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:	IRS
Name of Submitter/POC:	Varun Lal
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	N/A	N/A	N/A	N/A	NIST should develop a shared responsibility model - responsibilites of CSP vs the agency RP	Create a shared responsibility model (CSP responsibilities vs. agency RP)
2	N/A	N/A	N/A	N/A	Agencies can benefit with guidance from NIST on standardized practices for multi-CSP environment (where an agency is using multiple CSPs). How should compliance look? How should agencies handle users with multiple credentials?	Provide additional guidance on best practices for a multi-CSP environment. Details should include compliance and how to handle a user with multiple credentials.
3	Base	N/A	N/A	N/A	The identity technology market has not been able to keep up with the requirements in NIST 800-63-3.	NIST should consider the state of the market capabilities and design requirements around those abilities, at least at the lower assurance levels, rather than seek to drive the market to create compliant products.
4	Base	Note to Reviewers	ii	149	The second to last word on line 149 "Identify" is misspelled.	Update 'identify' to 'identity'
5	Base	5.1.3 Identify Potential Impact Levels	28	1100	Impact Category label missing.	Missing "Loss of sensitive information"
6	Base	5.1.3 Identify Potential Impact Levels	28	1101 - 1109	The section "Damage to trust and reputation" has two sets of Low, Moderate, High examples, with the second set having reference to [FIPS199]. Was this a mistake in leaving this set in the base document? If not, why doesn't the other impact categories have examples with reference to [FIPS199]?	Clarify if lines 1101-1109 are a different section than lines 1093-1099.
7	Base	N/A	N/A	N/A	Why are the xAL diagrams removed from Rev. 4? NIST 800-63-3 has Figures 6-1 Selecting IAL; Figure 6-2 Selecting AAL; and Figure 6-3 Selecting FAL. In Rev. 3 base volume, there is guidance (via a diagram) on selecting xALs; this is found in Section 6 - Selecting Assurance Levels (p.27, p.30, p.32). In Rev. 4, the diagrams are moved.	Include diagrams in NIST SP 800-63-4?
8	Base	5.2.2.1. Identity Assurance Level	31	1198	IAL0 is not listed with its definition.	Add IAL0 and definition for quick access instead of only being referred to in 63A
9	Base	5.2.2.2 Authentication Assurance Level	31	1213	Line 1213 reads, Proof of possession and control of two different authentication factors. Why not just state MFA instead of '2 different authenticators'.	Replace '2 different authenticators' with Multi-Factor Authentication (MFA)?
10	Base	5.1 Conduct Initial Impact Assessment	24	965 - 1169	Lack of understanding for this section, please clarify: •Is this section supposed to tell agencies how to perform the initial impact assessments? There are no defined steps to perform the analysis of the Impact categories against the xALs and how to determine the level needed to avoid the risk of identity proofing, authentication, or federation. •Is the Initial Impact Assessment process designed to replace the Impact Category section that was in the Decision Trees? •Table1 makes no sense on how you can use it to determine the levels (low, moderate, high) and there is no explanation on if when combining the Impact Levels do you use High Water mark method?	Section 5.1 is lacking some guidance on how to perform the four steps listed. Can some guidance on how to perform the analysis or defined processes be added?
11	Base	Note to Reviewers	ii	145	Public perception of biometric technology is causing heated debates. (Note: Similar language appears in all volumes.)	Suggest direct engagement with the controversy by including a description of biometrics, its use as a tool, and the importance of agency decisions in managing the risks (both technologically and reputationally) in using this tool.
12	Base	2.3.2 Privacy	8	542	The language states that the Privacy Act established a set of fair information practices. The recommendation is to update the statement to include the actual history of the Privacy Act.	Suggest correcting language to match the actual history of the act: The Privacy act was built on a set of fair information practices…
13	Base	5.1.4 Impact Analysis	29	1158	The process of authenticating and passing the authentication attributes bears similar risk of over-collection of data to the identity proofing process.	Suggest including an analysis of the use of excessive information in Authentication, similar to the third bullet in Identity Proofing.
14	Base	5.2.1 Assurance Levels	31	1180	Organizations should consider all potential risks when determing assurance levels.	Suggest removing the exclusive "cybersecurity" from the sentence "based on cybersecurity risk and mission needs."
15	Base	5.2.3 Initial Assurance Level Selection	32	1238	The initial selection of assurance levels must consider all angles of risk.	Suggest removing the exclusive "cybersecurity" from the sentence "These initial selections are primarily based on cybersecurity risk, but will be tailored"
16	Base	N/A	N/A	N/A	Agencies can benefit if NIST can provide separate guidance on CSP strategy and additional information what CSPs could obtain for better fraud management.	Provide separate guidance on CSP strategy and additional information what CSPs could obtain for better fraud management.
17	Base	5.5 Cyber, Fraud, and Identity Program Integrity	39	1493, 1497	Both lines are written as SHOULD statements. The recommendation is to change both statements from SHOULD to SHALL.	Replace "SHOULD" with "SHALL"
18	Base	4.3.3 Authentication Process	19	N/A	Guidance is needed regarding allowing multiple subscriber accounts to the same authenticator (e.g., many subscriber accounts with the same SMS MFA).	N/A
19	Base	5.4 Continuously Evaluate & Improve	39	1479 & 1481	The Continuous Evaluation and Improve section contains two SHOULDs which seem insufficient given the number and variety of threat actors and their continuously evolving capabilities. In order to ensure a robust risk management framework, consider changing the two SHOULDs to SHALLs.	Replace "SHOULD" with "SHALL"
20	63C	N/A	N/A	N/A	Agencies would benefit from more guidance around how to manage accounts across multiple CSPs.	Provide more guidance around how to manage accounts across multiple CSPs. For instance, guidance on how to implement a reciprocity schema or how to securely associate new credentials to an existing account that was proofed by another entity.
21	63C	4 Federation Assurance Level (FAL)	6	439, 442	The IdP and RP have agreed to participate in a federation transaction with each other for the purposes of logging in the subscriber to the RP. This can be traced back to a static agreement between the parties or occur implicitly from the connection itself.	What information must the static agreement betwwen the IdP and RP have?
22	63C	4 Federation Assurance Level (FAL)	7	Table 1 - FALs	There are multiple questions around Table 1, which references Dynamic and Static for Trusted Agreement & Registration •What is the difference for the use of Static & Dynamic in the Trust Agreement versus the Registration? •Under the Registration column of Table 1, is the use of Static or Dynamic related to Knowledge Based Authentication (KBA)? •If the use of Static or Dynamic for Registration are intended for KBA, why would Static be used on all three and Dynamic used on FAL1 and 2 only when Dynamic is more stringent? •Why isn't Enhanced Dynamic KBA considered? •Should definitions for Static and Dynamic (as it relates to KBA) be included in Appendix A of NIST 800-63-4 (Base)?	Provide more clarity/context on this statement.

23	63C	Assurance Level 2 (FAL2)	9	514, 539	Confirm correct FIPS 140 reference; should it be FIPS140 or FIPS140-3	Update reference to FIPS140-3 if needed
24	63C	4.4. Requesting and Processing xALS	10	556-560	Further explain "IdP may indicate no claim is made to IAL or AAL for given federation transaction." How would there be "no IAL?"	Clairify what this paragraph means by IdP may indicate no claim is made to IAL or AAL for given federation transaction.
25	63C	4.1. FAL1, 4.2. FAL2, 4.3. FAL3, 4.4 Requestion and Processing xALs	7--11	463-587	Each section provides lengthy in depth detail about assertion requirements and recommendations for each of the FAL levels.	Create a process flow to visualize how scores are processed for better understanding if possible.
26	63C	N/A	N/A	N/A	There are no longer decision trees for FAL	Add in the decision trees or additonal guidance about how to select the correct FAL level under given circumstances
27	63C	5.1 Trust Agreements	14	642	Data minimization is a key privacy consideration in this aspect of the relationship. There should be more emphasis on the importance of data minimization.	Emphasize importance of data minimization, with language such as: The RP and IdP SHALL organize their data exchange agreements to ensure only they exchange only the minimum data necessary to achieve mission needs, maintain security and prevent fraud. These data elements SHALL be reviewed periodically to avoid over-collection or unnecessary exchange of data.
28	63C	5.5 Privacy Requirements	30	1109-1111	Commercial organizations have historically chosen to implement their consent basis in an "opt-out" model that defaults to users sharing data, whether they specifically choose to do so or not. A better privacy model is to implement an "opt-in" model, where user data is not used, unless specifically approved.	Add language to the paragraph such as: When building consent measures, the IdP SHOULD utilize an "opt-in" model that defaults users to a state where their data is not used for any other service unless they choose to allow it.
29	63B	4.1.2 Authenticator & Verifier Requirements 5.1.1.2 Memorized Secret Verifiers 5.2.12 Connected Authenticators 6.1 Authenticator Binding	N/A	N/A	Is an adversary-in-the-middle (AitM) considered the same as a man-in-the-middle attack (MitM)? V4 removed any reference to MitM and added AitM.	N/A
30	63B	4. Authentication Assurance Levels	6	434	Line 434 states, [FIPS140] requirements are satisfied by FIPS 140-3 or new versions. Is FIPS 140-3 or higher revisions the minimum FIPS 140 that is to be implemented?	Update to FIPS140-3 if needed
31	63B	4.1.2 Authenticator and Verifier Requirements	7	469	Confirm correct FIPS 140 reference; should it be FIPS140 or FIPS140-3	Update to FIPS140-3 if needed
32	63B	4.2.2 Authenticator and Verifier Requirements	9	524, 535	Confirm correct FIPS 140 reference; should it be FIPS140 or FIPS140-3	Update to FIPS140-3 if needed
33	63B	4.3.2 Authenticator and Verifier Requirements	11	597, 599, 600	Confirm correct FIPS 140 reference; should it be FIPS140 or FIPS140-3	Update to FIPS140-3 if needed
34	63B	Table 1 AAL Summary of Requirements	13	Table 1, 2nd Row	Confirm correct FIPS 140 reference; should it be FIPS140 or FIPS140-3	Update to FIPS140-3 if needed
35	63B	5.1.7.1 Single-Factor Cryptographic Device Authenticators	28	1119	Confirm correct FIPS 140 reference; should it be FIPS140 or FIPS140-3	Update to FIPS140-3 if needed
36	63B	5.1.9.1 Multi-Factor Crypotographic Device Authenticators	30	1206	Confirm correct FIPS 140 reference; should it be FIPS140 or FIPS140-3	Update to FIPS140-3 if needed
37	63B	4.5. Summary of Requirements	13	Table 1 - AAL Summary of Requirements	Table 1 AAL Summary of Requirements does not list Records Rention Policy or Privacy although required at all levels. Why was it removed from the table when it allows for easier understanding of AAL requirements at a glance?	Add Records Retention Policy and Policy back into AAL Summary of Requirements table
38	63B	4.4 Privacy Requirements	12	653	The e-Gov Act requires a privacy impact assessment on "informatin technology" that processes information in identifiable form.	Suggest a change to the wording on the requirement for a PIA that more closely aligns to the e-Gov Act requirements.
39	63B	9.2 Privacy Controls	59	2002	Privacy is important throughout the full lifecycle of the data, as mentioned in the current draft. Much of the requirements are covered in the 63 Base and 63A. With appreciation for the continued inclusion of privacy in 63B, there are some other key privacy controls worth mentioning in this context.	Update the sentence to read, "These controls cover notices, redress, role-based training, and other important considerations for successful and trustworthy deployments."
40	63B	5.2.3 Use of Biometrics	32	1255	The use of biometrics is an especially sensitive topic. In order for individuals to properly consent to its use there must be clear notification of its collection, purpose, use and security.	Include a requirement that the CSP SHALL provide clear notice concerning the collection, use, purpose and options when applying biometrics as an authentication factor.
41	63B	7.1.1 Browser Cookies	49	1865	OMB M 10-22 includes requirements for notification of the use of cookies on a government website. Recommend including OMB M-10-22 reference.	Include reference to OMB M-10-22, "Guidance for Online Use of Web Measurement and Customization Technologies."
42	63B	5.2.3 Use of Biometrics	32	953 (63A) & 1283 (63B)	63A says in 5.1.8 #2: When collecting and comparing biometrics remotely, the CSP SHALL implement liveness detection capabilities to confirm the genuine presence of a live human being and to mitigate spoofing and impersonation attempts. However, 63B says in 5.2.3: The biometric system SHOULD implement presentation attack detection (PAD). These two sections appear to be inconsistent in approach. Shouldn't both be SHALL statements?	Replace "SHOULD" with "SHALL"
43	63A	N/A	N/A	N/A	Maybe more emphasis on identity governance? Things like account maintenance, ability to change permissions, etc. This could be more on the 53 side but could be handy in a zero trust approach.	N/A
44	63A	4.3.4.1 Evidence Validation	N/A	N/A	How would a CSP operator confirm evidence is not counterfeit and not tampered with?	N/A
45	63A	4.3.4.4 Validation Sources	13	636-654	Can you provide examples of each of the source bullet points in this section? Who would be an original source of a First Name/Last Name or Address?	Provide examples of each of the source bullet points.
46	63A	5.1.7 Requirements for Notifications of Identity Proofing	22	895-897	Why is there from SHALL to SHOULD for sending notifications of proofing and enrollment codes to different validated addresses?	Provide more clarity/context on this statement.
47	63A	5.3.3 Evidence and Core Attributes Validation Requirements	27	N/A	In remote identity proofing of IAL1, how would the CSP validate the genuineness of each piece of FAIR evidence by visual inspection by trained personnel in real life workflows? What if an MNO record or credit report accessed by a Phone Number/SSN is used?	N/A
48	63A	6.3 Subscriber Account Lifecycle	35	N/A	Is there any guidance for notification of Subscriber Account Termination by the CSPs?	N/A
49	63A	5.4.2.1 Evidence Collection	28	1105	In the list of Evidence collection, to be more clear and to match Section 5.3.2.1, suggest adding ", or" after 1. One piece of SUPERIOR EVIDENCE. The section would then read as "1. One piece of SUPERIOR evidence, or 2. One piece of STRONG evidence and one piece of FAIR evidence"	Suggest adding ", or" after number 1

50	63A	2.2 Identity Assurance Levels 5.1.9.1 Requirements for Trusted Referees	4 (Section 2.2) 24 (Section 5.1.9.1)	420-421 (Section 2.2) 994-995 (Section 5.1.9.1)	Under Section 2.2 Lines 420 and 421 it states for IAL3 "via a supervised remote identity proofing session", however, in section 5.1.9.1 requirements for Trusted Referees on line 995 it only lists IALs 1 and 2. The supervised remote identity proofing session statement for IAL3 would support the use of a Trusted Referee for remote identity proofing for IALs 1, 2, and 3. A Direct to Virtual-in-Person (VIP) process with a Trusted Referee should be able to support the ID Proofing process even at IAL3.	Recommend changing line 995 to "proofing at all IALs."
51	63A	2.2. Identity Assurance Levels	4	408	Added new IAL0 level where there is no requirement to link the applicant to real life identity (neither validated or verified). How does this impact existing applications at the different IAL levels? Does this mean the level is downgraded by one (e.g., from IAL1 to IAL0)	Clarify what this might mean for existing applications at IAL1 and IAL2.
52	63A	5.6. Summary of Requirements	33	Table 1 - IAL Requirements Summary	There are multiple questions regarding Table 1 for IAL Requirements Summary. Given that IAL1 and IAL2 are the same, •If IAL2 requires "stronger evidence and a more rigorous process," why is the evidence required the same for IAL1 and IAL2? •Why was the option of 2 pieces STRONG, or 1 STRONG plus 2 FAIR removed that were previously listed for IAL2 in Rev 3?	Explain reasoning
53	63A	1 Purpose	2	361	Identity proofing may be required for a variety of interactions with individuals. This document currently only specifically identifies online and telephone interactions. Recommendation is to include language that 800-63 series does not include ID-proofing requirements for written or faxed correspondence.	Suggest adding that the 800-63 series does not include ID-proofing requirements for written or faxed correspondence.
54	63A	2 Introduction	3	390	Privacy controls are not optional. They should be noted as "Normative."	Update privacy to "Normative"
55	63A	Validation, and Verification	6	427	Editorial. The current revision says "This section provides and overview…"	Correct spelling, the statement should read: "This section provides an overview…."
56	63A	4.1 Identity Proofing and Enrollment	7	463	This section outlines expectations for collecting information from applicants, including describing what information must be presented.	Provide guidance to RPs to notify applicants of available choices concerning CSPs, identity document requirements, and related privacy notices.
57	63A	4.1.1 Process Flow	8	467	This is a good example of the process, but comes before the context being analyzed.	Move the example to a point in the document after the definitions immediately below it, so that the example can include an analysis of how well it meets those definitions.
58	63A	4.2 Identity Resolution	9	491	The statement sets the expectation to use the smallest set of attributes possible.	Add context as to why that matters. Include an explanation that, by collecting only the minimum amount of data, there is less risk to the applicant and less overhead for the CSP/RP related to storing and protecting unnecessary information. There may be other worthwhile reasons to notate.
59	63A	4.3.1 Characteristics of Acceptable Physical Evidence	9	516	An informed applicant can help streamline the process and minimize burden for all and contributes to better overall privacy protections.	Suggest adding a "should" statement for CSPs to describe what is being collected, why, and how to meet the expected evidence requirements, in an order to support a well-informed applicant.
60	63A	4.3.4.4 Validation Sources	14	653	It's important that vendors, contractors and sub-contractors protect data to acceptable standards and that individuals are informed regarding who has access to their information.	Suggest adding guidance that CSPs/RPs "shall" ensure data protections, including all applicable security and privacy controls, are met by any vendor or their tertiary service providers.
61	63A	5.1.1 Identity Service Documentation and Records	16	720	The e-Gov Act requires government agencies to publish privacy impact assessments, with limited exceptions. CSPs should be expected to support the government PIA, if not contribute directly to it.	Suggest adding guidance about CSP support for PIAs, possibly as a best practice.
62	63A	5.1.1.1 Ceasing Operations	17	725	Businesses often cease to exist for a variety of reasons. A common reason is being bought out and rolled into another company.	Suggest adding clarity that the "Ceasing Operations" includes any and all cessations, transfers, reorganizations, recharacterizations or other changes to business organization or ownership.
63	63A	5.1.1.2 Fraud Mitigation Measures	17	739	An important element of privacy risk mitigation is notifying individuals about how their information is used.	Suggest adding guidance that CSPS should notify individuals about the use of their information, including fraud mitigation measures. This does not mean exposing specific tactics to the public, but the simple awareness that information they provide may be used to prevent fraud.
64	63A	5.1.2.2 Additional Privacy Protective Measures 5.5.8 Requirements for	18 (Section 5.1.2.2) 32 (Section 5.5.8)	773 (Section 5.1.2.2) 1225 (Section 5.5.8)	Privacy and security role-based training is critical for an effective workforce.	Suggest adding guidance that CSPs "shall" provide privacy training to employees, contractors, sub-contractors, in conjunction with requirements by the RP. The training "shall" apply to any member of the company or a tertiary service provider who has access to any sensitive information in the conveyance of the contract.
65	63A	5.1.5 Additional Requirements for Federal Agencies	20	842	The e-Gov Act requires a privacy impact assessment on "informatin technology" that processes information in identifiable form.	Suggest a change to the wording on the requirement for a PIA that more closely aligns to the e-Gov Act requirements.
66	63A	5.1.9.2 Requirements for Applicant References	25	1009	Applicant referees are entitled to the same privacy and security protections as the individuals they are assisting in meeting identity proofing requirements.	Recommend further explination, such as CSPs shall ensure that privacy and security training for employees, especially Trusted Referees, includes an understanding of the need to protect information about the Applicant References as securely as information about the applicant.
67	63A	5.3.3 Evidence and Core Attributes Validation Requirements	27	1076	Data must be protected throughout its lifecycle, including when being processed by a vendor.	This is another section that should include additional clarification and emphasis on the requirement to ensure privacy and security protections in sub-contractor or tertiary service provider systems.
68	63A	5.5.3.2 Core Attribute Validation Requirements	30	1182	Data must be protected throughout its lifecycle, including when being processed by a vendor.	This is another section that should include additional clarification and emphasis on the requirement to ensure privacy and security protections in sub-contractor or tertiary service provider systems.
69	63A	7.1 Threat Mitigation Strategies	38	Table 3 Row 5 (Social Engineering)	Social engineering has become a prevalent attack technique.	Suggest additional detail on how to identify and prevent social engineering attacks.
70	63A	6.3 Subscriber Account Lifecycle	35	N/A	Agencies can benefit if NIST can provide additional details/stepsframework on subsriber account life cycle management - standardized across all CSPs.	Provide additional details/stepsframework on subsriber account life cycle management - standardized across all CSPs.
71	63A	6.3 Subscriber Account Lifecycle	35	N/A	Can OMB/DHS/GSA establish standard framework for CSPs (like a framework) for digital identity and thus be the certifying entity for CSPs? Agencies can benefit from Federal standaridzed requirements (framework) for CSPs.	Establish standard framework for CSPs (like a framework) for digital identity and thus be the certifying entity for CSPs? Agencies can benefit from Federal standaridzed requirements (framework) for CSPs.
72	63A	5.1.9.1 Requirements for Trusted Referees	24	993	Providing Trusted Referees (Sec. 5.1.9.1) explains the CSP shall train its trusted referee to make risk-based decisions based on the specific applicant circumstances". Agencies may benefit if NIST can provide specific guidance and details on criteria and what entails "risk-based decsion".	The recommendation is to provide specific guidance and details on criteria and what entails "risk-based decsion".
73	63A	6.3.2 Subscriber Account Termination	35	1292	*Based on the below statement, agencies will benefit if NIST/NARA establish strict guidelines/mandates for record retention and disposal requirements. "The CSP SHALL delete any personal or sensitive information from the subscriber account records following account termination in accordance with the record retention and disposal requirements."*	Establish strict guidelines/mandates for record retention and disposal requirements.

74	Base	3.3 Authentication Proces	19	801	There are unintended consequences from the implementation of facial recognition technology including privacy invasion, public trust, fraud, and use of an emerging technology. A safer less intrusive biometric would be retinal scan which is genetically unique to every individual and equally effective. User cases should demonstrate effective application of specific, measurable, actionable objectives to ensure the benefits outweigh the risk.	Delay use facial recognition until sufficient evidence suggest the option will prove useful. Consider alternatives such as fingerprint and retinal scan first.
75	63A	N/A	N/A	N/A	Provide a "Track changes" redline document of NIST changes so the whole document does not need review.	Provide a "Track changes" redline document of NIST changes so the whole document does not need review.
76	63A	4.3.4.4 Validation Sources	13	629-631	Based on the statement below, does this mean that documents visually inspected by a trusted referee would not be required to be authenticated with the authoritative source? Core attributes that are contained on identity evidence that has been validated according to Sec. 4.3.4.1 can be considered validated, in which case no further validation is required.	Provide more clarity/context on this statement.
77	63A	5.1.1.2 Fraud Mitigation Measures	17	733-736	Consider making the below statement a SHALL statement. The CSP SHOULD obtain additional confidence in identity proofing using fraud mitigation measures (e.g., examining the device characteristics of the applicant, evaluating behavioral characteristics, and checking vital statistic repositories such as the Death Master File ([DMF]).	Update SHOULD to SHALL statement
78	63A	5.1.6 Requirements for Enrollment Codes	21	N/A	What is the reasoning in allowing an enrollment code to be used to verify identity but not authentication? Line 887 states "5. The enrollment code SHALL NOT be used as an authentication factor." Yet in section 5.3.4. Identity Verification Requirements, the CSP SHALL verify the binding of the applicant to the claimed identity by one of the Following: Line 1086 states "3. Verification of the applicant's return of a valid enrollment code Sec. 5.1.6"	Provide more clarity/context on this statement.
79	63A	5.3.5 Notification of Proofing Requirement	27	1088-1089	Why is the following statement SHOULD and not SHALL, is it because IAL1 is a lower risk? Upon the successful completion of identity proofing at IAL1, the CSP SHOULD send a notification of proofing to a validated address for the applicant, as specified in Sec. 5.1.7	Provide more clarity/context on this statement.
80	63A	6.2 Subscriber Account Access	35	1266-1271	Based on the following statement, is the AAL2 or AAL3 applicable for account access for IAL1 proofed accounts? In order to meet the requirement that accounts containing PII be protected by multi-factor authentication (MFA), the CSP SHALL provide a way for subscribers to access the information in their subscriber account through AAL2 or AAL3 authentication processes using authenticators registered to the subscriber account. The CSP SHALL provide the capability for subscribers to change or update the personal information contained in their subscriber account.	Provide more clarity/context on this statement.
81	63A	5.1.9 Trusted Referees & Applicant Referees	24	977-992	Multiple questions for Section 5.1.9 •Could the concept of an "applicant reference", while increasing accessibility and equity, also potentially increase a fraud vector? (i.e., one fraudster successfully ID proofs himself, and then helps another fraudster "ID proof", for example, as the new "Mrs. HighProfilePerson"). •What strength level is the vouching of an applicant reference considered? •What potential liability would an applicant reference have if someone they vouched for commits fraud? •Should CSPs be required to let Relying Parties know that a user was ID proofed with the aid of an applicant reference (as RPs form trusted partnerships with CSPs, not with an applicant reference)?	Provide more clarity/context on this statement.
82	63A	5.3.4 Identity Verification Requirements	27	1081	What is the difference in the first Identity Verification Requirement for IAL1 (Section 5.3.4) and IAL2 (Section 5.4.4)? Additionally, the verification option for Section 5.3.4 is not listed in Table 1 under Verification for IAL1.They are worded slightly different but appear to be saying the same thing.	Add clarity on the difference between Section 5.3.4 and Section 5.4.4. If they're meant to be the same, please write them the same.
83	63A	4.3.2 Characteristics of Acceptable Digital Evidence	10	540 - 541	Lines 540-541 reads, "If applicable, the presented digital evience can be verified through authentication at an AAL or FAL commensurate with the assessed IAL." Does this mean that if the application assesses at an IAL1/AAL2/FAL2 that the digital evidence should be verified using the higher level digital evidence for AAL and/or FAL?	Provide more clarity/context on this statement.
84	63A	N/A	N/A	N/A	Is there a process where IdP's can leverage validation/verification of users registration against other IdP's?	Setting up the ability for an IdP to coordinate with other IdP's to validate/verify a user when registering as a part of the registration process. For example, if John Doe has registered with ID.me and has been validated/verified at IAL2/AAL2/FAL2, and the user is now registering with Login.gov, Login.gov can through a back channel connection with ID.me to save time and validate/verify an individual that has already been vetted and speed up the process, and potentially reduce the potential for fraud. This cross check process can helpful if not already in place.
85	63A	N/A	N/A	N/A	There are multiple references to "physical comparison" of an applicant's face to the identity evidence, both in-person & remote. Should this say "visual comparison" instead, for clarity, since the operator won't be physically comparing anything? (the great Wikipedia says "A visual comparison is to compare two or more things by eye.", while an online search for "physical comparison" mostly turns up results about actually physically comparing characteristics of bullets, using tools, in crime labs)	Update references of 'physical comparison' to 'visual comparison'. This would provide more clarity as the operator won't be physically comparing anything.
86	63A	5.1.1 Identity Service Documentation & Records	17	723	There is an extra ; and at the end of the statement	Remove ; and
87	63A	5.1.2.1 Privacy Risk Assessment	18	771	The word dilligence is spelled incorrectly	The correct spelling is diligence
88	63B	5.1.5.2. Multi-Factor OTP Verifiers	26	1050	The word authentictor is spelled incorrectly	The correct spelling is authenticator
89	63B	5.1.8.1. Multi-Factor Cryptographic Software Authenticators	29	1157	The word requirementss is spelled incorrectly	The correct spelling is requirements
90	Base	5.5. Cyber, Fraud, and Identity Program Integrity	39	1493-1495	The following statement reads, "Organizations SHOULD establish consistent mechanisms for the exchange of information between critical security and fraud stakeholders". The recommendation is to update this statement from SHOULD to SHALL.	Update SHOULD to SHALL statement

91	Base	5.5. Cyber, Fraud, and Identity Program Integrity	39	1496-1497	The following statement reads, "Where supporting service providers, such as CSPs, are external, this may be complicated, but SHOULD be considered in contractual and legal mechanisms". The recommendation is to update this statement from SHOULD to SHALL.	Update SHOULD to SHALL statement
92	Base	2.3 Enterprise Risk Management Requirements and Considerations	6	489	Similar to the 'Security' sub-section under Section 2.3.1, there should be a 'Data Management' sub-section under Section 2.3, to address data management guidelines, and availability requirements.	The following language is suggested if a 'Data Management' section is added: Maintaining account creation data, account management records and user end point data in a retrievable and analyzable format is critical to fraud detection and analytics. This data will also be critical to legal process. To facilitate fraud analytics by end user client and legal process by law enforcement authorities, the CSP should be prepared and able to provide unmodified data records for the above-mentioned data types, if requested. This includes a standard data formatting, a data retention policy, ability to securely transfer data and all requisite policies and procedures to maintain these capabilities. To facilitate this capability, the CSP must establish and maintain a secure data repository that meets all relevant security standards but maintains the data in an unmodified format upon decryption and is accessible to both the CSP and authorized partners and parties.
93	Base	5.5 Cyber, Fraud, and Identity Program Integrity	39	1484	There should be a section on 'Data Capture Requirements', which should include a baseline (unexhaustive) list of data fields needed for fraud detection and monitoring that the CSPs should capture for internal and/or client fraud detection and response.	Refer to general comments document provided by CFAM.
94	Base	5.5 Cyber, Fraud, and Identity Program Integrity	39	1484	Security should also include fraud considerations, particularly fraud analytics for detection, root cause analysis to identify successful threat vectors and remediation strategies and implementation procedures. Fraud poses as high of a threat to sensitive application processes and data as traditional cyber security threats such as hacking. Through identity theft, social engineering, phishing and other strategies, criminals can pose as one or many identities. These identity owner's personal data, benefits and financial resources are put at grave risk when this happens, as well as the organizations processes and assets.	The recommendation is to provide additional information on the threat posed by insufficient identity protection to emphasize importance of fraud detection and monitoring.
95	Base	5.5 Cyber, Fraud, and Identity Program Integrity	39	1484	Add a requirement for the development of a comprehensive overall fraud detection posture, to be shared with CSP partners.	The CSP should maintain a comprehensive fraud analytics, detection, and response posture. This posture shall include indicator development and monitoring, data analytics-based threat hunting, dedicated fraud analyst personnel and technical access and capability to identify the root cause of successful fraudulent exploitation of the CSP Identity validation process. This posture shall be applied to all log types of record documented in section 2.3.1. Refer to general comments document provided by CFAM.
96	Base	5.5 Cyber, Fraud, and Identity Program Integrity	39	1484	Level of rigor applied to fraud detection and analytics is tied to the sensitivity of the data delivered by the applications protected. This results in higher IAL processes being the target of the most rigorous detection posture.	Fraud detection posture needs to be tied to the sensitivity of the data delivered by the applications protected.
97	Base	5.5 Cyber, Fraud, and Identity Program Integrity	39	1484	Request the addition of language regarding threat intelligence sharing for fraud detection, and the development of major fraud remediation playbooks. This will allow for CSP partners to quickly respond to new TTPs and rapid implement remediation strategies.	Include language such as: The CSP must inform RPs of accounts detected to be fraudulent. The CSP must maintain secure pathways and procedures to exchange two-way threat intelligence and investigation findings with all clients.
98	Base	5.5 Cyber, Fraud, and Identity Program Integrity	39	1484	CSP must maintain a mechanism for end users to report potential fraudulent activity or account takeover. This mechanism should also allow for the account to be disabled to prevent further harm to the user. Information on this self reported fraudulent activity should be passed along with the account information in order to allow for partners to conduct their own fraud investigation and remediation.	Include language such as: The CSP must maintain a self-reporting mechanism for CSP clients (end users) who believe they have been a victim of fraud along with a function for users to be disabled at both the account, and identity level. Record of these communication and actions shall be documented and shared within account management data.
99	Base	5.5 Cyber, Fraud, and Identity Program Integrity	39	1484	Customer notification is a critical aspect of identity protection; without notification of potential account changes, a customer is particularly vulnerable to account takeovers by bad actors.	Include language such as: The CSP shall maintain a posture of notifying the account owner upon all account management and update actions (e.g. 2FA method update, password reset, account suspension, email update, etc.). The CSP shall inform the identity of the existence of multiple accounts upon login to the CSP.
100	Base	5.5 Cyber, Fraud, and Identity Program Integrity	39	1484	Define Fraud analytics, Root Cause Analysis, & Fraud Activity Remediation within section 5.5. This will provide a common understanding of these activities.	The following definitions are recommended: •Fraud Analytics – Analytics applied to proofing, application, and web transaction data augmented with identity data sources to identify suspicious behavior patterns indicative of fraud activity. Critical data includes but is not limited to, source device and network information, user entered unique values, data validation response codes and internal and taxpayer driven account suspension information. •Root Cause Analysis – Review of identified fraud behaviors in the context of existing identity validation strategy to identify exploitation vectors used by fraudulent actors to gain unauthorized access to accounts and data other than their own. •Fraud Activity Remediation – The modification of Identity Validation process to eliminate a weakness that is being exploited by criminals to gain fraudulent access to accounts or data that are not their own.
101	Base	4.2 Enrollment and Identity Proofing	14	706	Currently language on subscriber accounts reads "..subscriber account to uniquely identify each subscriber". The language needs additional clarity requiring that an identity be bound to a single active account. Allowing for an identity to have multiple accounts provides threat actors the ability to potentially proof and create a duplicate account, allowing for actions to be taken without the subscribers knowledge or consent.	Include language such as: The CSP then establishes a subscriber account to uniquely identify each subscriber and record any authenticators registered (bound) to that subscriber account. An individual identity may only have only one active subscriber account.
102	63A	4.1.1 Process Flow	8	470	The resolution section does not explicitly state the phone number is a required attribute. Later in the verification section (row 483) it's required. The way it's worded in the resolution section, a phone number appears to be optional.	Update the text to explicitly state the phone number is a required attribute.
103	63A	4.1.1 Process Flow	9	483	Line 483 references the validated phone number but does not state the phone number should be validated against the identity.	Update the text to explicitly state the phone number referenced is validated against the identity.
104	63A	4.1.1 Process Flow	8	476	Should include language to mention that the goal is to confirm that the person proofing is the owner of the identity.	Include text that explicitly states the goal is to confirm the person proofing is the owner of the identity.
105	63A	4.3.3.3 Superior Evidence Requirements	12	590	Line 590 states, "….contains at least one reference number that uniquely identifies and resolves to the person to whom it relates." This is not a strong enough evidence unless the reference number on the document is checked against an authoritative source.	The true identity should match this identity in an accepted system of record. Gathering data and checking the data gathered must correlate for true identity proofing.
106	63A	5.1.1.2 Fraud Mitigation Measures	17	732	This section only addresses fraud mitigation during the initial proofing and is not relevant to the mitigation of new or emerging threats.	Add fraud detection/mitigation process post account creation based on patterns and connections.
107	63A	5.1.2.1 Privacy Risk Assessment	18	771	Risk assessment measures do not preclude the ability to protect systems and processes from fraudulent activity.	Add language to protect systems and processes from fraudulent activity.

108	63A	5.1.2.2 Additional Privacy Protective Measures	18	773-775	Lines 773-775 reads, "Processing of PII SHALL be limited to the minimum necessary to validate the existence of the claimed identity, associate the claimed identity with the applicant, and provide RPs with attributes they may use to make authorization decisions." Authorized processing reasons should include detection and mitigation of fraud activity.	Add language to include fraud in authorized processing of PII.
109	63A	5.1.7 Requirements for Notifications of Identity Proofing	22	895	IAL2 account notifications should be sent by the CSP to validated home of record address or phone.	Incorporate notification language for IAL2.
110	63A	5.1.8 Requirements for Use of Biometrics	23	952	Suggest the language here be further refined to ensure the biometric data matches both the applicant and the true identity owner.	Add additional clarity.
111	63A	5.1.9.1 Requirements for Trusted Referees	25	1002	Recommend a requirement clause be added for logging of proofing steps taken by the trusted referee in each session.	Add proofing step requirement for trusted referee.
112	63A	5.4.1 Automated Attack Prevention	28	1096	Suggest a section be added requiring the implementation of a fraud detection process with similar language to the automation attack prevention.	Add a section requiring the implementation of a fraud detection process with similar language to the automation attack prevention.
113	63A	5.4.4.1 Remote Identity Proofing	29	1132	Recommend this be SUPERIOR evidence only (assuming the change is made that this rating requires unique identifier validation by authoritative source).	Recommend this be SUPERIOR evidence only.
114	63A	5.5.1 Automated Attack Prevention	29	1148	Suggest the same additions and updates made to IAL 2 be carried over consistently throughout the document.	Suggest the same additions and updates made to IAL 2 be carried over consistently throughout the document.
115	63A	5.6 Summary of Requirements	33	Table 1 - IAL Requirements Summary	Suggest consistent changes to Evidence and Validation of SUPERIOR vs STRONG/FAIR.	Suggest consistent changes to Evidence and Validation of SUPERIOR vs STRONG/FAIR.
116	63A	6.3.2 Subscriber Account Termination	35	1280	Recommend adding clause for the user to report an unauthorized account.	Add self-reporting of unauthorized access.
117	63A	8.1 Collection and Data Minimization	40	1346	PII Retention should be conducted only for the purpose of facilitating further account validation processes and fraud detection and prevention activities.	Add language to specify use of PII for fraud.
118	63A	8.1 Collection and Data Minimization	40	1348	Suggest adding clarifying language on minimization of PII to address fraud.	Include additional language in line 1348. Suggested language, "…but minimization procedures should be weighted against valid needs of threat mitigation, fraud detection and security processes when established".
119	63A	8.5 Privacy Risk Assessment	42	1429	This section does not cite the risk of NOT taking specific steps regarding data collection and its Security Risks.	Include additional guidance or specific steps regarding data collection and its Security Risks.
120	63A	9.3 Enrollment and Proofing Session	48	1641	Recommend ensuring the enrollment code is accompanied by a message that clearly states what the user is enrolling for - based on CFAM's lessons learned .	Add accompanying message to enrollment code.
121	63B	4.2 Authentication Assurance Level 2	8	491	Add 'identity owner' after claimant.	Update line 491 to read, "AAL2 provides high confidence that the claimant and identity owner controls authenticators bound to the subscriber account".
122	63B	6.1 Authenticator Binding 6.1.1 Binding at Enrollment	41, 42	1582, 1617	Recommend that 2FA device cannot be updated or added to account without a separate 2FA code validation by the existing device on the account, solely to validate this new binding. This would add some mitigation to account takeovers, limiting criminals' ability to set up persistent account access without direct notification of the account owner.	Recommend that 2FA device cannot be updated or added to account without a separate 2FA code validation by the existing device on the account, solely to validate this new binding. This would add some mitigation to account takeovers, limiting criminals' ability to set up persistent account access without direct notification of the account owner. Similar language does exist in line 1636-1642.
123	63B	6.1.2.3 Account Recovery	44	1681	Expound on 'addresses of record' statement by incorporating authoritative source validation.	*Recommend updating line 1681 to read, "one of the subscriber's address of record, which has been validated against records maintained by an authoritative source".*
124	63B	8.1 Authenticator Threats	52	1933	Incorporate social engineering scenario.	Recommend adding, "Legitimate owner may be manipulated into providing access to secrets, without deliberate collusion".
125	63B	8.1 Authenticator Threats	55	Table 3 - Endpoint Compromise	Add text forwarding of SMS code due to modified configuration of the victims device settings by the criminal	Add text forwarding of SMS code due to modified configuration of the victims device settings by the criminal
126	63B	8.2 Threat Mitigation Strategies	57	Table 4, Social Engineering Row	Explicitly state the reason for the authentication code delivery in the SMS sent to the user. "This code is being used to authenticate with 'CSP name' for 'X agency'"	Explicitly state the reason for the authentication code delivery in the SMS sent to the user. For instance, "This code is being used to authenticate with 'CSP name' for 'X agency'" .
127	63B	8.1 Authenticator Threats	52	N/A	Incorporate security consideration for risk assessment	Recommend adding 3rd consideration: The impact to the integrity of the authentication system and user if data is not retained.
128	63B	6.1.2.4. External Authenticator Binding	44	1701	Recommend incorporating language that acknowledges overall risks of using a Federated model.	Recommended language includes: •Including potential for fraud targeting one agency to proliferate at another •Limitations for CSP to tailor their ID proofing strategies based on risks to individual clients (i.e. more stringent data attribute checks for different partners) •Reduced visibility into third party vendor proofing parameters
129	63C	5.4.4 Attribute Collection	29	1067-1069	Lines 1067-1069 states, "All attributes associated with an RP subscriber account, regardless of their source, SHALL be removed when the RP subscriber account is terminated." There should be an exception added in the case of fraudulent activity response or legal due process.	Add an exception to the statement in the case of fraudulent activity response or legal due process
130	63C	5.5 Privacy Requirements	30	1112-1117	This paragraph cites that the CSP should discourage tracking of a user across multiple clients. It is recommended further emphasizing the need for a CSP MUST have their own, in house, cross client, fraud detection, analysis and response posture.	Provide more emphasis that a CSP MUST have their own, in house, cross client, fraud detection, analysis and response posture
131	63C	5.7 Shared Signaling	32, 33	1201, 1207	Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account". The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.	Update MAY to MUST statement
132	63C	6.3 Identity APIs	45	1536	Should be specific on what data attributes are required for federated model via the API.	Recommend being more specific on what data attributes are required for federated models via the API
133	63C	10.2.1 User Perspectives on Online Identity	63	1960	Recommend adding the ability for users to lock their identity from account creation.	Recommend including the ability for users to lock their identity from account creation
134	63A	4.3.4.1 Evidence Validation	12	601	Either in 63A or in Implementation Guidance, there should be defined minimum data attributes, per piece of evidence, that should be required to be validated. This would set a standard across the CSPs on what will be validated on the evidence at each xAL level.	