Department of Education Comments for: NIST SP 800-63-4 Suite (Initial Public Draft)

Please submit responses internally by 2/17/2023

#	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63A	General	N/A	N/A	Regarding the question around alternative methods to proof a user at IAL2 without the use of facial biometrics with presentation attack detection, demonstrating access to a user account at IAL2 is a good option. It is common for students (who may have limited identification documents) to have a loan account or other educational resources, for example; these could be leveraged as additional pieces of evidence or showing federated access to the account may be able to constitute a verification of sorts. It could be worth explicitly mentioning agency IAL2/AAL2 accounts as part of the definition or implementation guide for credible sources to support this alternative.	
2	63A	General	N/A	N/A	Regarding the above comment - demonstrating access to an IAL3 account via PIV/DPC would be a helpful way to reduce time and cost of re-proofing a subset of users. The ability to validate additional core attributes that are not available on the PIV itself against USAccess or other authoritative sources would help streamline the process. NIST may wish to consider working with OMB and/or legislative bodies to make this option more of a reality.	
3	63A	General	N/A	N/A	Caution should be used when leveraging AI/ML-based verification techniques due to the lack of transparency typical to these models. As the Federal government focuses on improved supply chain security, it is critical to understand all aspects of a product, especially in the identity space, where attack vectors are common. Any data-driven alternative to biometric verification needs to include full details of the product and component services, to include location of data processing and storage servers, exact and comprehensive data sources used (also so that a proper privacy impact analysis can be conducted), a practice statement explaining data protection practices, and a detailed description of the risk model used and how each variable affects the outcome (also to identify and reduce bias in the service).	
4	63A	General	N/A	N/A	Due to the lack of publicly available test data around "good" identities, NIST should partner with agencies on a program to use real data (subject to active, informed user consent, with strong security and privacy controls) to test and compare the outcomes of identity proofing workflows. Metrics could include pass/fail rates across various demographics; outcomes based on different evidence types; average time to completion; false passes and false rejections.	
5	63A	General	N/A	N/A	To enable more rapid adoption of the Digital Identity Guidelines and future revisions, it would help agencies to have support in assessing and comparing potential products. NIST should work with OMB and DHS or GSA to re-invigorate the concept of an assessment program to provide a marketplace of compliant identity options, in partnership with established groups such as Kantara and FIDO (with select modifications such as adding FIPS 140 compliance, for example). A playbook or guide could also be developed to support agencies in how to factor in additional variables such as cost, scalability, user base, and overall fit.	
6	63A	2.1	4	397	The separation of validation into evidence validation and attribute validation is clear and helpful.	
7	63A	4.3.3.1	11	557	In the definition of FAIR evidence, it includes a requirement that the evidence be unexpired or be expired within the past six months. Would an otherwise valid, but recently expired STRONG evidence then be able to be counted as FAIR? This could be helpful if so.	
8	63A	4.3.4.2	13	617	At times this section has caused some confusion since not every attribute present on the evidence is sometimes possible to be validated. While each agency must define their own core attributes, it could help to clarify this section to indicate that any attribute that the agency/CSP will be gathering for the subscriber account must be validated; or reference the definition in section 5.1.1.	"Core attributes as defined in section 5.1.1"
9	63A	4.3.4.3	13	621	This section could be confusing as well, since it combines the two types of validation (document authenticity and authoritative source). It makes it seem as though you can choose one or the other. It also glosses over the question of whether a visual inspection by a trained personnel counts as both types of validation.	Potentially split the section into approved ways to conduct document authenticity checks vs. source validation; also clarify that if a visual inspection of the document takes place, a source validation event must still take place as well.
10	63A	4.3.4.4	14	651	Consider expanding the definition of credible source to indicate that the proofing event occurred at or above the target assurance level of the workflow.	
11	63A	4.4.1	15	684	Consider specifying that varification through demonstrated control of a digital account should be an account of comparable assurance levels. (This may be part of the implementation guidance rather than normative.)	
12	63A	5.1.1	17	723	Consider adding another aspect of what the CSP has to define, which would be the presentation of any metrics and performance statistics as defined by the RP agency and/or NIST. It would be good for the agency to understand CSP average pass rates and evolution thereof, in particular from the perspective of meeting equity requirements. As an example - CSPs should through regular intervals update their RPs proactively on proofing outcomes across different demographics and proofing pathways. In doing so, and especially in multi-CSP arrangements, agency RPs can evaluate to what extent their contracted CSPs are contributing to equitable access to government services (cf. Executive Order 13985) and hold those CSPs accountable for shortfalls.	
13	63A	5.1.2.1	17	747	The privacy risk assessment process described in this section is robust. NIST may wish to consider broadening the section or adding a short introduction refereincing the definition of PII, which includes information that could be combined to be able to identify someone uniquely within a population. This definition is a critical aspect of preserving privacy especially in the context of AI/ML models, which gather large amounts of data that may be innocuous on its own but is somewhat ambiguous as to the exact moment it becomes enough to uniquely identify an individual.	
14	63A	5.1.5	20	848	The addition of guidance around rollout and communications is clear and helpful.	

15	63A	5.1.6	21	869	NIST may wish to consider being more prescriptive around how to validate an email address of record. This is a common fraud vector, and especially with the new requirements allowing the enrollment code as verification at IAL1, measures should be undertaken to ensure more confidence in the email address of record.	
16	63A	5.3.3	27	1068	There may be additional ways to validate FAIR evidence in practice beyond visual inspection. For example, it is common among CSPs to use a validated phone number as FAIR evidence. NIST may wish to weigh the benefit of including such practices in the implementation guide.	
17	63B	4.2.2	9	539	NIST may wish to consider including one phishing resistant option as a SHALL rather than a SHOULD to urge agencies to comply with recent Federal policy.	
18	63B	5.1.1.2	16	732	The requirements to remove composition rules and rotation requirements are helpful and appropriate.	
19	63B	5.2.3	33	1282	NIST may wish to consider including a False Non-Match Rate in this section to match the biometrics requirements from 63A.	
20	63B	5.2.3	33	1303	NIST may wish to clarify the "certification by an approved accreditation authority"- would this be agency-approved? OMB perhaps?	
21	63B	6.2	N/A	N/A	NIST may wish to include guidance on how to calculate a risk score for authentication types, which would factor into a zero-trust model. This could include aspects like: geolocation, behavioral patterns if available, authenticator type, etc.	
22	63B	7.1	48	1829	NIST may wish to consider highlighting that this requirement precludes the use of a "remember my browser" feature as this can sometimes be a default product option.	
23	63C	4.4	9	N/A	Having fixed definitions for assurance levels is critical for federated interoperability among agencies. However, with a variety of options including risk-based decision-making at agencies, it could be helpful to create a standard way to assign a subscriber a risk score based on whether they underwent a fully compliant proofing/authentication flow or if they underwent proofing at an agency/Credential Service Provider/workflow that accepts compensating controls. The score could comprise aspects such as: number of compensating controls present in the workflow or user journey; number of steps a user did not undertake (for example if an international user's information could not be validated); or if any suspected fraud flags were raised throughout the process. This risk score could be associated with the subscriber account and then passed as an attribute along with the assurance level. See also: 63A Section 6.1.	
24	63C	5.1	13	N/A	NIST may wish to consider adding guidance or a reminder in 63C around classifying appropriate accounts that can fulfil the IAL2 verification requirement, when setting up a trust framework with these entities. See also: 63A Section 6.1.	
25	63C	5.1.2	15	707-710	We encourage NIST to be more prescriptive on Multilateral Trust Agreements. The current language "the federation authority conducts some level of vetting on each party in the federation to verify compliance with predetermined standards that define the trust agreement" leaves significant room for ambiguity (what does "some level of vetting mean"?). Perhaps this ambiguity and flexibility was exactly the intent, but we request for NIST to specify this vetting more by providing more prescriptive language, and ideally champion and make available to agencies a Multilateral Trust Agreement playbook, perhaps in collaboration with GSA (the latter as the publisher of other prescriptive and hands-on FICAM playbooks), or as Conformance Criteria/Implementation Guidance, or a Trust Agreement Profile that agencies can adopt and tweak for their use cases. See also our related comments (#25) related to 63C, Section 4.4 page 9	
26	63C	5.1	13, 14	628 - 637	With the introduction of a "core attributes" in 63A 5.1.1 item 4, we like for NIST to increase textual alignment with the "set of attributes" that is featured in 63C 5.1. Is the intent of the 63C 5.1 Trust Agreement to also prescribe the definition of a core attribute bundle within the federation? If so - we kindly request more clarity and alignemnt between the 63A and 63C Sections on that.	
27	63C	5.4	24	N/A	One challenge agencies may begin to encounter is information sharing in a multi-CSP environment. Questions around how to share potential fraud and coordinate the blocking of suspicious or malicious accounts across two or more CSPs are complex. NIST may wish to consider adding some guidance in the implementation guide for leading practices in this area. See also: 63A section 7.2.	
28	63A	5.1.9.1	24	993	NIST may wish to include implementation examples for how to identify and train Trusted Referee representatives and/or types of processes to work with an applicant reference. The list of use cases in which both could be used is a good start. Agencies may benefit from examples, especially involving TR/AR at the IAL3 in person or supervised remote level.	Add implementation guidance around using Trusted Referees and Applicant References, and detail out sample processes for engagement.
29	63-Base	7.1	17	1314	Have supply chain risks and threats been factored in as requirements for CSP assessments? How do we assess a third-party subcontractors and vendors?	Add in language on CSP Supply Chain Risk Management assessment, such as requiring CSPs to provide an SBOM.
30	63-Base	N/A	N/A	N/A	Rev 4 does not provide clear traceability to latest, relevant, and applicable ICAM guidance from other NIST publications, EOs, DHS, and OMB guidance (e.g., M-19-17). As a result, it is challenging for agencies to establish standardized ICAM policy consistent with all available guidance and challenging to assess effectiveness in ICAM capabilities.	Develop a matrix of ICAM requirements/guidance similar to the CSF's informational references section.

Department of Education Comments for: NIST SP 800-157

Please submit responses internally by 2/17/2023

#	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change	Your Name (Will not be submitted to NIST - just for internal follow-up)
1	1.6	4	362	The term subscriber - aligns with most NIST publications but there may be a few instances of confusion, for example in the glossary of 800-72 ("An individual applying for a Derived PIV Credential") versus someone who already has the derived PIV credential in hand.		
2	2	5	380	In Figure 1, is there a way to indicate that non-voluntary termination of a DPC may get flagged for a review of the PIV as well? This could be in instances of suspected fraud or misuse of the DPC; the PIV account may wish to be monitored as well.		
3	2.1	6	395	When a non-PKI authenticator is lost, stolen, or damaged, does the credential being invalidated on the issuer side remove the DPC altogether similar to a re-key event, or could it be revalidated without having to undergo the issuance process again?		
4	2.2	7	436	It may be good to provide examples of how to notify the PIV holder that a DPC has been issued; and are there requirements around this process, e.g. it would have to go to a validated address of record?		
5	2.2.1	8	461	It's implied, but at AAL2, it might be good to specify that the public/private keypair for the DPC is different than the keypair created for the PIV itself.		
6	2.2.2	8	476	Including the FIPS 140 requirements may rule out non-certified FIDO authenticators.		
7	N/A	N/A	N/A	General - are there special requirements or guidance around the use of DPCs for physical access? Is this up to the issuing agency?		
8	2.3.1	9	513	In the event of a name change, does the subscriber need to undergo the binding process again, or is the certificate just updated?		
9	2.4	10	538	Tracking the termination status of a PIV card is indeed a large challenge for PKI management. Maybe include a line to indicate that agencies should have processes in place to routinely cross-check for expired, revoked, or invalidated accounts with active PKI-based DPCs attached.		
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						
33						
34						
35						
36						
37						
38						
39						
40						
41						
42						
43						
44						
45						
46						
47						

Department of Education Comments for: NIST SP 800-217

Please submit responses internally by 2/17/2023

#	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change	Your Name (Will not be submitted to NIST - just for internal follow-up)
1	General	N/A	N/A	No additional comments on this document that have not already been identified in comments for SP 800-157.		
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						
33						
34						
35						
36						
37						
38						
39						
40						
41						
42						
43						
44						
45						
46						
47						