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

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

Organization:	*Department of Defense Manpower Data Center (DoD/DMDC)*
Name of Submitter/POC:	*Tim W. Baldridge*
Email Address of Submitter/POC:	[REMOVED]

Comment #	**Publication (Base, 63A, 63B, 63C)**	**Section**	**Page #**	**Line #**	**Comment (Include rationale for comment)**	**Suggested Change**
1				General	While for CAC CSP products tend to perform both identity vetting and credentialing, CSPs outside of CAC issuance don't necessarily perform both functions within the same product. Continuing to use the term "CSP" to include identity vetting could be confusing to new identity vetting product vendors and/or CSP vendors. Similarly, non-PKI credentials tend to be bound to an IdP, not a credential provider.	Recommend creating a new term that encompasses products that only verify an applicant's identity; explain how assertions from the identity vetting vendor can be passed to the CSP to bind an identity to a new credential, and discuss how the IdP comes into play, and can also be the CSP. A great example of a product that can perform all three functions is login.gov, whereas there are multiple IdPs on the market now that bind identities to credentials that they create and authenticate users, but don't vet them.
2	63-Base	2	3	351-381	These four introductory paragraphs seem unnecessary and to some extent are confusing. The first paragraph isn't about digital identity, there is a reference to natural vs. legal persons that was not introduced previously nor is it expanded upon which could be confusing for some readers. There is a statement that establishing digital identity is intended to demonstrate trust, however the one does not necessarily lead to the other. In all, these 4 paragraphs don't add value to a document that is setting guidelines for the issuance and use of digital credentials	Delete these four paragraphs from the Introduction and begin the Introduction with Line 382.
3	63-Base	2	3	385	The sentence: "The model is supported by a series of processes: identity proofing, authentication, and federation." Binding the digital identity to the physical identity is missing here. The series of processes should be identity proofing and binding (or issuance), authentication, federation.	Recommend including 'binding' here and modifying the following sentence as follows: The identity proofing process establishes that a subject is a specific physical person and binds that physical identity to a digital identity.
4	63-Base	2.1	4	419	Opening clause is unnecessary here. Does not add value to the narrative.	Drop "Not all digital services require identity proofing or authentication; however," and begin with "This guidance applies to. . ."
5	63-Base	2.3.1	7	510	What is meant by "availability issues" and how does it relate to "fraudulent activity"? Throughout the document 'availability' is used in several contexts.	Review this sentence for clarity and understanding. Perhaps reword "availability issues" to make it clear that it is talking about the dearth of identity source information (if that is in fact the correct interpretation).
6	63-Base	2.3.1	7	520	What are "equivalent standards". Is there any such thing? Could you give examples of an industry standard NIST considers equivalent to FISMA?	Recommend revising this sentence to assist industry with identifying such equivalence.
7	63-Base	4.1	14	669	This Step 3 explanation is actually capturing Steps 3, 4, 5, & 6.	End this explanation after the 1st sentence.
8	63-Base	4.1	14	689	This is confusing. "In all cases, the RP should request the attributes it requires from a CSP or IdP before authenticating the claimant." Isn't it true that the IDP needs to authenticate the subject such that the RP will have confidence about who they will now request additional attribute information about? This seems important to bind the subject to the attribute information request. The attributes will be used to make a suitability/authorization decision. Authentication should already have happened.	Review this sentence for clarity, accuracy and understanding.
9	63-Base	4.2	15	719	"Subscribers have a duty to maintain control of their authenticators and comply with CSP policies in order to remain in good standing with the CSP." This appears to put requirements on Subscribers who are notoriously hard to control and are not likely to read this document.	Recommend rewording this sentence to something along the lines of "CSPs SHALL(?) ensure subscribers understand their responsibilities to maintain control of their authenticators and comply with CSP policies in order to remain in good standing with the CSP."
10	63-Base	4.2	15	721	"In order to request issuance of a new authenticator,. . ." This is actually referring to 'reissuance' or issuance of a second authenticator when the subscriber already has a relationship with the CSP.	Recommend revising this sentence for accuracy and clarity. Otherwise confusing.
11	63-Base	4.3.1	17	741-743	The usage of device leveal signals to enhance a user's authentication is becoming more prevalent, and is explicitly required in M-22-09, implementation for contextual authentication is relatively new.	While discussion of contextual authentication and device level signals would be beneficial in Rev. 4, recommend including them in Rev. 5 to avoid delays to Rev. 4 release.
12	63-Base	4.3.1	18	788	The word "Some" should be "Multiple". "Some" is vague, whereas "multiple" clearly indicates the intent and is the term being used throughout.	Replace 'some' with 'multiple'. Could also use "minimum of two" here if prefered.
13	63-Base	4.3.3	19	814	Figure 4 does not have a step by step explanation as is present for other figures. This could lead to misunderstanding.	Recommend some sort of explanation of Figure 4 for clarity
14	63-Base	4.3.3	20	819-822	Remove 'can' from this sentence. It becomes more assertive as opposed to appearing tentative.	Revise the sentence as follows: Well-designed protocols can protect the integrity and confidentiality of communication between the claimant and the verifier both during and after the authentication, and can help limit the damage that can be done by an attacker masquerading as a legitimate verifier.
15	63-Base	4.3.3	20	823	Replace the first 'can' from this sentence with 'should'. It becomes more instructive as opposed to conversational.	Revise as follows: "Additionally, mechanisms located at the verifier can should be implemented to mitigate online guessing attacks against lower entropy secrets —. . ."
16		4.4.1	21	883	Is this true? While there will be some advantage, RPs will still need to manage identities within their infrastructures, particularly for repeat visitors and to protect PII.	Recommend rephrasing this statement to accurately represent the advantages.
17	63-Base	5.1.3	28	100	Header missing	Add the header "Loss of Sensitive Information" here.
18	63-Base	5.2.3.2	35	1334	Editorial recommendation	Remove the word "as" from this line as follows: ". . .which will be as assessed against additional potential impacts as described . . ."
19	63-Base	5.3.2	37	1439	Editorial recommendation for clarity.	Remove "select to" from this sentence as follows: ". . .they MAY select to implement a compensating control."
20	63-Base	General	Genera	General	One of the major reasons for this special publication is to promote interoperability and trust among federal agencies. HSPD-12 and various OMB guidelines require all federal agencies to issue IAL3 and AAL3 authenticators to employees. As such, there should be specific call out in this document to outlined how HSPD-12 PIVs and PKI certificates are expected to be handled to ensure interoperability.	Recommend where possible identify specific normative or informative guidelines for federal agencies when interacting with applicable employees using HSPS-12 PIVs or Derived PIV credentials.
21	63-Base	General	Genera	General	As with FIPS-201, there continues to be major challenges for RP and IdP to understand that the John A. Smith being authenticated is the same John A. Smith that is already known to the federal agency due to previous encounters, relationships or current affiliation. A classic example is a reservist in U.S. Army who is also a contractor/civilian employees with Department of State or Department of Energy. It is unreasonable to expect seperate, unconnected IDs were be created within DoD for the same indivdual.	Recommend the document acknowledge these scenarios and identify specific mechanisms and required person identifiers federal agencies can to perform identity resoltions to single person identity wihtin their federal agency.
1	63A	1	2	360-361	Last sentence is confusing since use of a call center for identity proofing is one of the solutions offered.	Revise, clarify intent of this sentence.
2	63A	2	3	368	The word 'some' is unnecessary in this sentence	Remove 'some' as follows: "Examples of this include accessing some government services or executing financial transactions."

3	63A	2.1	4	402	Mitigate is defined as "make less severe, serious or painful". Is that what we're trying to do here? Or are we trying to prevent fraudulent access altogether?	Recommend use of a different action word here. "inhibit" may be a good choice as follows: Fraud Prevention: mitigate inhibit attempts to gain fraudulent access to benefits, services, data, or assets.
4	63A	2.2	4	405	Do the IALs 'describe' identity assurance or do they 'define' the assurance we can place in an identity assertion	Recommend replacing "describe" with "define" here as follows: Assurance in a subscriber's identity is described defined using one of the following Identity Assurance Levels (IAL).
5	63A	4	6	450	IAM products have advanced since the last iteration, and CSP can now also be an IdP or RP. Recommend making a clear distinction between the products to make the document less confusing to those readers who are new to IAM.	Recommend including clear delineations between a CSP, IdP, and RP in the definitions so vendors and practitioners can better translate the guidelines into IAM products.
6	63A	4.1.1	8	480	"The CSP asks the applicant to take a photo of themself, with liveness checks." and then what? What is a "liveness check" in this context? This is the only instance of the use of this phrase in the entire document. Elsewhere the term used is "liveness detection".	Recommend revising this statement to indicate the photo is sent to the CSP. If the expectation is that the photo is taken with the device's camera, should say so. Replace "liveness checks" with "liveness detection".
7	63A	4.1.1	8	482	Editorial recommendation. It is not a foregone conclusion that they match.	Revise sentence as follows: The CSP compares the pictures on the license and the passport to the photo of the live applicant's photo from the previous step and determines whether they match.
8	63A	4.1.1	9	485	Editorial recommendation.	Remove the word 'they' as follows: ". . .verifying they the applicant is in possession and control of the validated phone number."
9	63A	4.3.2	10	540	Should this be #6 or should it be a closing paragraph. The intro to the list states "Acceptable digital evidence SHALL contain all of the following characteristics". #6 states "if applicable" and refers to verification of the evidence not the characteristics or presentation of the evidence.	Recommend removing #6 from the list and making it a closing paragraph to the section. Also recommend fleshing out the sentence for clarity.
10	63A	4.3.3.1	11	553	The term "reasonably assumed" seems very subjective. In M-04-04, the term "balance of probabilities" was used, which suggested some calculation or statistical reasoning had been employed.	Recommend revising this bullet to replace "reasonably assumed" with a more measurable term.
11	63A	4.3.3.1	11	557	Allows evidence to have expired within the past 6 months which contradicts the statement in Section 4.3 (line 498) that evidence is unexpired.	Recommend revision here or in Section 4.3 to remove this contradicts.
12	63A	4.3.3.3	12	586	What does "visually identified the applicant" mean? Does this statement indicate that the id proofing encounter was in-person (or supervised remote)? Why not say so? Thinking about a passport, this would eliminate passports from Superior classification unless comparing new picture submitted for passport replacement with existing picture is 'visual identification.'	Recommend revision here to indicate that Superior Evidence requires in-person id proofing or describe what "visually identified" means?
13	63A	4.3.4.1	12	606	How does one "confirm" evidence is not counterfeit or tampered with? Is there a section in this document that goes into detail on this? Should there be? Is visual inspection sufficient? And how is that accomplished adequately remotely?	Recommend either adding some information here on confirming evidence is not counterfeit/tampered with or giving reference to where that is discussed in the document.
14	63A	4.3.4.4	14	653	"Maintains identity attribute information obtained from multiple sources that is checked for data correlation for accuracy, consistency, and currency." This sentence does not read well. Seems awkward. Should there be a 'for' in front of 'accuracy'?	Recommend review, revise sentence for clarity.
15	63A	4.4.1	14	664	Is Supervised Remote included in the definition of "In Person" here?	If Supervised Remote is included in the In-Person definition, make a statement to that effect in this definition. Ditto if it is part of the Remote definition.
16	63A	4.4.1	15	684-688	Digital Account / Verifiable Credentials are not clearly defined. There's no definition in the base document; they are briefly mentioned in 63A. Assumption is the NIST is only describing verifiable credentials as defined in ISO 18013-5; however, NIST might be describing a more-holistic list of digitial accounts, to include Login.gov credentials.	Recommend defining digital account/verifiable credential. The definition should include a discussion on how IALs are transferrable as well as the need for a minimum AAL required to prove each IAL. For example: credentials issued at AAL1 can only verify the identity at IAL1, however, credentials issued at AAL3 can verify the applicant's identity at IAL1-3 (depending on which IAL is bound to the credential); similarly, for an applicant to assert proof of posession for IAL3 vetting, a strong, phishing resistant MFA would be required. Regardless, presenting a verifiable credential should be able to transfer the IAL of the credential to the new credential (e.g., lines 578-581 in 800-157r1).
17	63A	5.4.1	20	822-839	M-22-09 requires encryption for data at rest and in transit, suggest being more explict and state "encrypted" instead of "protected" chanel	Explicitly state encryption of data is required.
18	63A	5.1.4	20	829	Editorial recommendation - either remove 'an' or make controls singular.	The CSP SHALL assess the risks associated with operating its identity service, according to the NIST risk management framework [NIST-RMF], and apply an appropriate baseline security controls.
19	63A	5.1.8	22	909	"Behavioral characteristics" are included in the definition of "Biometrics" but not expanded upon in the examples. What is a qualifying "behavioral characteristic"? All other sections in this document use "behavioral analytics" as a fraud mitigation measure, not as an identity proofing measure. How does a behavioral characteristic enable a CSP to uniquely resolve an individual identity within a given population or context, verify that an individual is the rightful subject of identity evidence, etc.?	Consider revising this text to include a behavioral characteristic example. Or if not germane to the id verification process (picture, iris scan, fingerprint) say so here.
20	63A	5.1.9	24	960	. . .CSPs provide Trusted Referees. Is this a MUST statement?	Make an assertive statement as to whether CSPs are REQUIRED to provide trusted referees.
21	63A	5.1.9	24	987-989	States that ". . . applicant references are not authorized to represent subscribers in transactions with RPs." So does this mean that an applicant reference cannot have custodial authority or power of attorney over the applicant? This seems limiting in a context where the individual needing the assistance with the identity proofing/enrollment process also needs help conducting transactions	Review this prohibition concerning its validity/usefulness.
22	63A	5.1.9.1	24	994-995	Do Trusted Referees constitute an in-person interaction in an otherwise remote identity proofing process? Why not make this statement?	Clarify whether Trusted Referees meet in person with an applicant in an otherwise remote id proofing process.
23	63A	5.1.9.1	24	996	Why the caveat "Where Trusted Referees are offered" if CSPs must make them available - see comment #34	If supposition in comment #34 is correct, remove this caveat. Otherwise, make it clear in 5.1.9 that CSP provision of trusted referees is optional.
24	63A	5.1.9.2	25	1010	Why the caveat "If the CSP allows for the use of applicant references" in the 3rd item?	Recommend removing this and aligning the 3rd item with the 2 above.
25	63A	5.1.10	25	1014	Does this suggest that the provision of id proofing services to minors is optional. Should it say that explicitly here?	Recommend making a clear statement that CSP either MUST or MAY offer id proofing services to minors.
26	63A	5.2	26	1034	NIST added an additional IAL - 0.	Recommend adding and defining IAL0 in this section, even if it only includes a short paragraph.
27	63A	5.3	26	1040	Why the use of "Notably" here?	Recommend removing "notably" from this sentence
28	63A	5.3.2.1	26	1056	The evidence requirements at IAL1 are the same as IAL2. This seems excessive. Based on the definition, it appears a driver's license is STRONG not SUPERIOR (cryptographic processes are missing in many cases) and yet we use Drivers Licenses as our base id proof in all contexts. If that is a correct conclusion, it seems that IAL 1 should be satisfied with one piece of STRONG evidence.	Consider revising the Evidence requirements at IAL 1 to allow one piece of strong evidence (i.e. drivers license or equivalent).
29	63A	5.3.4	27	1078	At IAL2 there is discussion of id proofing as a remote process and as an in person process. This is missing here, even though Section 5.3.1 indicates in-person proofing is an option.	Consider paralleling the language in Section 5.4.4 as applicable for in-person proofing at IAL1 here in 5.3.4.
30	63A	5.3.4	27	1084-1085	Any AAL would suffice to prove proof of possession of a credential with an IAL1	"Demonstrated association with a digital account through an AAL1, AAL2, or AAL3 authentication or at a minimum an AAL1 and FAL1 federation protocol, or"
31	63A	5.3.5	27	1088	Not sure why this is a SHOULD. It seems that even at IAL1, sending a notification to an address of record is a basic process for preventing fraud.	Recommend reconsidering whehter notification to address of record should be SHOULD or SHALL.
32	63A	5.4.3	28	1111	There is no requirement here to validate FAIR evidence (this existed in IAL1).	Consider adding requirement to validate the FAIR evidence, when presented.
33	63A	5.4.3	28	1118	Editorial comment	Recommend including the word "both" here: "The CSP SHALL validate all core attributes by both:
34	63A	5.4.4.1	29	1133-1134	Either AAL2 or AAL3 would suffice to prove proof of possession of a credential with an IAL2	"Demonstrated association with a digital account through an AAL2 or AAL3 authentication or at a minimum an AAL2 and FAL2 federation protocol"

35	63A	5.4.5	29	1140	Does the requirement to send notification to an address of record also apply for in-person proofing?	Review this requirement for accuracy
36	63A	5.5.1	29	1150-1152	Does automated bot detection and the other mitigation factors listed here apply to in-person id proofing interactions.	Review this section for its applicability to an in person identity proofing process.
37	63A	5.5.4	31	1190-1191	Only AAL3 would suffice to prove proof of possession of a credential with an IAL3	"Demonstrated association with a digital account through an AAL3 authentication or an AAL 3and FAL2 federation protocol"
38	63A	5.6	33	Table 1	Any AAL would suffice to prove proof of possession of a credential with an IAL1; Either AAL2 or AAL3 would suffice to prove proof of possession of a credential with an IAL2; Only AAL3 would suffice to prove proof of possession of a credential with an IAL3	Recommend updating Verification requirements for IAL1-3 in accordance with the above suggested changes.
39	63A	6.1	34	1241-1242	Editorial Comment	Remove final phrase as follows: ". . . establish a unique subscriber account for that subscriber following the successful identity proofing of an applicant.
40	63A	7	37	Table 2	Editorial comment	Third Row/Last column "credit cards" should be singular.
41	63A	8.1.1	40	1362-1364	Not sure why there is a Section 8.1.1, when there is no Section 8.1.2. Seems unnecessary to create this subsection. That said. . . The example given here concerning transmission/storage of SSN appears to be a non-sequitur. For validator to give a yes/no answer, the SSN would need to be communicated by the third party, which also means the third party would know/possibly store it.	Review/consider revising the example given here
42	63A	8.3	41	1404	"Consult your SAOP" would apply only to Federal agencies, not all CSPs are Federal agencies	Recommend revising this opening clause to state: "Federal agencies should consult their SAOP"
1	63B	2	3	368	"pseudonymous or non-pseudonymous" doesn't seem necessary here.	Recommend removing "pseudonymous or non-pseudonymous" and simply saying "an identifier".
2	63B	2	3	387-389	Isn't it true that IAL 1 only requires single factor, but there is no prohibition on using multifactor? This should be made plain here.	Recommend revising this sentence as follows: "AAL1 requires either single factor or multi-factor authentication using a wide range of available authentication technologies. Optionally, multi-factor authentication may also be used."
3	63B	2	4	393	Not sure why the term "two different authentication factors" is used here instead of multi-factor. Should it not be "at least two different authentication factors"? And on line 402 the term "two distinct authentication factors" is used. Why the difference in terminology?	Recommend reviewing/revising this sentence for accuracy and intent. At a minimum add "at least" before "two different authentication factors" And consider settling on a single term "different" or "distinct".
4	63B	4.1	6	442	Use of the term "some assurance" is vague. In the following section (4.2), AAL 2 is described as "high confidence", it seems to me that AAL1 should also be expressed in relation to confidence.	Revise this sentence to express AAL1 assurance in terms of confidence as follows: AAL1 provides some assurance a basic level of confidence that the claimant controls an authenticator bound to the subscriber account.
5	63B	4.1	6	443	See comment 53 above. AAL 1 requires a single factor authenticator, may use multifactor	Recommend revising this sentence as follows: "AAL1 requires either single-factor or multi-factor authentication. Multifactor authentication may also be implemented using a wide range of available authentication technologies
6	63B	4.2.2	9	523-524	"Authenticators procured by federal government agencies SHALL be validated to meet the requirements of [FIPS140] Level 1." A companion statement is needed to indicate that non-Federal organizations should meet an equivalent standard.	Add a sentence here that says: "Authenticators procured by non-federal organizations SHALL be validated to meet the requirements of [FIPS140] Level 1 or an equivalent standard."
7	63B	4.2.2	9	539-543	This entire paragraph is confusing. Federal agencies must offer phishing resistant authenticators but they're generally not required, only recommended? And encouraging use of phishing resistant authenticators by whom? Is this a subscriber decision? A relying party decision? Or both? How does a verifier encourage use since verification is after the fact?	Revise this paragraph for clarity. Perhaps require phishing-resistance.
8	63B	4.3.1	10	576-587	The Federal space is a unique one which, since the early 2000s, has utilized PKI technology to aid in federation of a single CAC throughout DOD and - in theory - throughout the Federal government. In draft NIST 800-63-4, NIST is suggesting to change AAL3 (previously reserved for PIV/CAC/other methods of PKI with a PIN) to include phishing-resistant authenticators that are combined with other form factors to create MFA. While the DMDC agrees that phishing-resistant MFAs should be rated high within authentication levels, it does not agree that phishing-resistant authenticators should be at the same authentication level as PCAC. In fact, draft 800-157r1 proves that PKI-based MFA must be treated differently than non-PKI MFA (e.g., the lifecycle management is vastly different and non-PKI authenticators can only be utilized locally). A user does not need to perform any additional steps after binding their PKI-based credential to their CMS to utilize that credential within their agency's systems. For a non-PKI authenticator to be used within an agency's systems, it must not only be bound to the agency CMS, but also to the individual IdPs that the user needs to authenticate to; additionally, the second factor to obtain AAL3 is bound to the IdP, not the authenticator. Similarly, if a user's PIV is terminated, the CMS can simultaneously revoke all PKI certificates that have been issued to the user - including those issued on mobile devices. The user would then be prevented from authenticating to the IdPs within the agency's network. However, if one of the user's derived PIVs was a non-PKI-based derived PIV, then the agency would be required to collect that phishing-resistant authenticator to ensure the prohibition of the user's unauthorized access to the network. While implementing joiner/mover/leaver principles within the agency's IdP would enable the agency to reduce the risk of unauthorized access, the best method would be to collect the authenticator. Because the only way to reach AAL3 with a non-PKI authenticator is with a single factor crytographic device and an additional factor that is bound to the IdP, not the authenticator, and because the only way to revoke a non-PKI authenticator is to collect it from the end user, non-PKI authenticators should not be in the same AAL as CACs in NIST 800-63B and in this document.	Recommend changes throughout the document: have the AALs to align more with the current draft IALs: Move AAL1 factors down to AAL0, as the factors currently in AAL1 allows for single factors, do not protect systems, and provide a false sense of security; change AAL2 factors to AAL1, as the factors currently in AAL2 allow for phishable MFA, which are not the most secure MFA option; change AAL2 to include all factors in AAL3 except for multifactor crytographic device, based on the comment and as some of those combinations of MFA would not realistically be adopted by end users (e.g., utilizing an OTP device ontop of a phishing resistant authenticator); and change AAL3 requirements to indicate that a multifactor cryptographic device is the only authenticator that meets AAL3. Thefore, the AALs would become: AAL0 (Single Factor Authenticators) •E.g. Look-Up Secret, Out-of-Band Device, Single-Factor OTP Device, Single-Factor Cryptographic Software, Single-Factor Cryptographic Device AAL1 (Phishable MFA) •Multi-Factor Out-of-Band Authenticator, •Multi-Factor OTP Device •Combination of two single-factor authenticators AAL2 (Phishing-Resistant MFA) •Single-Factor Cryptographic Device used in conjunction with a Memorized Secret •Single-Factor Cryptographic Software used in conjunction with a Memorized Secret •Multi-Factor Cryptographic Software Authenticator AAL3 (MFA Cyrptographic Device) •Multi-Factor Cryptographic Device
9	63B	4.3.1	10	577	Editorial comment	Review the following sentence: "AAL3 authentication SHALL occur by the use of one of a combination of authenticators satisfying the requirements in Sec. 4.3". I believe the 'of' here should be 'or'.
10	63B	4.5	13	Table 1	See comment above on AALs.	Change table to include: AAL0 (Single Factor Authenticators) •E.g. Look-Up Secret, Out-of-Band Device, Single-Factor OTP Device, Single-Factor Cryptographic Software, Single-Factor Cryptographic Device AAL1 (Phishable MFA) •Multi-Factor Out-of-Band Authenticator, •Multi-Factor OTP Device •Combination of two single-factor authenticators AAL2 (Phishing-Resistant MFA) •Single-Factor Cryptographic Device used in conjunction with a Memorized Secret •Single-Factor Cryptographic Software used in conjunction with a Memorized Secret •Multi-Factor Cryptographic Software Authenticator AAL3 (MFA Cyrptographic Device) •Multi-Factor Cryptographic Device
11	63B	5.1.3.1	21	875	Editorial comment	The word 'the' does not belong here: ". . . rather than by the presenting a secret that the claimant transfers. . ."

12	63B	5.1.5.2	26	1050	Editorial comment	The word 'authenticator' is misspelled
13	63B	5.2.2	31	1234-1235	100 failed consecutive attempts seems excessive.	Recommend some explanation/rationale for allowing 100 consecutive failed attempts.
14	63B	5.2.10	38	1461-1463	Why allow the use of restricted authenticators at all? Or is this a way of allowing use of previously issued authenticators until such time as they can be replaced.	Please clarify the intent of allowing use of restricted authenticators and the circumstances.
15	63B	6.1	41	1571-1573	What does throttling have to do with Binding? Seems throttling is more about use of an authenticator than binding the authenticator to my subscriber account.	Review/revise/explain this statement as appropriate.
16	63B	6.1	42	1593-1594	the statement "and to attempt to determine that the endpoint and authenticator are free from malware" introduces a great deal of uncertainty "attempt to determine"?	Recommend removing 'attempt' from this statement or removing this final clause.
17	63B	6.1.2.4	44-45	1696-1698	This is a very long runon sentence that is hard to read.	Recommend revising for clarity/readability as follows: The binding process MAY begin with a request from Once an endpoint that has authenticated to the CSP and obtaininged a binding code from the CSP, that is input into the endpoint associated with the new authenticator and sent to that CSP.T the binding process MAY begin.
18	63B	6.4	47	1793-1795	While the surrender of authenticators is laudable. Fraudulent or deceased subscribers won't participate. What does it mean for a subscriber to "certify destruction"? There seems to be a lot of room for error here. CSPs could burn a lot of cycles chasing down subscribers to ensure this requirement is met. If these are in the hands of the subscriber and the subscriber has been adequately informed concerning PII associated then it seems that should be sufficient.	Consider reviewing/revising this requirement to ensure its viability. Could this be a "SHOULD"?
19	63B	7.2	50	1891	"Prior to session expiration, the reauthentication time limit SHALL be extended by prompting the subscriber for the authentication factors specified in Table 2." This statement is confusing. What is the 'reauthentication time limit'? Is this following termination? Or can it prevent termination? If so, is it contradictory?	Review/revise for clarity.
20	63B	7.2.1	51	1898	Not sure why there is a Section 7.2.1, when there is no Section 7.2.2. Seems unnecessary to create this subsection. It can just as easily be included in the superior section 7.2. That said. . . The title of this subsection is "Reauthentication from a Federation or Assertion", however it only describes reauthentication in the context of a Federation through the use of an asssertion. Seems the 'or' in the title is misleading	Consider revising the document to remove subsections that are 'only children'. Also review this header for its relationship to the following text and whether it is an accurate representation.
21	63B	11	75	2477-2479	"This inequity can be addressed by making inexpensive authenticators such as look-up secrets (see Sec. 5.1.2) available for use in the event of a primary authenticator failure or loss". Inexpensive authenticators such as look up secrets could very well lower the AAL. Seems there should be some mention of AAL equivalence here.	Review/revise this statement/example for its effect on the subscriber's ability to conduct the business intended.
1	63C	2	3	356	The term "single sign on" does not appear in the Definitions and Abbreviations section of the -63 Base document	Recommend adding "single sign on" definition to -63 Base.
2	63C	4	6	441-442	"This can be traced back to a static agreement between the parties or occur implicitly from the connection itself." This is confusing. If this is describing a 'dyamic' agreement, why not use that term?	Check word usage. Should 'occur' be "inferred"? If 'implicitly' is replaced with 'dynamically', the word 'occur' works here.
3	63C	4.1	8	485	"In existing federation protocols. . ." Not sure the intent of this. Does it mean the federation protocols that exist today? Is it necessary? In this dynamic world, a new protocol could pop up by the time this document is signed, or immediately thereafter. Could it just be "For example. . ."	Recommend the opening of this paragraph is revised to remove the phrase "In existing federation protocols"
4	63C	4.2	8-9	493-515	The word "also" is unnecessary here. The statement has already been made that these are additional requirements. Nor do following paragraphs contain 'also'. Could this section benefit by placing bullets at the beginning of each new requirement? Seems the first two paragraphs are related, while the third & fourth paragraphs are distinct requirements. Does each new requirement need to start with "At FAL2"? Again already stated.	Remove "also" from line 493. Replace "being injected" with "injection" (readability). Consider placing bullets at the beginning of lines 493, 505, and 513 and removing "At FAL2" from each of these paragraphs. And on Line 506 replace "limits of" with "limits on".
5	63C	4.3	9	519-539	Could this section benefit from placing bullets at the beginning of each new requirement? Does each new requirement need to start with "At FAL3"?	Consider placing bullets at the beginnin of lines 519, 531, and 538 and removing "at FAL3" from each of these paragraphs.
6	63C	5.1	13	622	Does this mean that subscribers are not considered members of the Federation? It would seem that the Federation is comprised of IDPs, RPs and Subscribers, so IDPs need trust agreements with both RPs and subscribers and RPs need trust agreements with IDPs and subscribers that access RP resources. This is especially true if subscribers are sponsored by an affiliated organization (employer, etc.).	Review this statement for accuracy. Consider including subscribers.
7	63C	5.1	14	646	Editorial comment	Replace 'are' with 'is'
8	63C	5.1.2	16	Fig.2	On lines 706-707, it states "In this model, the federation authority manages the membership of IdPs and RPs in the federation agreement." However, Figure 2 seems to suggest that Federation Authority oversight is limited to the IDPs.	Recommend revising the Figure to show that RPs can also fail to meet a Federation's requirements.
9	63C	5.1.3	18	753	Editorial comment	The word 'federation' on this line should be 'proxy'. It is the 'proxy' that is being discussed here.
10	63C	5.1.3	18	798	Recognizing "well-known location" is a term of art, it should be defined and/or explained.	Recommend adding "well-known location" to the Definitions and Abbreviations in the -63 base document.
11	63C	5.3	19	823	Construction of this section and its subsections is messy. Reorganization around topic area (allowlist, blocklist, runtime decision) would make it flow better.	Suggest a subsection of Allow Lists with additional sub-sub sections on IDP/RP allowlists (unless they could adequately discussed in a single sub section). Ditto Block Lists. Ditto Run-Time Decisions.
12	63C	5.3	19	835-840	The trust agreement between IDPs and RPs and the runtime decision of the subscriber are not either/or decisions. Regardless of whether there is an existing trust agreement or that trust agreement is being established dynamically, the subscriber still makes a run-time decision. This language appears to contradict that notion. Also, the term 'authorized party' used here is confusing. IDPs are the 'authorized party' for the attributes released iaw with trust agreement, but the subscriber (or representative of the subscriber) is the 'authorized party' for the run-time decision.	Revise this paragraph to make it clear that trust agreements/allowlists/blocklists do not override subscriber run-time decisions. This should not say 'when the authorized party is the subscriber', it should say 'for run-time decisions'
13	63C	5.3	19	836	Back in Section 5.1 line 662, the word organization was introduced as an alternative to IDP. In addition, enterprise service was introduced as an alternative to RP. Not sure why as this does not add value and could be confusing. Here, the term 'RP' is used along with the term 'organization'. This is confusing. The document should be consistent. Readers understand IDP, it is used in all of the other -63 documents, why suddenly start referring to it as 'organization'?	Replace use of 'organization' as a substitute for 'IDP' with 'IDP' throughout the document.
14	63C	5.3.3	22	872-878	This is a confusing paragraph. If an RP were on a blocklist with the IDP, that would seem to negate any trust relationship. This should begin by explaining that it is the subscriber's run time decision concerning release of attributes regardless of any static or dynamic agreement.	Review/revise for clarity. Use language that parallels previous references to runtime decisions. For example lines 835-840, which reference this paragraph, but this paragraph should also reference back to the statement there. Concerning the blocklist, recommend adding language to 5.3.2 similar to that in Section 5.3.5 concerning operating under the same federation authority.
15	63C	5.4	24	957-959	This final sentence is confusing. Not sure it is in context with the rest of this paragraph. An established, enduring subscriber account at the RP would be authenticated once established and used, and wouldn't be unauthenticated just because the subscriber logged out. It is only the session that is being terminated, not the subscriber account as is discussed in earlier paragraphs.	Review/revise for clarity.

16	63C	5.4.1	26	984-986	"The RP also collects attributes about users who have not interacted with the RP system yet, which can cause privacy issues." Not sure why this sentence is here. All information stored at the RP could cause privacy issues, regardless of whether the subscriber has initiated a transaction with the RP, so why single this out? If this needs to be addressed, it should have its own paragraph and not just be tossed in here without explanation.	Remove this sentence.
17	63C	5.4.2	27	1010-1011	Editorial comment	On line 1010 insert "IDP" before subscriber account (both RP and IDP have subscriber accounts). On line 1011, remove "with".
18	63C	5.4.2	28	1026-1028	This seems overly onerus on the subscriber. If the subscriber decides to change IDPs, the entire relationship with the RP may need to be reestablished. Or is this only referring to the data related to accessing the RP	Clarify what is being erased here.
19	63C		28	1049	This is confusing: "A provisioning API SHALL NOT be made available under a dynamic or implicit trust agreement." Aren't "dynamic" and "implicit" two terms for the same thing? None of these terms are in the Definitions in -63 Base document.	Settle on one term and keep using it. Dynamic?
20	63C	5.4.3	29	1061	Earlier in the document, IDP notification to the RP is a SHOULD. Here it says if an API is used it is a SHALL. This is contradictory and can be confusing. People don't read these documents cover to cover, they reference them and if it says two different things in two different locations, the right answer might be missed. Also, is the IDP required to provide the reason for termination? Seems that might make a difference.	Revise the paragraph beginning on line 1022 to include this exception case. Consider ramifications of requiring a reason code.
21	63C	5.4.5	29	1079-1085	There is a difference between not accessible and not used. This opening sentence doesn't relate to the discussion in the rest of paragraph about orphan accounts that haven't been accessed in awhile. In addition, the last sentence of this paragraph can also be problematic for users of government services where interaction may be spotty, maybe once annually or even less, but the user wants to maintain the account and finds themselves having to go through initial registration all over again because it has been a year since last access. The 120 day example is not realistic for many interactions with Federal applications but could get widespread adoption simply because it is in this document.	Review/revise this paragraph for clarity. Also consider not giving a 120 day period of inactivity example.
22	63C	5.5	30	1112	Editorial comment	Insert "IDP" in front of subscriber account.
23	63C	5.5	31	1143	What does "given the wide nature of information access" mean in this context. Is this suggesting that access to an API = a wide nature of information access? There are already requirements to limit access based on trust agreements and subscriber runtime decisions.	Review/revise this paragraph for clarity.
24	63C	5.5	31	1146-1149	Simply because a user is authorized to use an RP doesn't mean they will. So this is not a logical conclusion.	Review/revise for clarity.
25	63C	5.6	32	1178-1186	What does "along with an assertion" mean in this context? Also concluding sentence is confusing, does not seem to be supported by the rest of the paragraph.	Review/revise this paragraph for clarity. Consider using shorter sentences and more punctuation.
26	63C	6	35	1256	Why is this #1 when there is no #2?	Recommend making this a paragraph.
27	63C	6	35	1263-1265	This appears to contradict the statement in line 1230. If the list above is conditional that should be made clear. Passing the AAL should be made mandatory.	Consider adding "where applicable" to the intro statement on line 1230.
28	63C	6	35	1280	Not sure what "along with the "assertion" is intended to mean here. Could it be that the RP may be given access to the identity API at the time it receives the assertion from the IDP? If so, it should say that.	Consider revising this section for clarity
29	63C	6.1.1	36	1306	800-63 Base document defines a Bearer Assertion as "The assertion a party presents as proof of identity, where possession of the assertion itself is sufficient proof of identity for the assertion bearer." This is not helpful. In Section 4 (line 447) a bearer assertion is contrasted with a bound authenticator. It is not clear that the subscriber will be the one presenting the bearer assertion. Most certainly the subscriber will present the bound authenticator. Recommend additional introductory text here to make it clear what a bearer assertion is, who presents it, where it gets its authority, etc.	Review/revise to add more information concerning bearer assertions.
30	63C	6.1.2	36	1318	Should mention that Bound Authenticators are required only at FAL3. Optional at other FALs.	Add a statement at the beginning of 6.1.2 that Bound assertions are required at FAL3.
31	63C	6.1.2.2	40	1370	"The administrator of the RP SHALL determine through independent means that the party to which the authenticator is issued is the identified subject. . ." So in the event that the RP provides the bound authenticator, they use 'independent means' (not defined) to establish identity. Seems like a punt and puts the RP in the role of CSP. Nor is it mentioned that this bound authenticator's 'independent means' must meet the criteria SP 800-63A. If this is supposed to deter an AitM, it might be said that weak identity proofing at the RP will aid AitM.	Revise the sentence starting on line 1370 to state that "the administrator of the RP SHALL determine through independent means, in accordance with SP 800-63A, that the party to which the authenicator is issued is the identified subject of the RP subscriber account.
32	63C	6.1.2.2	40	1395-1401	Not sure it is clear what the real-world application of this paragraph is. Unless it is accounting for a situation in which a fraudulent user has active FAL3 sessions when the authorized subscriber realizes their bound authenticator has been compromised. Otherwise, it would be unlikely that a subscriber would unbind a bound assertion in the middle of an RP session.	Provide some clarification of this scenario.
33	63C	6.2.3	43	1461	Is assertion encryption mandatory? Only in certain scenarios/FALs? Should lead with that	Revise to indicate whether and/or when assertion encryption is mandatory. Or lead into the section with the sentence beginning on line 1468.
34	63C	6.2.5.1	44	1501	Editorial comment	Remove the two instances of "itself" from this line.
35	63C	6.2.5.2	45	1519	Since this is an exception case, should make that clear by juxtaposing "however" against "normally"	Insert "however" at the beginning of the 2nd sentence: "However, an IDP MAY generate. . ."
36	63C	6.3	46	1569	Gives a scenario for an API hosted by the IDP, but does not give a scenario if that is not the case.	Review/revise to indicate requirements (or lack thereof) when the API is not hosted by the IDP.
37	63C	6.3.1	46	1575	Why a 6.3.1 if there's no 6.3.2?	Suggest either two subsections (IDP hosted attribute provider and independent attribute provider) or none.
38	63C	6.3.1	46	1580	Editorial comment	Insert "external" before "attribute provider"
39	63C	7.1	48	1619	This should make provision for a "family of RPs" as discussed previously	Add "or family of RPs" to #1
40	63C	7.1	48	1621	What constitutes "a small number of minutes"? Very subjective. Where is calculating the"small" number explained?	Consider revising this statement to make it less ephemeral.
41	63C	7.2	51-52	1656-1670	This seems very pejorative. It gives the reasons not to do Front Channel, but doesn't identify itself as the drawbacks to front channel. It would also be neater to identify the drawbacks last, not right under the diagram. In fact, narrative that describes the front channel process (as is seen for back channel in 7.1) seems to be missing.	The description of what is going on in the diagram above should be inserted here. These two paragraphs should be prefaced with language such as "Drawbacks to front channel communication include" or words to that effect. They should also be at the end of the section, so the requirements below don't get missed.
42	63C	12	69-71		NIST breifly discusses some vunerabilities in the assertion technology section, however the discussion is not in depth enough to give a clear picture of why those vunerabilities matter to organizations accepting assertions.	Recommend either going in depth and exploring all the known vunerabilities for each of the technologies, or mention briefly in the opening paragraph that each technology contains known vunerabilities, and organizations should evaluate them to determine the amount of risk they want to take when accepting federated assertions.
43	63C	General	Genera	General	For federal employees using a HSPD-12 PIV or Derived PIV, the document lack the specific PIV identifiers that Federated IDP or Identity APIs must make available (i.e., GUID, CHUID).	Recommend requiring GUID or CHUID of Federal PIVs or Derived PIVs be made availabe in federation and Identity APIs for all federated identify and authentication transactions. This will allow the RP and IDP to understand the claiments affiliation with a federal agency and a unique idnetifeir.