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: *Easy Dynamics*	
Name of Subn *Michael Magrath*	
Email Address [redacted]	

Comm	Publica	Section	Page #	Line #	**Comment** (Include rationale for comment)	**Suggested Change**
1					**General comment:** Easy Dynamics welcomes the second public draft of this critical document suite. We found the document suite to be comprehensive, readable in plain language, and attentive to modern opportunities and threats. The themes of equity, privacy, and enterprise risk management are present throughout. We commend the entire NIST team and support staff for your diligence in recovering thousands of comments, and your thoughtful consideration of holistic digital identity management.	
2	63A	2.4.1.1	11	679	Requiring physical security features on all FAIR identity evidence, signifcantly reduces potentially acceptable evidence, which increases security but could impact equity and inclusion. Utility bills will no longer be valid and ID cards from schools will need to have physical security features to comply. These are important evidence types currently being used for lower-assurance proofing flows.	Suggest accepting FAIR evidence without physical security features at IAL1. Physical security features shall be required for identity evidence at IAL2 and IAL3.
3	63A	2.4.2.2	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 sufficent quality for trained personnel to determine if it is a legitimate document.	
4	63A	3.1.1.	16	845	Can NIST offer any minimum training and qualification requirements? This is very important.	
5	63A	3.1.10	26	1186		Add "Validated Address" and its definition to the glossary.
6	63A	3.1.11	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.	Suggest requiring an annual review.
7	63A	3.1.11	29	1273	Add the term Liveness Detection. This is what agencies are seeking.	
8	63A	3.1.12	29	1296	Reads, "CSPs SHOULD deploy technology controls to prevent the injection of document images,..." Why is this not a SHALL?	CSPs SHALL deploy technology controls to prevent the injection of document images,..."
9	63A	3.1.12	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,..."
10	63A	4.2.6.2	43	1759	Many evidence types, including passport and many types of FAIR evidence, will have difficulty validating the unique identifier against an authoritative source. Not a comment for NIST per se, but a reminder to implementors that in OMB M-19-17, "Agencies that are authoritative sources for attributes (e.g., SSN) utilized in identity proofing· events, as selected by 0MB and permissible by law, shall establish privacy enhanced data validation APis for public and private sector identity proofing services to consume, providing a mechanism to improve the assurance of digital identity verification transactions based on consumer consent." This will be critical now!	
11	63A	4.3.4	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.	
12	63A	4.3.7	46	1855	Should specify minimum technical specifications for image quality and auditing purposes.	
13	63A	4.3.7	47	1873	The retention schedule should be provided to the applicant in the request for consent.	
14	63A	4.3.8	47	1894	Should specify minimum technical specifications for image quality and auditing purposes.	
15	63A	5.4	52	1988	There should be a maximum amount of time that the CSP shall delete any personal or sensitive information from the subscriber account.	
16	63B	2.1.2	5	522	The paragraphs from lines 523-525 and 528-529 are confusing. The former reads the implementation need not be validated under FIPS 140 while the latter that cryptography used by verifiers operated on or behalf of federal agencies at AAL1 shall be validated to meeting FIPS 140 Level 1.	Suggest rewording and providing examples.
17	63B	3.2.3	30	1275	"The biometric system SHOULD implement PAD." Given the threat vector, this should be a SHALL.	"The biometric system SHALL implement PAD."

18	63B	3.2.3	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…"
19	63B	3.2.5.1	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.	
20	63B	3.2.9	35	1446	Provide examples of restricted authenticators. SMS-OTP is restricted. It would be good to list it here and also include any other restricted authenticators. Agencies shouldn't have to guess.	
21	63B	4.2.1.3	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.
22	63B	Appen	88	2919	General Comment. The Syncable Authenticators section needs to be re-written so a CSP can be audited.	
23	63-Bas	1.3	4	463	General comment. Easy Dynamics welcomes the broad discussion of risk management and the inclusion of enterprise risk factors and context. It aligns nicely with the CSF and other risk management materials. We also appreciate the infusion of risk management practices across the document suite, for example in empowering CSPs to define a period of validity for expired documents (63A 2.4.2).	
24	63-Bas	3.2.1	29	1148	It's included under the examples, but consider pulling fraud up as its own impact category, to underscore its importance in a risk management program.	
25	63-Bas	3.4.4	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.	
26	63-Bas	3.6	48	1740	There have been examples across industry of redress being paid-only (although have not heard of this in the public sector). It's implied, but consider underscoring that redress for issues encountered during identity-related interactions should not be pay-for-play.	
27	63-Bas	3.8	50	1817	The section on AI/ML in identity systems is strong. One risk vector that may arise relates also to customer redress - that due to non-transparent algorithms, claimants may not know where/how they failed out of an identity process. Consider mentioning that AI systems need to work with redress systems to provide transparency into how their issues can be addressed.	
28	63-Bas	3.8	50	1817	AI in the identity context has specific privacy threat vectors related to PII search, correlation, processing, retention, training models, etc. Privacy risk management and AI risk management are well documented in 800-63 suite as well as the broader NIST universe of interconnected documents. However, it may be worth specifically calling out AI-related privacy risks in 63.4 Section 3.8.	
29	63-Bas	Genera	Genera	Genera	General comment. The Federal Reserve has developed a great taxonomy for talking about fraud and scams. https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/	Consider reviewing the Fed materials to see if there are any areas that are appropriate to align terminology and concepts.
30	63C	Table 1	4	491	Is it "a priori" or "Apriori"? Table 1 reads "a priori" while Section 4.3.1 reads "Apriori"	
31	63C	3.15.1	39	1614	This describes PIV and CAC. If so, suggest naming them as examples.	
32	63C	3.15.2	39	1638	Add "binding ceremony" to the glossary	
33	63C	4.2	44	1731	Add each numeric step to the steps in the diagram in Fig. 6 to make it easier for the reader to follow.	
34	63C	4.2	44	1736	Step 2 does not seem to appear in Fig. 6. If it does, suggest rewording for clarity.	
35	63C	4.3.1	46	1779	Is it "a priori" or "Apriori"? Needs consistency	
36	63C	4.11.1	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."
37	63C	4.11.1	66	2427	In Fig. 11, suggest adding the word "Subscriber" where applicabe for clarity	
38	63C	5.2	70	2527	In Fig. 13, suggest numbering the steps to coincide with the steps detailed in Lines 2525 to 2537, for clarity and readability.	
39	63C	5.3	71	2548	Add colon at the end of the line.	