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:	*Department of Justice*
Name of Submitter/POC:	*Devin Powers*
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63A	2.1.2	7	555-571	Clarify the difference between a trusted referee and a proofing agent: the trusted referee is empowered by the CSP to make deviations from the required evidenced following pre-established guidelines. Yes, there may be some difference in training, but both need fraud and social engineering detection skills.	Add language about training to end of proofing agent definition. Add language about deviations to definition of trusted refere
2	63A	2.4.1.3	12	720-721	Enrollment should only be onsite attended for superior evidence, not remote attended. Given the rise of deepfake technology and how easy it is for bad actors to impersonate their victims and socially engineer live service desk workers, superior evidence should only be given to those people who must go onsite to obtain the evidence (e.g., DMV, PIV office, etc.)	"The issuing source had the subject participate in an onsite attended enrollment..."
3	63A	2.5.1	14	795	denotes "attended" but does not denote co-location as referenced in the base volume; is this intentional and why?	
4	63A	2.5.1	14	784-786	Returning a confirmation code is not a strong enough piece of evidence. It does not prove that the applicant is more than likely than not the claimed identity at IAL2 or IAL3; it could be acceptable for IAL1, as that level of assurance is considerably weaker. Because the section requires "one or more" method, this evidence alone should not be considered enough to verify the linkage of the applicant to the identity	Remove these lines
5	63A	2.5.1	14	799-808	Visual facial image comparisons should only be conducted at the time the person presents the evidence (i.e., attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect potential fraud, ask the applicant questions, and observe the applicants facial movements to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a deep fake could easily pass a proofing agent who reviews the evidence after capture.	"Remote (Attended) visual facial image comparison. The (*trusted referee (see comment above on necessity of social engineering*
6	63A	3.1.2.1	18	857	What is the scope of the term used "addressing"; as in steps to continue the identify proofing after remediation of noted errors and/or policy SHOULD include methods for addressing ID Proofing errors?	
7	63A	3.1.2.1	18	907	Recommend considering including other fraud check techniques: device fingerprinting and correlation, VPNs and proxy servers, predictive analytics	
8	63A	3.1.2	19	932	Draft states CSPs may employ knowledge-based verification (KBV) as a part of its fraud management program; however, 2.5.1 states KBV shall not be used for identity verification. The guidelines appear to suggest KBA can be used as a component to assess the overall fraud risk, but not as a component to verify a user's identity (which is a component of verifying fraud risk). Seems like competing statements.	Provide clarity and consider updating language so that CSP has a clear understanding of when KBV can/not be used.
9	63A	3.1.2.1	19	949	first use of the term "Digital Identity Acceptance Statement" between CSP and RP; no further delineation of this statement outside of the statement denotes deviation from this standard's guidance which ultimately leaves interpretation of the deviation to the CSP and/or RP; should there be more codification or example of a deviation that warrants this statement to be documented and provided?	
10	63A	3.1.2.2	19	954	Is this intended to imply CSPs cannot collect additional attributes to support fraud mitigation? Recommend clarifying that the CSP can collect additional attributes, even if the RP should only request the core, except for these fraud exceptions in this clause	Add similar language to 3.1.2.1
11	63A	3.1.2.3	20	989	#3 assumes that "failed fraud checks in unattended remote checks" automatically meet the "exceptions" that require an elevation to a Trusted Referee and negates the possibility/opportunity for Proofing Agents to address the more commoditized remediations unless you're assuming all fraud checks with the CSP necessitate a risk-based assessment and decision.	
12	63A	3.1.3.1	21	1038	"If SSNs are collected, CSPs SHOULD..." as a recommendation, why not SHALL to make it a requirement per these guidelines?	
13	63A	3.1.8	25	1159	21 days for CONUS but 30 for OCONUS? Not sure this is enough time for postal mail delivery OCONUS. Is 30 days fed by metrics of average delivery time or maximum delivery duration for OCONUS locations (i.e., embassies or military bases).	Suggest additional 2 weeks for total of 35 days.
14	63A	3.1.8	26	1162	24 hours is too long or email.	Lower 24 hours to 1 hours
15	63A	3.1.9	26	1164	Authentication at an appropriate AAL is sufficient as an option as well	Authentication at a corresponding AAL or higher is sufficient to obviate the need for a continuation code
16	63A	3.1.9	26	1174	By which methods can the CSP deliver the code?	
17	63A	3.1.13.2	32	1394	No reference is made to include option for updating list of use cases that are eligible for use of the trusted referee.	Include SHOULD statement to allow for CSPs options for documenting and updating list of eligible use cases for Trusted Referee.
18	63A	3.1.13.5	34	1460	Applicant References are themselves identified individuals. Mention is made for certifying validity of the applicant reference (prof cert/power of attorney), but not the validity of the individual. Should there be a section similar to the other roles (Proofing Agent, Trusted Referee) that denotes this validity?	Suggest inserting clause or note on validating the applicant references as well.
19	63A	3.2	35	1490	Subscribers should have to authenticate at the AAL that corresponds to the upgraded identity, not the highest.	Authenticate at an AAL at or higher than the upgraded IAL
20	63A	4.1.10	39	1625	Authenticators can also be bound prior to the proofing event	before, at the time of, or after the proofing event

21	63A	4.2	40	1648	If biometrics are optional at IAL2 then an agency that requires biometrics for security reasons will not be able to accept an IAL2 credential that was established by an agency with a higher risk tolerance. This breaks the consistency and trust that enables federation.	Either require biometrics for IAL2 or split IAL2 so that the use of biometrics during identity proofing is clearly captured and transmitted to all RPs so they can make a decision on its use or absence, and make sure the pathways are clearly marked such as IAL2-B (biometrics) and IAL2-O (other). These two pathways are *not* equivalent from a security and fraud-deterrence perspective. The non-biometric pathway is highly vulnerable to attack by family members, caregivers, and acquaintances, which can lead to devastating financial and life consequences for disabled beneficiaries and the elderly who rely on their benefits. Capturing the facial image of the individual who is applying for benefits is a strong deterrent to impersonation, particularly for individuals who are personally acquainted with a victim. There is no equivalent deterrent in the non-biometric pathway. Individuals with common names are also highly vulnerable to attacks when address verification is used for proofing without sufficient additional controls. Records may show that a number, email address, or home address is strongly associated with a James Smith, for example. There are 38,313 James Smith's in the United States. This is a common attack that is happening at scale today. https://www.statista.com/statistics/279713/frequent-combinations-of-first-and-last-name-in-the-us/
22	63A	4.2.6.1	42	1716-1724	FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence.	Remove the requirement for FAIR evidence
23	63A	4.2.6.1	42	1720-1724 & 1730-1734	The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security.	Add a sentence that indicates that these are not equivalent in terms of fraud prevention.
24	63A	4.3.3	45	1804	Self-assertion to meet core attributes leaves opportunity for risk-based decision to be skewed as a result. Self-asserted attributes inherently carry risk due to social engineering or relational spoofing.	Strike "it MAY collect attributes that are self-asserted by the applicant."
25	63A	5.1	50	1941	The type of proofing should be for each piece of evidence and step in the process.	Type of proofing for each type of identity evidence
26	63A	A.2 Table 5	78	2728	When not validated, the passport is on par with a driver's license (Sec. 4.2.4). Passport should be in SUPERIOR only when NFC chip is read.	Add Passport to "STRONG", when only visual inspection is used.
27	63A	A.1	78	2728	Consider adding a column for allowable proofing type. For instance, is SSN acceptable if remote so long as it's presented as an image of a card and not just the number?	
28	63B	3.2.2	28	1216	100 attempts is too high.	Suggest reducing the amount of attempts to below 100.
29	63B	5.2	51	1986	"Consequently, when an RP session expires and the RP requires reauthentication, it is possible that the session at the IdP has not expired and that a new assertion could be generated from this session at the IdP without explicitly reauthenticating the subscriber." This consideration does support the reauthentication requirements (24/10/1); and it is assumed assertion channels from the IdP to RP are secure as stated earlier in the 2DP; however, does this limit the probability of impersonation between the IdP and RP if IdP is provisioned this functionality? It should be mentioned that the RP termination and subsequent reassertion should trump IdP session to meet RP requirements rather than the IdP requirements as a fail-safe.	Include MAY/SHOULD statement to combat this use case.
30	63B	1	1 & 2	403-413	In the introduction, NIST recommends "applications assessed at AAL1 offer" MFA, which suggests that AAL1 is barely a "basic confidence" assurance level. More strongly, NIST requires "applications assessed at AAL2 must offer a phishing-resistant authentication option." While this is a great mandate, if an application has both phishable and phishing resistant authenticator options, the application continues to be phishable and the phishing-resistant option mandate loses its purpose - to effectively protect against phishing attacks. Additionally, federation assertions don't always assert whether an authenticator was phishing resistant or not, just that it was MFA/2FA, so adding an additional AAL would create a need for vendors to insert greater veracity in their assertions. As such, phishable MFA should become AAL1, AAL2 should be phishing resistant and an AAL0 should be created to allow for single factor authentication scenarios.	Create an AAL0 that is a low assurance and allows for single factor; AAL1 should become phishable MFA, whereas AAL2 shoul

31	63B	3.1.7.1.			Improve guidance readability as to if Multi-Factor Cryptographic Authenticators can be non-exportable and "syncable". In section 3.1.7, guidance is key cannot be exported - "Depending on the strength of authentication needed, the private or symmetric key may be stored in a manner accessible to the endpoint being authenticated or in a separate, directly connected processor or device from which **the key cannot be exported**." In section 3.1.7.1, guidance seems to imply key can be exportable by this "OR" clause - "The key SHOULD be stored in appropriate storage available to the authenticator (e.g., keychain storage), **or if the key is to be non-exportable**, it SHALL be stored in an isolated execution environment protected by hardware or in a separate processor with a controlled interface to the central processing unit of the user endpoint." Further in section 3.1.7.1, guidance implies some Multi-Factor Cryptographic Authenticators can be "syncable" - "**Some cryptographic authenticators, referred to as "syncable authenticators,"** can manage their private keys using a sync fabric (cloud provider). Additional requirements for using syncable authenticators are in Appendix B." Then in Appendix B, guidance states syncing violates non-exportability requirements of AAL3 which Multi-Factor Cryptographic Authenticators are a permitted type. - "Syncing authentication keys inherently means that the key can be exported. Authentication at AAL2 may be supported subject to the above requirements. However, **syncing violates the non-exportability requirements of AAL3**. Similar protocols using keys not stored in an exportable manner that meet the other requirements of AAL3 may be used."	Suggest striking "The key ~~SHOULD be stored in appropriate storage available to the authenticator (e.g., keychain storage), or if the key is to be non- exportable, it~~ SHALL be stored in an isolated execution environment protected by hardware or in a separate processor with a controlled interface to the central processing unit of the user endpoint." And striking "~~Some cryptographic authenticators, referred to as "syncable authenticators," can manage their private keys using a sync fabric (cloud provider). Additional requirements for using syncable authenticators are in Appendix B.~~"
32	63-Base	1	1	362	Typo	an organization
33	63-Base	2.5	21	913	Does step 6 need to be a 2 way Federation protocol per Figure 5? At the point that the Subject has gone thru federated activation of the authenticator held by the Subscriber, RP is just ingesting the attribute bundle from the wallet to complete the authenticated session. Unless the intent is for the RP to communicate back to RP for further validation? Step 6 is described as a one direction ingestion by the RP of the digital wallet assertion/attribute bundle.	modify language of the bidirectional nature of the Federation protocol OR modify figure 5 to match the narrative.
34	63-Base	3.1	27	1090	"estimated availability", shouldn't this be "established availability" for the forms of identity evidence to address storage of possible PII?	established availability
35	63-Base	3.1	28	1120	"all impacted" assumes the system user groups and impacted entities are fully characterized; this also assumes a bit of supply chain risk management as tertiary and above impacted entities SHALL be fully documented. Is it the intent of this SP to enforce SCRM aspects in its impact assessments to an unknown degree? Or should this statement say "all identified impacted entities"?	all identified impacted entities
36	63-Base	3.1	28	1123	"directly impacted" or "indirectly impacted?	directly or indirectly impacted
37	63-Base		34	1347	AAL is defined later in the document as "the level of assurance that the claimant is the same individual to whom the credential or authenticator was issued."	Recommend replacing: "The robustness of the authentication process itself, and the binding between an authenticator and a specific individual's identifier." with "the level of assurance that the claimant is the same individual to whom the credential or authenticator was issued."
38	63-Base	3.3.2.1	35	1358	Given the significance of the change, call out that no identity proofing is no longer IAL1. There should be an IAL0 so it can be recorded properly when agencies do assessments vs. when they do not.	Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities ar
39	63-Base	3.2.2	36	Table 2:AAL2	"Support" for MFA is not the same as an MFA requirement.	Change "Support multifactor authentication" to "Requires multifactor authentication" or "Enforces…"
40	63-Base	3.2.2	36	Table 2:AAL3	"Providing" (the option of) phishing resistance is not the same as a phishing resistance requirement.	Change "Provide phishing resistance" to "Requires phishing resistance"
41	63-Base	3.4	39	1505	Standard recommends (should) the tailoring process for the xALs, but then requires (shall) pieces of the tailoring documentation. This assumes that the CSP committing to the tailoring based on their population of RPs is subject to the prescribed standard for the tailoring process of the controls, both supplemental and compensating, whereas the CSP may just opt for the more standard approach for a unified control set without any tailoring and leave it to the RPs to provide address the supplemental/compensating controls. This places a good bit of burden on the RPs seeking integration with the CSP.	replace all "shall" statements in the 3.4 to "should"
42	63-Base	3.4.1	42	1581-1591	Consideration of "known threats" based on current set of TTPs negates the opportunity for continued threat assessments for an evolving threat landscape.	specific, known, and potential threats
43	63-Base	3.4.4	44	1648-1662	Impact assessments are already done for application ATOs; however, in order to associate applications (RP) to a CSP, additional compensating controls need to be identified based on xALs for that RP. This is an added burden to the RPs seeking to integrate with the CSP.	
44	63-Base	3.4.4	44		"initially assessed xALs" are required in a DIAS, which is required to be created by a CSP. This requirement doesn't make sense for CSPs, as CSPs should not be assessing what the xAL should be for a given RP. While the CSP can help the RP create the xAL assessment, CSPs must create workflows to meet their customer's needs, which means their assessed xALs, tailored xALs, and compensating controls will be determined by their customers - the RPs - not by the CSPs themselves.	Remove requirements for CSPs to create aDIAS; keep the requirement to aid RPs in creating their DIAS
45	63-Base	3.5	45	1686	"shall" statements for actions an organization may or may not have the capacity to address; agreed organizations, especially those supported by IT systems governed by FISMA have an obligation to address these activities; however, either consider "should" OR corroborating "may" statement(s) allowing for organization to transfer these actions to supporting organizations.	should

46	63-Base	3.1			Scale of impact is a critical missing element from the user group discussion, which focuses exclusively on role. Similarly, the impacts on the organization/application itself also needs to be assessed, as well as any other impacted entities.	Update impact review
47	63C	1	1	403-407	While a digital wallet could be used as an IdP, it's not advised to be used as one.	Remove subscriber-controlled device as an IdP.
48	63C	2.5	7	600	The lowest IAL in the guidelines is IAL0 (no proofing), not IAL1.	Change IAL1 to IAL0
49	63C	3.1.2	11	688-689	Because there are two distinct places where identity evidence is stored on behalf of the subscriber of digital identity wallets (device or the cloud), a wallet should not be protected just by an activation factor (PIN/password) if a subscriber-controlled wallet doesn't require a private key (which is the case for mDLs).	Remove either the presentation of an activation factor and/or of subscriber-controlled wallets in Section 3
50	63C	3.4	17	896-897	How does a trust agreement "establish usability and equity requirements" in a federation transaction? To the user, they are only operating with the RP and, in some cases, will be able to understand that they are also using another vendor's program. Because a federated transaction is basically based on protocols, how can we ensure that those universally standardized protocols hit "usability and equity" requirements?	Remove or change to a SHOULD statement
51	63C	3.4	17	897-899	While the trust agreement should include details of the proofing process, adding compensating controls and exception processes to the trust agreement could be a security issue if the trust agreement is required to be public.	Suggest changing SHALL to SHOULD
52	63C	3.5.2	22	1064-1072	The use case presented in this paragraph to reach FAL3 negate the Usability factors of the standard and intent of the digital-wallet in the first place. Ultimately, this equates to the end-user having an additional appliance to meet FAL3, thus wouldn't digital-wallets evidently never be driven to meet FAL3 as CSPs and IdPs would never take this into consideration for their end-user workflow? Agreed that for FAL3, this is a necessity, but in real life practice, this may be difficult to execute.	
53	63C	3.11.2	32	1408-1422	Should a digital-wallet, considered an IdP in some transactions, be held to the same requirements set forth in 3.11.2 for derived attributes?	Include clarifying language in digital wallet section around the attribute bundles similar to these requirements when the wallet is acting as the IdP to some degree.
54	63C	3.14	37	1568-1569	How would an RP know that the assertion has a "phishing resistant" authenticator when technology vendors do not transmit that level of veracity on authentication assertions?	Create a new AAL - AAL0, which would be for single factor authenticators; AAL1 would be for MFA phishable, AAL2 would be
55	63C	4.8	62	2297 & 2306	It is critical that RPs and IdPs be informed when either suspects that an account has been compromised, especially when RPs are involved that hold highly sensitive data or allow access to funds.	2297 - Remove this item from the 'SHOULD' list and change to: "The IdP **SHALL** send a signal **or other notification** regarding any subscriber account suspected of being compromised." 2306 - "The RP **SHALL** send a signal **or other notification** regarding any subscriber account suspected of being compromised."
56	63C	4.9	64	2364-2365	There are instances in these guidelines where phishing resistant authenticators are required, yet they do not have their own assurance level.	Either move the "authentication event" into the SHALL statement of the assertion on line 2348 or do the more sensible change
57	63C	5.1	69	2507	An activation factor should always be required before any operation that is using a wallet's signing keys is involved.	change SHOULD to SHALL