5.3.2.1, 5.4.2.1, 5.5.2.1			If Trusted Referee is used in lieu of collecting evidence, logically these evidence requirements are not met and IAL1 cannot be asserted.	Add "3. Trusted Referee attests to IAL1 equivalent identity proofing" or similar in the other two sections.
17	63A	5.3.2.1		1056	IAL1 is too close to IAL2. Address in part by slight weakening of evidence requirement.	Remove "and one piece of FAIR evidence".
18	63A	5.3.3		1068-69	The requirement does not permit use of automated means of validating FAIR evidence.	Permit all of the validation methods available at IAL2 for validation at IAL1.
19	63A	5.3.3		1070-75	IAL1 is too close to IAL2. Address in part by weakening the attribute verification requirement. This also helps IAL1 be an option for populations that tend to be underrepresented in authoritative or credible sources typically available, ie, those with access or equity challenges.	Omit item #1, ie, consider attributes presented on validated evidence to be validated attributes (for IAL1).
20	63A	5.3.4, 5.4.4, 5.5.4			IALx permit "demonstrated association" as a verification method. Shouldn't the subscriber account to which association is demonstrated have the desired IAL bound to it?	In all three sections (ie, for each IALx), insert "bound to a subscriber record at IALx" between "digital account" and "through an AALx authentication".
21	63A	5.6, Table 1				Align Evidence and Validation for IAL1 with suggested changes in Comment #s 17 and 19.
22	63A	6.1		1258	Clarify to avoid a misunderstanding that, eg, photos of evidence must be stored.	Amend to "Issuer and type of validated identity evidence".
23	63B				The term “claimant” is used in many places where “subscriber” should be used instead, following the usage established in 800-63 base volume.	Replace "claimant" with "subscriber" appropriately.
24	63B				The usage “CSP or verifier” is used in several places in order to account for whether the verifier is part of the CSP’s operation or is operated by a third party. But this can lead to confusing statements. Suggest that “verifier” should always refer to a technical component, that all obligations should be on the CSP (and not “CSP or verifier”), and separately address the situation of a CSP some elements of which are operated by third parties. The CSP is always responsible, and they must be satisfied that any third party operations meet the CSP’s obligations.	Replace "CSP or verifier" with "CSP" appropriately, and add statements, if necessary, about CSPs ensuring that any reliance they have on third parties supports the CSP's obligations.
25	63B	4		426-30	An authentication process need not produce any subject identifiers or attributes - these might be supplied by the RP itself. Any attributes provided by a CSP to an RP upon successful authentication of a subscriber should be addressed in 63C since authentication protocols addressed in 63B do not themselves transport attributes from CSP to RP. Also, in a federated context there are use cases in which it is not desirable for the IdP to NOT send the same subject identifier each time the subject authenticates to a given RP, even if it is pseudonymous.	Omit statement from 63B. This is covered in 63C.
26	63B	4		435-36	This statement is addressed in 63A and again in 63C. It does not belong in 63B. Further, "digital identity service" is ambiguous: does it mean CSP or RP or both?	Omit from 63B.
27	63B	4.2.3, 4.3.3			Reauthentication is something an application may initiate in managing an application session with a subject. This section should make clear that its statements apply to RPs. Also, in many cases a verifier has no connection with an RP session, and so cannot prompt user activity before RP session timeout. And does it matter whether a verifier or any other RP-affiliated agent prompts the user?	Declare these statements to apply to RPs. Do not prescribe that a verifier should have any role in RP session management.
28	63B	5.1.3.1		856-57	If a VoIP phone number is registered with an e911 service, as many businesses with internal VoIP phone systems do, should possession of the associated phone be considered as proven?	

29	63B	6.1.1			In 63A 5.3.4 and 5.4.4.1 the notion of “demonstrated association” is a recognized method of verifying a claimant’s identity. This method relies on the claimant authenticating, with appropriate strength, to a digital record that serves as suitable identification evidence. For a CSP that accepts this method for identity proofing, shouldn’t its use also be permitted to establish that the same person is acting in different sessions of an authenticator enrollment process?	Add a demonstrated association means of establishing that the same subject is acting across multiple authenticator management sessions for both remote and in-person transactions.
30	63B	6.1.1		1610-13	This statement limits address types compared to requirements in 63A and definition in 63 glossary.	Align statement with address types permitted by 63A.
31	63B	6.1.3		1737-38	63A defines IAL0 as no identity proofing. IAL1 requires more proofing than can be assumed by any arbitrary social network provider.	Replace "IAL1" with "IAL0".
32	63B	7.1		1824-26	There are often two types of sessions: single sign-on sessions and application sessions. A verifier may indeed create single sign-on “session secrets” (as termed in the draft), but in general it has no connection with the “secret used for session binding” used in session management between an application host and subject. This section asserts a dependence of the latter upon the former - that dependence should be removed. Although the following section 7.2.1 correctly addresses this in the federation context, even without federation (or single sign-on) an enterprise authentication service relied upon by an application also separates the verifier from the application.	Use different terminology that makes a clear distinction between the different types of sessions that may be operative.
33	63B	8.1		Table 3	The rows on “Assertion Manufacture or Modification” are in the analogous table in 63C, where they belong. Any assertions produced as a consequence of an authentication event seem not the result of authenticator compromise but of compromise to the assertion protocol and management, ie, federation. Also, Table 4 has no rows corresponding to these.	Remove from Table 3.
34	63C					Consider refactoring along the lines of 63A so that concepts are defined and discussed before being specified in FALx requirements.
35	63C				Some requirements are repeated in different sections, increasing the chance that their wording varies by context and seeding confusion of what the requirement actually is.	Each requirement should be stated once, and where that is not feasible, ensure that the same wording is used.
36	63C				Some normative sections read more as informative, contain speculation, or even go as far as promoting specific approaches over other legitimate choices. Focus wanders too often from the business of identifying mitigations to risks associated with federated access. The other material may be useful, but should not be normative.	Material from sections 5.4-5.4.3 (provisioning), 5.7 (shared signaling), and 6.3 (identity APIs) should largely be made informative.
37	63C				Clear agreement among parties is required by 63C about a variety of different concerns. That is fine. However, all such concerns are prescribed to be addressed in a single trust agreement, the net result of which is that the only parties that might have a perspective on every concern it addresses are an IdP and RP pair. This does not permit other parties, such as a federation authority or some other mutually trusted third party, to establish terms of agreement about some of those concerns.	Don't require all terms of agreement that must exist before a transaction occurs between an IdP and an RP to be part of a single "trust agreement". Let agreements be established in whatever ways work, with whatever parties can execute them, provided that IdP and RP have each agreed on terms that address all 63C requirements before a transaction occurs between them.
38	63C	2		347-49	Sharing subscriber's identity with an RP is contraindicated in some use cases.	Change to say that "The RP uses the information in the assertion to identify the RP subscriber record and ..."
39	63C	2		364-65	Subscribers are not identified in all federated access use cases. Sometimes only one or more non-identifying attributes are all that the RP needs.	An assertion may include ...
40	63C	4		440-41	"Logging in", ie, establishing some form of RP session, is not the only use of federation.	Suggest replacing "for the purposes of logging in the subscriber to the RP" with "to enable subscribers' access to RP's services".
41	63C	4		444	Clarify that direct and indirect methods of exchange are both acceptable.	The IdP and RP have directly or indirectly exchanged identifiers

42	63C	4		459-61	Since Low impact systems are to use FAL1, shouldn't the standard of security employed also be Low at that FAL level? Similarly for High and FAL3.	Revise to align standard of security with assessed impact level.
43	63C	4.4		552-55	Overly prescriptive. There's no risk engendered by sending the same xAL level with every assertion.	SHALLs should be SHOULDs or MAYs.
44	63C	4.4		560	IAL0 is the lowest numbered IAL defined in 63A-4.	Omit ", the lowest numbered IAL described in this suit". Also, replace "no IAL" with "IAL0".
45	63C	4.4		574-575	This statement might be read as requiring the RP to verify the IdP's side of FALx in addition to its own obligations.	The RP SHALL ensure that its processing of the federation transaction...
46	63C	5.1		647-48	This is probably contrary to stated usability considerations. Subscribers cannot be expected to know anything about xALs or other parameters of a trust agreement. Explaining anything about those parameters in the middle of a federated authentication transaction is the worst possible time to try to explain anything. It will serve no actual informative value.	For consumer/citizen oriented IdPs, inform applicants during their enrollment process. For enterprise IdPs (in which the organization is the authorized party), incorporate these notifications into existing vehicles for informing their employees, students, etc. Since these contexts cannot be sensitive to each RP encountered dynamically by each subscriber, the notifications instead acknowledge the range of possibilities the IdP is operated to address. For RPs requiring subscriber attributes from the IdP in order to perform a service, obtain subscriber's consent.
47	63C	5.1.2		704-07	Doesn't account for possible role of interfederation in the establishment of trust agreements.	Amend to encompass interfederation, ie, when there may be different federation authorities for IdP and for RP who have executed a common interfederation agreement.
48	63C	5.1.2		711-17	A federation authority is unlikely to already be set up to perform audits, so this presents a substantial hurdle to achieving FALx for an existing federations of any scale. It is also not the only way to achieve trustworthy expression of claims and use of subscriber attributes.	Enable the fed authority to leverage its role as a trust broker by requiring it to devise policy and process for assuring trustworthy operations of those of its members wishing to participate in xALx level transactions rather than requiring it to operate an audit function. For example, a fed authority may determine that a research cyberinfrastructure consuming subscriber attributes will indeed honor its contractual commitment (expressed in the trust agreement) to only use them for their service and apply appropriate security measures to protect them, or that a university IdP will produce accurate claims (as required by the trust agreement) in good faith given its mission and disincentive to “cheat” (eg, loss of standing to apply for federal grants). The fed authority may also choose to recognize attestation letters submitted by internal or external auditors who assessed a member organization’s IdP or RP, or accept IdP operations that incorporate third party services that have been successfully assessed by federally recognized means (such as a Kantara Initiative IAL2 Trust Mark). Such good faith determinations can be backed up by policy and process (identified in the trust agreement) for dealing with a situation in which a concern arises about some party’s performance of their obligations embodied in the trust agreement.
49	63C	5.2		768-71	This statement doesn't seem to encompass the typical situation in multilateral federation, in which manual registration of IdPs and RPs with a federation authority occurs once and subsequently systems exchange info without direct human involvement. In particular, info is entered into a federation system, not into each target's system.	"enter the information into the target systems (for bilateral registration) or a federation system (for multilateral registration) ... without direct human involvement, or both."
50	63C	5.2.1			This section doesn't seem to encompass the typical situation in multilateral federation, in which manual registration of IdPs and RPs with a federation authority occurs once and subsequently systems exchange info without direct human involvement. In particular, info is entered into a federation system, not into each target's system.	Update the section to incorporate the model in which manual registration is made to the operator of the federation to which the IdP or RP belongs.
51	63C	5.2.2		798-99	Needlessly prescriptive - a well-known location not at the IdP is a common practice, with possibly less risk than obtaining the info from the IdP.	Omit "at the IdP".

52	63C	5.2.2		803-04	This need not be the only, or best, way to establish which attributes the IdP will include in its assertions to the RP. Leave that to federation operating practices in the multilateral case.	Suggest "For bilateral federation, the RP sends its attributes to the IdP, and the IdP associates those attributes with the RP. For multilateral federation, the RP follows federation-established operating practices to enable IdPs to associate those attributes with the RP".
53	63C	5.3			1. The approach of only using allow/blocklists is overly prescriptive - there are other, and often better, ways to operate an IdP in conformance with policy decisions made by authorized parties. Egs, entity categories, IdP policy configuration language, IdP operation linked to an external access management system, etc. Virtually all of the criteria defined in section 5.3 are currently expressed in terms of allow/blocklists, and these must all be replaced with language that does not constrain established good practice or further innovation in access management techniques. 2. As recognized elsewhere in 63C-4, a federation might define "tiers" of membership, one of which could be the subset of its entities that constitute a FAL2 federation, say. The criteria in this section should be restricted to IdPs and RPs in that tier, not impinging on an IdP's or RP's operation in other contexts.	Re (1), language such as "previously authorized for runtime operation" might be useful in rewriting this section.
54	63C	5.3.1		847-48	1. This should not pertain to RPs that don't require FALx, ie, IdPs and/or RPs may belong to federations not all entities of which are intended or authorized to function at specific FALs. 2. This may be interpreted to mean that each IdP must perform its own audit of each RP, or require each RP to show documentation of a successful audit.	Broaden the criterion to encompass having the IdP check with a trusted party, which could be the RP itself, but might also be the federation authority or another party they trust to know, and narrow the criterion to pertain only to IdPs expressing an FAL level to the RP.
55	63C	5.3.3		874-75	This statement is debatable, generally false in B2B contexts, and irrelevant. Further, throughout this section if the intention is to state some requirements that only pertain when the authorized party is the subscriber, then say so. They make little sense when the authorized party is the IdP organization.	Omit this statement, and amend section 5.3.3 to refer specifically to when the authorized party is the subscriber.
56	63C	5.3.4		903-05	This may be interpreted to mean that each RP must perform its own audit of each IdP, or require each IdP to show documentation of a successful audit.	Broaden the criterion to encompass having the RP check with a trusted party, which could be the IdP itself, but might also be the federation authority or another party they trust to know.
57	63C	5.3.6			This section only makes sense when the authorized party is the subscriber.	Rewrite the section to make clear that it applies when the authorized party is the subscriber and not the IdP organization (which can't even be present in a transaction as required by one criterion in this section).
58	63C	5.4			Why is this entire section important in 63C? What threats engendered by reliance on federation for user access does this section address? RP subscriber accounts, provisioning, and deprovisioning are used across all manner of user access frameworks and are not specific to federation. Furthermore, adding corresponding material to trust agreements places those outside of the purview of federation authorities.	See comment #36.
59	63C	5.4.4		1074-75	SORN requirement is specific to federal agencies.	Say so.
60	63C	5.6		1170-72	This is incompatible with trust agreements in a multilateral federation, which are not specific to particular RP-IdP pairs among federation members. Also, 63B-4 already stipulates max 12 hours IdP session lifetime for AAL2, 30 days for AAL1. Further, it is unnecessary given other requirements for IdP to report authentication time to RP and requirement to perform reauthentication on RP request, which together permit an RP to implement a shorter lifetime without the added complexity of signaling an RP-specific authentication lifetime to the IdP.	Just use the AAL attribute and omit any requirement for IdP-RP specific signaling or term of agreement over authentication lifetime.

61	63C	5.7			Shared signaling is not an aspect of federated access, although it can be used to enhance operations and security of federated (and non-federated) entities. But many other technologies and frameworks also can potentially improve operations and security of federated entities. Why should 63C scope be expanded to cherry-pick shared signaling?	Make this material informative guidance, possibly outside of 63C, such as in best practice documents that suggest overall application architectures suited to a federated context or an implementation profile that can itself serve as a standard for adoption by parties wishing to adhere to a common standard.
62	63C	6, 6.1.2.1, 6.1.2.2		1255-58	When an RP bound authenticator is required, with the implication that bearer assertions are not strong enough for the RP, why would the RP choose to rely on a bearer assertion to manage this concern? Further, this statement does not permit an RP wishing to use RP bound authenticators to manage them by itself. Subscriber IdPs must be in on the plan, which is needlessly complex in general.	Omit this and other 63C requirements that involve IdP operations in managing RP bound authenticators. Possibly include such requirements in an implementation profile, outside of 63C, for whatever environments it might suit.
63	63C	6		1263-65	Above in lines 1230-52 it says SHALL for these items. Which is it?	Make requirement consistent between its various restatements, or better, reference one instance rather than repeating it.
64	63C	6.2.5.1		1506-10	Shouldn't security incident response be added as a permitted purpose?	Add security incident response.
65	63C	6.3		1543-44	There are also downsides of course. Notably, it expands the attack surface of the IdP.	Omit this sentence.
66	63C	6.3		1552-54	This statement is non-substantive and false in some contexts (especially B2B use of federation, in which incentives can work to minimize sending PII).	Omit this statement.
67	63C	6.3		1561	Any upper bound? 100 yrs? It seems a risk to leave it open to an RP beyond RP session creation. Utility for on-going attribute synchronization is questionable, given the downside of IdP thereby undermining its ability to protect its subscribers' privacy.	Use of identity APIs in 63C should be constrained to the context of providing a back channel for delivery of subscriber attributes associated with a specific federated transaction.
68	63C	6.3		1573-74	If an identity API is to be used to offset assertion payload, isn't the logical conclusion to require that no party shall be given blanket access? If the value is not exposing PII to hostile browsers (even though assertions are already required above to be encrypted), is it acceptable that one compromised credential outside of the IdP's control can expose PII for all subscribers held by that IdP?	Use of identity APIs in 63C should be constrained to the context of providing a back channel for delivery of subscriber attributes associated with a specific federated transaction.
69	63C	6.3.1			This topic is not adequately treated in this section, understandable given limited real world experience with it. Would it be better to make some high level statements such as "risk to subscriber PII held by or obtained through an attribute API shall be protected to a level similar to that of PII obtained from their IdP" and "RP shall authenticate the attribute API provider and validate its assertion protections"?	If by "attribute provider" 63C refers to a third party contracted by an IdP to provide a back channel attribute service for its assertions, then this section is not needed because the IdP is already bound to meet applicable criteria, which includes its third party operations. If it refers to a 3rd party independent of any IdP, then the requirements in this section do not make sense, yet it would be useful to address that circumstance since there are such entities in real world federation.
70	63C	6.3.1		1582-83	As in the example below, the provider of an attribute API may be independent of the IdP, so the latter cannot be responsible for the former. Since the attribute API provider is an independent party having standing in the federation analogous to the IdP and the RP, it should have its own trust agreement with the federation or with individual RPs.	If by "attribute provider" 63C refers to a third party contracted by an IdP to provide a back channel attribute service for its assertions, then this section is not needed because the IdP is already bound to meet applicable criteria, which includes its third party operations. If it refers to a 3rd party independent of any IdP, then the requirements in this section do not make sense, yet it would be useful to address that circumstance since there are such entities in real world federation.
71	63C	7.1		1627-31	This paragraph contradicts requirement (2) above (line 1620). It also contradicts statements elsewhere in this doc concerning the attributes that may be sent from IdP to RP. In particular, RP is not permitted to receive attributes outside those bounds.	Omit paragraph.
72	63C	7.1		1632-36	Omit. SHOULD for FAL2 is already stated elsewhere. Moreover, the RP opens the back channel connection to the IdP and so does not expose a corresponding end point to attack.	Omit paragraph.
73	63C	7.1		1644-47	This sentence offers implementation guidance and is not substantive.	Omit.

74	63C	7.2		1657-60	This non-substantive statement further reinforces the impression that the author is promoting one style of presenting attributes in a federated context over others. Even if they believe it is superior, it's not their call and other architectures are used and usable.	Omit.
75	63C	7.2		1661-70	This non-substantive paragraph repeats statements made elsewhere, contains speculation and opinion, and is at best informative.	Omit.
76	63C	7.3		1683-86	This paragraph expresses opinion and doesn't belong in a normative section. Also, there are no standards for expressing much of this info, so even as friendly advice it is not practical.	Omit.
77	63C	7.3		1692-94	Suggest weakening these to SHOULDs and remove "where feasible" and "to the extent possible". This in recognition that support for derived attribute values is not common. Maybe for 800-63-5 things will have matured to the point that SHALL can be reinstated.	Weaken these criteria to SHOULDs or MAYs and remove "where feasible" and "to the extent possible".