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

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

Organization:	**Internal Revenue Service (IRS)**
Name of Submitter/POC:	Simone Alcorn, Varun Lal, Elizabeth Roberson
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63A	2.4 Identity Validation and Identity Evidence Collection	10	649	If expired SUPERIOR evidence will still be used as part of the evidence collection, consider lowering the evidence level to STRONG. There is concern with the confidence level of using an expired SUPERIOR piece of evidence to prove identity. If the requirement is for SUPERIOR and evidence is expired, that essentially triggers the need for additional documentation.	If expired SUPERIOR evidence will still be used as part of the evidence collection, consider lowering the evidence level to STRONG.
2	63A	4.2.6.1 IAL2 Verification Non Biometric Pathway	42	1716-1719	Do not remove the requirement for confirmation of address. This adds an additional layer when dealing with account compromise; having an enrollment code sent to the user and having the user confirming the code provides added security. Only providing notice to the address of record prevents the user from being notified early that their account has been accessed.	Do not remove the requirement for confirmation of address; keep it in the final version of 63-4.
3	63A	4.2.6.3 IAL2 Verification - Biometric Pathway	44	1772-1776	It states automated comparison of applicant's facial image to facial image on evidence. Isn't this in person? If so, would it not be physical representation to what is in the system (same as the airports)? If not, has NIST performed a risk assessment on the risks, such as deepfake?	N/A
4	63A	2.4.2.2 Evidence Validation Methods	13	751	NIST should include baseline/minimum technical requirements for scanner and camera requirements, such as pixels or DPI, to assure that the identity document image is of sufficient quality for trained personnel to determine if it is a legitimate document.	Include baseline/minimum technical requirements for scanner and camera requirements, such as pixels or DPI, to assure that the identity document image is of sufficient quality for trained personnel to determine if it is a legitimate document.
5	63A	3.1.10 Requirements for Notifications of Identity Proofing	26	1186	Add "Validated Address" and it's definition to the glossary.	Add "Validated Address" and it's definition to the glossary.
6	63A	3.1.11 Requirements for Use of Biometrics	28	1235	Reads, "CSPs shall have their biometric algorithms periodically tested." This should specify how often and the maximum number of time, in months or years, between tests is required for auditing purposes.	Specify how often and the maximum number of time, in months or years, between tests is required for auditing purposes.
7	63A	3.1.12 Requirements for Evidence Validation Processes (Authenticity Checks)	30	1307	Reads, "CSPs should have their evidence validation technology periodically tested...." Replace periodically with annually.	"CSPs should have their evidence validation technology tested annually,..."
8	63A	4.3.4 Evidence Validation	45	1816	Examples of digital FAIR identity evidence would be helpful, either in this section or in the table in Appendix A on page 78.	Include examples of digital FAIR identity evidence, either in this section or in the table in Appendix A on page 78.
9	63A	4.3.7 Onsite Attended Requirements (Locally Attended)	46	1855	Should specify minimum technical specifications for image quality and auditing purposes.	Specify minimum technical specifications for image quality and auditing purposes.
10	63A	4.3.7 Onsite Attended Requirements (Locally Attended)	47	1873	The retention schedule should be provided to the applicant in the request for consent.	The retention schedule should be provided to the applicant in the request for consent.
11	63A	4.3.8 Onsite Attended Requirements (Remotely Attended - Formally Supervised Remote)	47	1894	Should specify minimum technical specifications for image quality and auditing purposes.	Specify minimum technical specifications for image quality and auditing purposes.
12	63A	5.4 Subscriber Account Suspension or	52	1988	There should be a maximum amount of time that the CSP shall delete any personal or sensitive information from the subscriber account.	N/A
13	63B	3.1.7.3 Usage with Subscriber-Controlled Wallets	27	1172	Based on workshops held, digital wallets are a form of multi-factor cryptographic authentication. Mentioning digital wallets as a 'special-case usage' can be interpreted as authentication with digital wallets are used on a special case basis.	Updated language (especially the 'special-case usage') to clearly state the intent of the section, that digital wallets are a form of authentication.
14	63B	5.2 Reauthentication	51	1971- 1973	This is not best practice. The IRM 10.8.1 has 30 minutes and OWASP recommends 30 minutes. The goal is to minimize the amount of time a bad actor/hacker has, to discover and exploit a session token. We want to ensure user experience, but also be cognizant of security. We do have mitigating controls in place, so the likelihood is probably low, but still a risk.	Inactivity Timeout should be no more than 1 hour.
15	63B	Appendix E	113	3603-3604	Removed the prohibition on the use of VoIP phone numbers for out-of-band authentication. There is a relationship between fraud and VOIP phone numbers - disagree with the removal.	Do not remove the prohibition on the use of VoIP phone numbers for out-of-band authentication.
16	63B	9 Equity	75-76	2514-2569	The discussion surrounding equity in 63B is interesting and encourages compliant alternatives. Since it is informative it does not establish directives for the CSPs so there is no way to hold them to equity considerations.	Establish requirements for Equity.
17	63B	3.2.3 Use of Biometrics	30	1284	Reads, "an overall limit of 50 consecutive failed authentication attempts or 100 if PAD is implemented..." This seems excessively high.	"an overall limit of 20 consecutive failed authentication attempts or 30 if PAD is implemented..."
18	63B	3.2.5.1 Channel Binding	33	1366	The channel binding description seems to map to PIV and CAC cards. If so, include PIV and CAC as examples. WebAuthn and FIDO2 are named as examples in the Verifier Name Binding section below. It would be good to have consistency.	N/A

19	63B	4.2.1.3 Recovery Contacts	44	1741	A subscriber may specify their spouse as their recovery contact. If they divorce, the subscriber should be able to remove the ex-spouse at anytime. This section should a section to enable the subscriber to remove or change recovery contacts.	If the CSP supports the use of recovery contacts the CSP SHALL provide methods for subscribers to view and manage recovery contacts. CSPs should send a reminder annually to subscribers to review their list of recovery contacts.
20	63B	Appendix B Syncable Authenticators	88	2919	Reads "Authenticators that generate private keys SHOULD support attestation features that can be used to verify the capabilities and sources of the authenticator (e.g., enterprise attestation). This should be a SHALL for AAL2. It could remain SHOULD for AAL1.	At AAL2 authenticators that generate private keys SHALL support attestation features that can be used to verify the capabilities and sources of the authenticator (e.g., enterprise attestation). At AAL1 authenticators that generate private keys SHOULD support attestation features that can be used to verify the capabilities and sources of the authenticator.
21	63B	Appendix B Syncable Authenticators	88	2919	General Comment. The Syncable Authenticators section needs to be re-written so a CSP can be audited.	The Syncable Authenticators section needs to be re-written so a CSP can be audited.
22	63-Base	3 Digital Identity Risk Management	22	930-933	The paragraph (lines 930 - 933) address the two dimensions for identification and management. This section should outline the identification and then the management of the risks that have been identified for the identity system. Line 933 uses the word "implemented", should this be changed to managed? Why would you implement a risk?	Change "implemented" to "managed".
23	63-Base	3 Digital Identity Risk Management	22	950-951	Lines 950-951 talk to the second dimension of risk and talks to identifying the risks posed by the identity system. The second dimension should be focused on how to manage the risks through the tailoring process.	Line 950-951 should be reworded to say "The second dimension of risk seeks to manage the risks identified with the identity system and informs actions necessary to tailor the initial assurance level."
24	63-Base	3 Digital Identity Risk Management	27, 28	1109-1115	plant (which are external), the technicians who control and operate the water treatment plant (internal), the organization that owns and operates the water treatment plant (internal), and auditors and other officials who provide oversight of the facility and its compliance with applicable regulations (external). The IRS currently only performs Digital Identity Risk Assessments (DIRA) on external-facing web applications that require ID proofing and authentication. Has this changed to all Digital Identity (both internal and external) now? If this applies to all Digital Identity for both internal and external groups/entities, this should be stated within the guidance somewhere to make this perfectly clear to all.	State explicitly within guidelines if applies to all Digital Identity for both internal and external groups/entities (if applicable)
25	63-Base	3.3.2.1 Identity Assurance Level	35	1365-1367	IAL3 states "IAL3 adds the requirement for a trained CSP representative (i.e., proofing agent) to interact directly with the applicant as part of an on-site attended identity proofing session as well as the collection of at least one biometric." Based on this statement, does this mean that only option 4, section 2.1.3 Identity Proofing Types in NIST SP 800-63A-4 apply to IAL3? Also, does a PIV or CAC qualify for the Onsite Attended Identity Proofing at an IAL3 Level? This poses an additional question with regard to the representative issuing a PIV/CAC, will this satisfy this statement when it states that the CSP representative to interact directly with the applicant as part of an on-site attended identity proofing session as well as collection at east one biometric (with PIV/CAC this is generally a fingerprint) Can be met with the PIV/CAC Issuer representative being considered the CSP representative? Does a PIV/CAC support both IAL3 and AAL3 requirements? If so, can this be stated somewhere in the Guidelines and/or 63A-4 or 63B-4?	State explicitly within the Guidelines and/or 63A-4 or 63B-4 if the requirement can be met with the PIV/CAC Issuer representative being considered the CSP representative (if applicable).
26	63-Base	2 Digital Identity Model	10	633-634	There is reference to entity in the sentence about Models grouping functions, such as creating subscriber accounts and providing attributes, under a single entity. Upon review of the Glossary, there is no explanation for "Entity" as it is used in these guidelines.	Add clarification on "Entities" in the Glossary and to this paragraph to make it a more clear on what an "Entity" is in context to these guidelines
27	63-Base	3.1 Define the Online Service Figure 6	26	Figure 6	Step 1 is the only part of the process flow that talks to entities. This step is to cover the defining of the online service which captures Functional scope, user groups, impacted entities. Do we need to assess the CSP/IdP against the Impact Categories to determine the level of impact for each CSP/IdP and document this in our initial impact assessment?	N/A
28	63-Base	3 Digital Identity Risk Management	23	991-992	There is reference to "user groups" in the sentence about Identity process failures may result in different levels of impact for various user groups. Upon review of the Glossary, there is no explanation for "User Group(s)" as it is used in these guidelines.	Add clarification on "user group(s)" in the Glossary and in the paragraph to make it more clear on what is meant by "user group(s)" in context to these guidelines.
29	63-Base	3 Digital Identity Risk Management	25	1061-1066	At a minimum organizations SHALL execute and document each step, consult with a representative sample of the online service's user population to inform the design and performance evaluation of the identity management approach, and complete and document the normative mandates and outcomes of each step regardless of the operational approach or enabling tools. If you are performing an initial assessment of a new application using Digital Identity for ID Proofing and Authentication, how can you consult a sample of the online service's user population to inform design and performance evaluation of the identity management approach?	Provide clarity regarding the requirement; if performing an initial assessment of a new application, how can you consult a sample of the online service's user population to inform design and performance evaluation of the identity management approach.
30	63-Base	3.1 Define the Online Service	27	1101-1102	It is important to differentiate between user groups and impacted entities as described in this document. The online service will allow access to a set of users who may be partitioned into a few user groups based on the kind of functionality that is offered to that user group. This sentence is not easy to differentiate between user groups and impacted entities.	Provide some information to help us understand the difference between a user group and entity as written in this guidance.
31	63-Base	3.1 Define the Online Service	27	1102-1104	As written in this guidance it appears that you want each Entity and User Group to be evaluated based on the functionality that each user group will have through the online service to determine that each user group will be assessed at the same or different xALs based on the difference in functions they can perform through the online service, is this correct? If this correct, then a separate initial assessment must be performed for each user group and/or entity to ensure the xALs are set to a high enough xAL to cover all user groups accessing the online service, is this correct? Does the documentation of each initial impact assessment for each user group and/or entity need to be documented as part of the	N/A
32	63-Base	3.2.1 Identify Impact Categories and Potential Harms	29	1151-1155	In the 2PD, you have only 5 Impact Categories versus the 6 that were listed in the IPD. Was the original "Damage to or Loss of economic stability" renamed to "Financial loss or financial liability"? Additionally, in the IPD you had an impact category for "Noncompliance with laws, regulations, and/or contractual obligations" was this removed or combined with another category?	N/A

33	63-Base	3.2.3 Impact Analysis	33	1290-1299	citizens who drink the water, the organization that owns the facility, auditors, monitoring officials, etc.) for each of the impact categories". There is mention throughout the document for user groups and entities that seems to be the same in some cases. For example the User Groups seem to fit in the same category as the entities. Can you please help explain these terms in a manner in which it is less confusing? The terms entity and user group seems to add multi-dimensional groups that need to be assessed.	Clarify with good examples of each or consider combining into a term that would cover all the groups that need to be analyzed.
34	63-Base	3.4.4 Digital Identity Acceptance Statement (DIAS)	44	1648	It would be helpful to agencies if NIST were to provide a Digital Identity Acceptance Statement template. I realize that agencies differ, but having a base template to work from would be appreciated.	Provide a Digital Identity Acceptance Statement template.
35	63C	Table 1 Federation Assertion Levels	4	491	Is it "a priori" or "Apriori"? Table 1 reads "a priori" while Section 4.3.1 reads "Apriori"	N/A
36	63C	3.15.2 Subscriber-Provided Bound Authenticator Binding Ceremony	39	1638	Add "binding ceremony" to the glossary	Add "binding ceremony" to the glossary
37	63C	4.2 Federation Transaction	44	1731	Add each numeric step to the steps in the diagram in Fig. 6 to make it easier for the reader to follow.	Add each numeric step to the steps in the diagram in Fig. 6 to make it easier for the reader to follow.
38	63C	4.2 Federation Transaction	44	1736	Step 2 does not seem to appear in Fig. 6. If it does, suggest rewording for clarity.	Reword for clarity.
39	63C	4.3.1 Apriori Trust Agreement Establishment	46	1779	Is it "a priori" or "Apriori"? Needs consistency	N/A
40	63C	4.11.1 Back Channel Presentation	65	2418	Reads, "In the back-channel presentation model shown in Fig. 11, the subscriber is given an assertion reference to present to the RP, generally through the front channel."	Reword to "In the back-channel presentation model shown in Fig. 11, the IDP gives the subscriber is given an assertion reference to present to the RP, generally through the front channel."
41	63C	4.11.1 Back Channel Presentation	66	2427	In Fig. 11, suggest adding the word "Subscriber" where applicable for clarity	Add the word "Subscriber" where applicable for clarity.
42	63C	5.2 Federation Transaction	70	2527	In Fig. 13, suggest numbering the steps to coincide with the steps detailed in Lines 2525 to 2537, for clarity and readability.	Number the steps to coincide with the steps detailed in Lines 2525 to 2537, for clarity and readability.
43	63C	5.3 Trust Agreements	71	2548	Add colon at the end of the line.	Add colon at the end of the line.