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	

			_			
	Publication				Comment	
Comment #	(Base, 63A, 63B, 63C)	Section	Page !	# Line #	(Include rationale for comment)	Suggested Change
					Clarify the difference between a trusted referee and a proofing agent: the trusted referee is	
1 1					empowered by the CSP to make deviations from the required evidenced following pre-established	
1 1			ı	1	guidelines. Yes, there may be some difference in training, but both need fraud and social engineering	
16	53A	2.1.2	7	7 555-571	detection skills.	Add language about training to end of proofing agent definition. Add language about deviations to definition of trusted refere
					Enrollment should only be onsite attended for superior evidence, not remote attended. Given the rise	
1 1			ı	1	of deepfake technology and how easy it is for bad actors to impersonate their victims and socially	
1 1			ı	1	engineer live service desk workers, superior evidence should only be given to those people who must	
	53A	2.4.1.3	_	720-721	go onsite to obtain the evidence (e.g., DMV, PIV office, etc.)	"The issuing source had the subject participate in an onsite attended enrollment"
E	53A	2.5.1	14	795	denotes "attended" but does not denote co-location as referenced in the base volume; is this intentional and	
3			-		why?	
1 1			ı	1	Returning a confirmation code is not a strong enough piece of evidence. It does not prove that the	
1 1			ı	1	applicant is more than likely than not the claimed identity at IAL2 or IAL3; it could be acceptable for	
1 1			ı	1	IAL1, as that level of assurance is considerably weaker. Because the section requires "one or more"	
را.			l	704 705	method, this evidence alone should not be considered enough to verify the linkage of the applicant to	la
4 6	3A	2.5.1	14	784-786	the identity	Remove these lines
1 1			ı	1		
		1	ı	1	Visual facial image comparisons should only be conducted at the time the person presents the evidence	1
1 1			ı	1	(i.e., attended sessions only). Proofing agents need to be trained enough in social engineering to be	
1 1			ı	1	able to detect potential fraud, ask the applicant questions, and observe the applicants facial	
1 1			ı	1	movements to detect possible fraudulent activities. This would not be available in unattended sessions,	
راء ا			l	700 000	and without the ability to biometrically compare the photographic evidence, a deep fake could easily	Language and the control of the cont
	53A	2.5.1	_	799-808	pass a proofing agent who reviews the evidence after capture. What is the scope of the term used "addressing"; as in steps to continue the identify proofing after remediation	"Remote (Attended) visual facial image comparison. The (trusted referee (see comment above on necessity of social engineerin
اء ا	53A	3.1.2.1	18	857	of noted errors and/or policy SHOULD include methods for addressing ID Proofing errors?	
<u> </u>			-	+	Recommend considering including other fraud check techniques: device fingerprinting and correlation,	
7 6	53A	3.1.2.1	15	907	VPNs and proxy servers, predictive analytics	
	53A	3.1.2	19	932	Draft states CSPs may employ knowledge-based verification (KBV) as a part of its fraud management	Provide clarity and consider updating language so that CSP has a clear understanding of when KBV can/not be used.
1 1		3.1.2	13	332	program; however, 2.5.1 states KBV shall not be used for identity verification. The guidelines appear to	Trovate clarity and consider apparating language so that con has a clear understanding of when how carry not be used.
1 1			ı	1	suggest KBA can be used as a component to assess the overall fraud risk, but not as a component to	
1 1			ı	1	verify a user's identity (which is a component of verifying fraud risk). Seems like competing statements.	
8			ı	1	verify a user's identity (which is a component of verifying flaud risk), seems like competing statements.	
- 6	53A	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	
1 1			ı	1	interpretation of the deviation to the CSP and/or RP; should there be more codification or example of a deviation	
9					that warrants this statement to be documented and provided?	
1 1			ı	1	Is this intended to imply CSPs cannot collect additional attributes to support fraud mitigation?	
1 1			ı	1	Recommend clarifying that the CSP can collect additional attributes, even if the RP should only request	
10 €		3.1.2.2	19		the core, except for these fraud exceptions in this clause	Add similar language to 3.1.2.1
	53A	3.1.2.3	20	989	#3 assumes that "failed fraud checks in unattended remote checks" automatically meet the "exceptions" that	
1 1		l	1		require an elevation to a Trusted Referee and negates the possibility/opportunity for Proofing Agents to address	
11		1	ı	1	the more commoditized remediations unless you're assuming all fraud checks with the CSP necessitate a risk- based assessment and decision.	
	53A	3.1.3.1	21	1038	based assessment and decision. "If SSNs are collected, CSPs SHOULD" as a recommendation, why not SHALL to make it a requirement per these	
12	nan.	3.1.3.1	21	1030	guidelines?	
	53A	3.1.8	25	1159	21 days for CONUS but 30 for OCONUS? Not sure this is enough time for postal mail delivery OCONUS.	Suggest additional 2 weeks for total of 35 days.
] [-	I	Ī	1	Is 30 days fed by metrics of average delivery time or maximum delivery duration for OCONUS locations	
13		l	l		(i.e., embassies or military bases).	
14 6	53A	3.1.8	26	1162	24 hours is too long or email.	Lower 24 hours to 1 hours
15 6		3.1.9	26		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 6		3.1.9	26		By which methods can the CSP deliver the code?	
	53A	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	Include SHOULD statement to allow for CSPs options for documenting and updating list of eligible use cases for Trusted
17				1	trusted referee.	Referee.
	53A	3.1.13.5	34	1460	Applicant References are themselves identified individuals. Mention is made for certifying validity of the	Suggest inserting clause or note on validating the applicant references as well.
1 [1	1	1	applicant reference (prof cert/power of attorney), but not the validity of the individual. Should there be	
1 1		l	l		a section similar to the other roles (Proofing Agent, Trusted Referee) that denotes this validity?	
18		l	l			
		1			Subscribers should have to authenticate at the AAL that corresponds to the upgraded identity, not the	
19 6	53A	3.2	35	1490	highest.	Authenticate at an AAL at or higher than the upgraded IAL
20 €	53A	4.1.10	39		Authenticators can also be bound prior to the proofing event	before, at the time of, or after the proofing event
		•				

						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
					If biometrics are optional at IAL2 then an agency that requires biometrics for security reasons will not	associated with a James Smith, for example. There are 38,313 James Smith's in the United States. This is a common attack
21	63A	4.2	40	1648	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.	that is happening at scale today. https://www.statista.com/statistics/279713/frequent-combinations-of-first-and-last-name- in-the-us/
	05/1			1010	FAIR evidence doesn't require facial images, and therefore should not require biometric or non-	in the day
22	63A	4.2.6.1	42		biometric methods to verify the evidence.	Remove the requirement for FAIR evidence
				1720-1724		
22	63A	4.2.6.1	4-	& 1730- 2 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.
23	63A	4.3.3	45	1804	Self-assertion to meet core attributes leaves opportunity for risk-based decision to be skewed as a	Strike "it MAY collect attributes that are self-asserted by the applicant."
					result. Self-asserted attributes inherently carry risk due to social engineering or relational spoofing.	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
24						
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.
	05/1	7 ILL TUBIC 5	,,	2,20	Consider adding a column for allowable proofing type. For instance, is SSN acceptable if remote so long	
	63A	A.1	78		as it's presented as an image of a card and not just the number?	
28	63B	3.2.2	28		100 attempts is too high.	Suggest reducing the amount of attempts to below 100.
	63B	5.2	51	1986	"Consequently, when an RP session expires and the RP requires reauthentication, it is possible that the	Include MAY/SHOULD statement to combat this use case.
					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.	
29					meet in regularities rather and the later equinements as a fair safe.	
					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	
30	63B	1	1 & 2	403-413	single factor authentication scenarios.	Create an AALO that is a low assurance and allows for single factor; AAL1 should become phishable MFA, whereas AAL2 should
				•		

In section 3.17, guidance is key cannot be exported. "Depending on the strength of authentication needed, the private or in a separate, directly connected processor or device from which the key cannot be exported." In section 3.17, guidance seems to imply key can be exportable by the "Off" clause. "The key SHOULD be stored in a propriete storage available to the authentication processing unit of the use of the private or in a separate, directly connected processor or device from which the key cannot be exportable. If SHALL be stored in a propriete storage available to the authentication, or if the key is to be non-exportable, it SHALL be stored in an absolated execution environment protected by hardware or in a separate processor with a controlled interface to the explanation goes in the separate provide in separate processor with a control interface to the explanation goes in the explanation of the user endopoint." Turber in a section 3.17.1, guidance implies some Multi-factor Cryptographic Authentications are provided in the section of the user endopoint. Turber in appendix 8, guidance states syncing violates non-exportability requirements for using synciable authentications are in appendix 8. Then in Appendix 8, guidance states syncing violates non-exportability requirements of AAL3 which have become requirements. The voice, syncing switched in an exportability requirements of AAL3 which have become requirements. The voice, syncing switched in an exportability requirements of AAL3 which have become requirements. The voice spendig switched in an exportability requirements of AAL3 which have become requirements. The voice spendig switched in an exportability requirements of AAL3 which have become requirements. The voice spendig switched in an exportability requirements of AAL3 which have become requirements of the switched or a control of the switched or an exportability spendigment or the switched or an exportability spendigment or the switched or an exportability spendigment or the switched or an exporta	63B	3.1.7.1.	Improve guidance readability as to if Multi-Factor Cryptographic Authenticators can be non-exportable	Suggest striking "The key SHOULD be stored in appropriate storage available to the authenticator (e.g., keychain storage), or
In section 3.1.7, guidance sites ye amont be copyrided. "Propriet price to the original half-broked and an account of the control or number of the price of the properties of the original half-broked and a section of the control or number of the sequence of the properties of the pro	035	51277121		if the key is to be non exportable, it SHALL be stored in an isolated execution environment protected by hardware or in a
needed, the private or symmetric tay may be Stored in a manner recessible to the exploit band submittation of the support development of the support of the				separate processor with a controlled interface to the central processing unit of the user endpoint."
submitted or in a soparate, directly connected processor of order for this the key cannot be experted. In section 3.1.1, guidance seams to imply key can be opportable by the "Ord" date. "The key SOULD best bord in appropriate leave the programment of the source of the programment of the processor of the programment of the source			In section 3.1.7, guidance is key cannot be exported - "Depending on the strength of authentication	
reported.* In section 3.1.3.1, printense seem to imply lay on the important by this 1/04" dates. "The lay stouched by the seed of the see				And striking "Some cryptographic authenticators, referred to as "syncable authenticators," can manage their private keys
In section 3.1.7.1, guidance seems to might key can be exportable by this "Off clause - "The key SHOUD be stored in appropriate storage enables for the authenticate fee, servicinis storaget, or if he key should be stored in appropriate storage enables for the sufferior to the central precessing out of the stored enables of the stored and the stored enables of the stored and the stored enables of the stored and the stored a				using a sync fabric (cloud provider). Additional requirements for using syncable authenticators are in Appendix B."
between the beautiful processing and interest of the heavy to be one experience. If the beautiful processing until of the heavy to be one experience. If the beautiful processing until of the user of impairs. Further in section 3.1.3 is, guidence implies some Multi-Factor Cryptographic Authenticators can be "synciated authenticators", can manage that private lays using a sync fairs (cloud procedur). Additional requirements for using younged authentications, referred on a synchrole authenticators, and in manage that private lays using a sync fairs (cloud procedur). Additional requirements for surge younged authentication are in processing until or surgery of the processing until or surgery or surg			exported."	
between the beautiful processing and interest of the heavy to be one experience. If the beautiful processing until of the heavy to be one experience. If the beautiful processing until of the user of impairs. Further in section 3.1.3 is, guidence implies some Multi-Factor Cryptographic Authenticators can be "synciated authenticators", can manage that private lays using a sync fairs (cloud procedur). Additional requirements for using younged authentications, referred on a synchrole authenticators, and in manage that private lays using a sync fairs (cloud procedur). Additional requirements for surge younged authentication are in processing until or surgery of the processing until or surgery or surg			In section 3.1.7.1 guidance seems to imply key can be exportable by this "OR" clause - "The key	
the key is to be non-exportable, it shall, be stored in an solidad execution environment protected by hardware or in a separate processing of the law cereapont." In the separate processing of the law cereapont of the law cereapont. It is a separate processing of the law cereapont. It is a separate processing of the law cereapont. It is a separate processing of the law cereapont. It is sufficient in separate processing of the law cereapont. It is sufficient in separate for using synchia with the processing of the law cereapont. A distinct and separate for using synchia with the law can be originally a separate for using synchia with the law can be originally a separate for using synchia with the law can be originally separated to the law can be originally requirements of AAA3 which built-factor (hypographic Authenticators are a permitted type. "Sporting authenticator with the law can be originally associated and the law can be originally separated and AAA3 which built-factor (hypographic Authenticators as a permitted type. "Sporting authenticator solidate to the law can be originally associated and AAA3 which built-factor (hypographic Authenticators as a permitted type. "Sporting authenticators with a separate processing authenticator and AAA3 which built-factor (hypographic Authenticators and AAA3 which built-factor (hypographic AAA3 whi				
Further in section 3.1.7.1, guidance implies some Multi-Factor Cryptographic Authenticators can be Synaphic "Some cryptographic authenticators," can specifically authenticators are in Appendix of Synaphic authenticators are in Appendix in Appendix in Synaphic authenticators are in Appendix in				
Further in section 3.1.7.1, guidance implies some Multi-Factor Cryptographic Authenticators can be "syncible". "Some cryptographic authenticators, referred to as "syncible authenticators or an image the Privale law using a synchrol (color produce). Authoris referred to sail syncible outhernicators are in Agrandia. Then in Agrandia & publisher some in Agrandia & publisher some production of the Agrandia of the Agrandia & publisher some as permitted by per. "Syncing authenticators and a Agrandia & publisher some production and ALT may be apported subject to the above requirements of ALT and which Multi-Sector Cryptographic Authenticators are a permitted type. "Syncing authenticators and production and ALT make accounts" 3.1			hardware or in a separate processor with a controlled interface to the central processing unit of the	
"syncable" - "Some cryptographic authenticators, referred to a "syncable authenticators are in Appendix a" Indicator shall be a support of the provide by any production are in Appendix a" Indicator shall be a support of the provide by any production are a permitted type "Synchronic states where you will be a support of the provide shall be a support of the show requirements. However, synchronic shall be a support of the show requirements of AAL3 which Adult factor Cryptographic Authenticators are a permitted type "Synchronic subject to the show requirements. However, synchronic shall be a support of the show requirements of AAL3 which Adult factor Cryptographic Authenticators are a permitted by the short of the show requirements of AAL3 which Adult factor Cryptographic Authenticators are a permitted by the short of the show requirements of AAL3 which are short of the show requirements. However, synchronic short of the shows requirements of AAL3 which Adult factor Cryptographic Authenticators are a permitted by the short of the requirements of AAL3 which Adult factor Cryptographic Authenticator are a permitted by the short of the requirements of AAL3 which Adult factor Cryptographic Authenticator are a permitted by the short of the requirements of the short of			user endpoint."	
syncable "Some cryptographic authenticators, referred to a "syncable authenticators," on ananges there private layer upon downly and plant private syncable authenticators are in Appendix a guidenticators are in Appendix a guidenticators are a permitted type. "Syncable authenticators are permitted bype. "Syncable authenticator bype. "Syncable authent			Further in section 2.1.7.1 guidance implies some Multi-Factor Countegraphic Authenticators can be	
manage their private keys using a sync fibric (loud provider). Additional requirements for using operations and provided by the control of the provided provided by the control of the provided provided provided by the control of the provided provided provided by the control of the provided p				
Then in Appendix B, guidance states syncing violates non-exportability requirements of AAL3 which Multi-Factor Cryptographic Authenticators are a permitted byte. "Syncing authentication keys inherently means that the key can be exported. Authentication keys inherently means that the key can be exported. Authentication keys inherently means that the key can be exported. Authentication keys inherently means that the key can be exported. Authentication keys inherently means that the key can be exported. Authentication keys inherently means that the key can be exported. Authoritication keys inherently means that the process of the specific process. The specific process of t				
Multi-Factor Cryptographic Authentications are a permitted type. "Syncing subrestations legs inherestly means that the key can be exported. Authentication and ALA may be supported subject to the above requirements. However, syncing violates the non-exportability requirements of AAL3. 32			syncable authenticators are in Appendix B."	
Multi-Factor Cryptographic Authentications are a permitted type. "Syncing subrestations legs inherestly means that the key can be exported. Authentication and ALA may be supported subject to the above requirements. However, syncing violates the non-exportability requirements of AAL3. 32				
inherently means that the key can be exported. Authentication at AAL2 may be supported subject to the above requirements. However, symptosic yolialises the non-exportability requirements of AAL3. Similar protocols using keys not stored in an exportable manner that meet the other requirements of 5-8 daise. 2.5 3.6 daise. 2.5 12 1910 2.5 3.6 daise. 2.5 12 1910 2.5 3.6 daise. 3.1 27 1990 4.6 daise. 3.1 27 1990 4.6 daise. 3.1 28 1120 3.6 daise. 3.1 28 1120 3.7 daise. 3.1 28 1120 3.8 daise. 3.1 28 1120 3.9 daise. 3.1 28 1120 3.0 daise. 3.1 38 1120 3.0 daise. 3.1 38 1120 3.0 daise. 3.0 d				
the above requirements. However, syncing violates the non-exportability requirements of AAL3. Similar protocols using leys not stored in an exportable manner that neet the other requirements of AAL3 make users.				
Similar protocols using keys not stored in an exportable manner that meet the other requirements of AAI man be larged and a man be used to be a 2 way Federation protocol per Figure 57 At the point that the Subject has gene this federated activation of the authenticator held by the Subscriber, RPI is just ingesting the authenticator held by the Subscriber, RPI is just ingesting the authenticator of the authenticator held by the Subscriber, RPI is just ingesting the protocol of the federated activation of the authenticator held by the Subscriber, RPI is just ingesting the subscriber to the RPI to communicate back to RPI for further validation? Step is idescribed as an one direction ingestion by the PPI of the display whether a tenth was a step of the subscriber and the PPI of the forms of the PPI of the Grant of the PPI				
31 32 (3 Bases 1 1 362 Type				
63-Base 2.5 21 913 Does step 6 need to be a 2 way Federation protocol per Figure 57 At the point that the Subject has gone thrus federated activation of the submerchated activation of the Subscribe, RP 8) such injection in gestion by the RP of the digital wallet assertion individual control in the Subject has gone thrus federated activation of the submerchated session, unliess the intent is for the RP to communicate bundle. 33 33 34 27 1090 Festimated availability, shouldn't have reliablative bundle. 34 63-Base 3.1 27 1090 Festimated availability, shouldn't his to "established availability" for the forms of identity evidence to address storage of possible PII? 35 63-Base 3.1 28 1120 Festimated availability, shouldn't his be "established availability" for the forms of identity evidence to address storage of possible PII? 36 63-Base 3.1 28 1123 Idriently impacted of Supply chain risk management as tertiary and above impacted entities SHALL be fully documented. Is it the intent of this Street of Supply chain risk management as tertiary and above impacted entities. SHALL be fully documented in the intent of this Street of Supply chain risk management as tertiary and above impacted entities. SHALL be fully documented in the intent of this Street of Supply chain risk management as tertiary and above impacted entities. SHALL be fully documented in the supply of the orders CRAM Street of Supply chain risk management as tertiary and above impacted entities. SHALL be fully documented in the supply of the management as tertiary and above impacted entities. SHALL be fully documented in the supply of the management as tertiary and above impacted entities. SHALL be fully documented in the supply of the more of the supply of the supply of the more of the supply of the su	~-			
gone thur federated activation of 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 lights awalet assertion, activate the work of the RP of the RP of the lights awalet assertion, activate the work of the RP of the RP of the lights awalet assertion, activation and the service of the RP of th	32 63-Base			
attribute bundle from the wallet to complete the authenticated session. Unless the intent is for the RP to communicate back to RP for other walldation? Sidescribed as a one direction ingestion by the RP of the digital wallet assertion/attribute bundle. 3	63-Base	2.5		modify language of the bidirectional nature of the Federation protocol Ok modify figure 5 to match the narrative.
to communicate back to RP for further validation? Step 6 is described as a one direction ingestion by the RP of the digital valies assertion/attivitate burst of degitals valies assertion/attivitate burst. 53-Base 3.1 27 1090 Settimated availability; shouldn't this be "established availability for the forms of identity evidence to address storage of possible pile? 53-Base 3.1 28 1120 Salimpacted assumes the system user groups and 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 HALL 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"? 55-Base 3.1 28 1123 "directly impacted" impacted" impacted of such assumance that the claimant is the same individual in the same individual is definited. The subject of assurance that the claimant is the same individual is definited; "this the level of assurance that the claimant is the same individual is definited;" with "the level of assurance that the claimant is the same individual is definited;" with "the level of assurance that the claimant is the same individual is definited;" with "the level of assurance that the claimant is the same individual is definited;" with "the level of assurance that the claimant is the same individual is definited;" with "the level of assurance that the claimant is the same individual is definited;" with "the level of assurance that the claimant is the same individual is definited;" with "the level of assurance that the claimant is the same individual is definited;" with "the level of assurance that the claimant is the same individual is definited;" with "the level of assurance that the claimant is the same individual is definited; with the level of assurance that the claimant is the same individual is definited; with "the level of assurance that the claima				
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 PIP? 3.1 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 and interest and above impacted entities SPLL 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"? 3.1 28 1123 "directly impacted" or "indirectly impacted" or "indirectly impacted" or "indirectly impacted" and 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"? 3.2 36 63-Base 3.1 28 1123 "directly impacted" or "indirectly im				
address storage of possible PII? 63-Base 3.1 28 120 '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, 91 to enter of this, 91 to enter of this, 92 to enter of this, 92 to enter of this, 92 to enter of the size of the supplemental of the statement say "all identified impacted entities SHALL be fully documented. Is it the intent of this, 91 to enter of this, 92 to enter of the supplemental	55			
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 fish samagaster as tertiary and above impacted entities SHALL be fully documented. Is it the ment of this SP to enforce SCRM aspects in its impact assessments to an unknown degree? Or should this statement say "all identified impacted entities." 36 63-Base 3.1 28 1123 "directly impacted?" "indirectly impacted?" AAL is defined later in the document as "the level of assurance that the claimant is the same individual sidentifier." with "the level of assurance that the claimant is the same individual sidentifier." with "the level of assurance that the claimant is the same individual sidentifier." with "the level of assurance that the claimant is the same individual sidentifier." with "the level of assurance that the claimant is the same individual sidentifier." with "the level of assurance that the claimant is the same individual sidentifier." with "the level of assurance that the claimant is the same individual sidentifier." with "the level of assurance that the claimant is the same individual sidentifier." with "the level of assurance that the claimant is the same individual sidentifier." with "the level of assurance that the claimant is the same individual sidentifier." with "the level of assurance that the claimant is the same individual sidentifier." with "the level of assurance that the claimant is the same individual sidentifier." with "the level of assurance that the claimant is the same individual sidentifier." with "the level of assurance that the claimant is the same individual sidentifier." with "the level of assurance that the claimant is the same individual sidentifier." with "the level of assurance that the claimant is the same individual sidentifier." with "the level of assurance that the claimant is the same individual sidentifier." with "the level of assurance that the claimant is the same individual sidentifier." with "the level of assurance th		3.1 27 1090		established availability
assumes a bit of supply chain risk management as tertiary and above impacted entities PALL be fully documented. Is it the intent of this 5P oe enforce SCRM aspects in its impact assessments to an unknown degree? Or should this statement say "all identified impacted entities"? 36 63-Base 31 28 1123 "directly impacted? directly impacted? directly or indirectly impacted management as "the level of assurance that the claimant is the same individual sidentifier." with "the level of assurance that the claimant is the same individual says application of the specific process itself, and the bir specific individuals' identifier." with "the level of assurance that the claimant is the same individual says application of the company of the specific process itself, and the bir specific individuals' identifier." with "the level of assurance that the claimant is the same individual says application of the company of the authentication process itself, and the bir specific individuals' identifier." with "the level of assurance that the claimant is the same individual says application of the company of the same as a process in the same individual says application of the claimant is the same individual says application of the claimant is the same individual says application of the claimant is the same individual says application of the claimant is the same individual says application of the claimant is the same individual says application of the same as a says		2.1 29 1120		all identified impacted entities
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"? 36 G3-Base 3.1 28 1123 "directly impacted" or "indirectly impacted?" AAL is defined later in the document as "the level of assurance that the claimant is the same individual sidentifier." with "the level of assurance that the claimant is the same individual's identifier." with "the level of assurance that the claimant is the same individual's identifier." with "the level of assurance that the claimant is the same individual's identifier." with "the level of assurance that the claimant is the same individual's identifier." with "the level of assurance that the claimant is the same individual's identifier." with "the level of assurance that the claimant is the same individual's identifier." with "the level of assurance that the claimant is the same individual's identifier." with "the level of assurance that the claimant is the same individual's identifier." with "the level of assurance that the claimant is the same individual's identifier." with "the level of assurance that the claimant is the same individual's identifier." with "the level of assurance that the claimant is the same individual's identifier." with "the level of assurance that the claimant is the same individual's identifier." with "the level of assurance that the claimant is the same individual's identifier." with "the level of assurance that the claimant is the same individual." and the intervention of the specifier individual's identifier." with "the level of assurance that the claimant is the same individual." and the intervention of the specifier individual's identifier." with "the level of assurance that the claimant is the same individual." There should an authenticator was issued." 38 G3-Base 3.2.1 3.2 3 16 Table 2-AALI 3 "Providing" (the option of) phishing resistance in olive the same is an individual individual individual's identifier. With "the level of assuran	03-base	3.1		an identified impacted entitles
35 36 3-Base 3.1 28 1123 "directly impacted" or "indirectly impacted? AAL is defined later in the document as "the level of assurance that the claimant is the same individual specific individual's identifier," with "the level of assurance that the claimant is the same individual specific individual's identifier," with "the level of assurance that the claimant is the same individual specific individual's identifier," with "the level of assurance that the claimant is the same individual specific individual's identifier," with "the level of assurance that the claimant is the same individual specific individual's identifier," with "the level of assurance that the claimant is the same individual specific individual's identifier," with "the level of assurance that the claimant is the same individual specific individual's identifier," with "the level of assurance that the claimant is the same individual specific individual's identifier," with "the level of assurance that the claimant is the same individual specific individual's identifier," with "the level of assurance that the claimant is the same individual specific individual's identifier," with "the level of assurance that the claimant is the same individual specific individual's identifier," with "the level of assurance that the claimant is the same individual specific individual's identifier," with "the level of assurance that the claimant is the same individual specific individual's identifier," with "the level of assurance that the claimant is the same as an the specific individual's identifier," with "the level of assurance that the claimant is the same as an the specific individual's identifier," with "the level of assurance that the claimant is the same as an the specific individual's identifier," with "the level of assurance that the claimant is the same as an the same as an the specific individual's identifier, with "the level of assurance that the claimant is the same as an the specific individual's identifier." with "the level of assurance that the c				
36 63-Base 3.1 28 1123 "directly impacted? directly impacted Recommend replacing: "The robustness of the authentication process itself, and the bir specific individual's identifier," with "the level of assurance that the claimant is the same individual authenticator was issued." 37 63-Base 3.3.2.1 35 1358 be an IALO so it can be recorded properly when agencies do assessments vs. when they do not. 40 63-Base 3.2.2 36 Table 2:AAL "Support" for MFA is not the same as an MFA requirement. 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 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 process of the controls. Base of the RPs to provide address the supplemental process of the controls. This places a good bit of burden on the RPs seeking integration with the CSP. 40 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. 41 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. 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. 43 1648-1662 (Impact assessments for an evolving threat landscape. 44 1648-1662 (Impact assessments for an evolving threat landscape. 45 1648-1662 (Impact assessments for an evolving threat landscape. 46 1648-1662 (Impact assessments for an evolving threat landscape. 47 1648-1662 (Impact assessments for an evolving threat landscape. 48 1648-1662 (Impact assessments for an evolv			unknown degree? Or should this statement say "all identified impacted entities"?	
AAL is defined later in the document as "the level of assurance that the claimant is the same individual specific individual's identifier." with "the level of assurance that the claimant is the same individual specific individual's identifier." with "the level of assurance that the claimant is the same authenticator was issued." ABL is defined later in the document as "the level of assurance that the claimant is the same individual specific individual's identifier." with "the level of assurance that the claimant is the same authenticator was issued." Given the significance of the change, call out that no identity proofing is no longer IAL1. There should authenticator was issued." Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not need to change "Support multifactor authentication" to "Requires multifactor authentication" to "Requires multifactor authentication" to "Requires phishing resistance" to "Indicate alloring 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. 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. 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. 163-Base 3.4.4 44 1648-1662 [Impact assessments are almost and controls, bowever, in order to associate applicati		24 20 4422		d:at, :_ d:at, :-
AAL is defined later in the document as "the level of assurance that the claimant is the same individual"s identifier." with "the level of assurance that the claimant is the same authenticator was issued." AAL is defined later in the document as "the level of assurance that the claimant is the same authenticator was issued." ABL is defined later in the document as "the level of assurance that the claimant is the same authenticator was issued." ABL is defined later in the document as "the level of assurance that the claimant is the same authenticator was issued." ABL is defined later in the document as "the level of assurance that the claimant is the same authenticator was issued." ABL is defined later in the document as "the level of assurance that the claimant is the same authenticator was issued." ABL is defined later in the document as "the level of assurance that the claimant is the same authenticator was issued." ABL is defined later in the document as "the level of assurance that the claimant is the same authenticator was issued." ABL is defined later in the document as "the level of assurance that the claimant is the same authenticator was issued." ABL is defined later in the document as "the level of assurance that the claimant is the same authenticator was issued." ABL is defined later in the document as "the level of assurance that the claimant is the same authenticator was issued." ABL is defined later in the document as "the level of assurance that the claimant is the same authenticator. Was assurance that the claimant is the same authenticator. Was assurance that the claimant is the same authenticator. Was assurance that the claimant is the same authenticator. Was assurance that the claimant is the same authenticator. Was assurance that the claimant is the same authenticator. Was assurance that the claimant is the same authenticator. And a bullet: No identify is not need. Change "Support multifactor authenticator. Change "Support multifactor authentication." Is near	36 63-Base	3.1 28 1123	directly impacted or indirectly impacted?	Recommend replacing: "The robustness of the authentication process itself, and the binding between an authenticator and a
Given the significance of the change, call out that no identity proofing is no longer IAL1. There should 38 63-Base 3.2.2 36 Table 2:AAL2 "Support" for MFA is not the same as an MFA requirement. 40 63-Base 3.2.2 36 Table 2:AAL2 "Providing" (the option of) phishing resistance is not the same as a phishing resistance requirement. 63-Base 3.4 39 Tob Standard recommends (should) the tailoring process for the xALs, but then requires (shall) pieces of the tailoring based on their population of RPs is subject to the prescribed standard for the tailoring process of the 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. 63-Base 3.4.1 42 Tob 1581-1591 Consideration of "Rnown threats" based on current set of TTPs negates the opportunity for continued threat assessments or a eliventic and early integrated and early integrated and early integrated threat assessments are already done for application ATOs; however, in order to associate applications (RP) to a CSP, additional compensating to integrate with the CSP.			AAL is defined later in the document as "the level of assurance that the claimant is the same individual	specific individual's identifier." with "the level of assurance that the claimant is the same individual to whom the credential or
38 63-Base 3.2.1 35 1358 be an IALO so it can be recorded properly when agencies do assessments vs. when they do not. 39 63-Base 3.2.2 36 Table 2:AALZ "Support" for MFA is not the same as an MFA requirement. 40 63-Base 3.2.2 36 Table 2:AALZ "Providing" (the option of) phishing resistance is not the same as a phishing resistance requirement. 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 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 control set without any tailoring and leave it to the RPs seeking integration with the CSP. 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 or an evolving threat landscape. 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.	37 63-Base	34	1347 to whom the credential or authenticator was issued."	authenticator was issued."
38 63-Base 3.2.1 35 1358 be an IALO so it can be recorded properly when agencies do assessments vs. when they do not. 39 63-Base 3.2.2 36 Table 2:AALZ "Support" for MFA is not the same as an MFA requirement. 40 63-Base 3.2.2 36 Table 2:AALZ "Providing" (the option of) phishing resistance is not the same as a phishing resistance requirement. 40 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 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 control set without any tailoring and leave it to the RPs seeking integration with the CSP. 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 or an evolving threat landscape. 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.			City the similar of the short of the short of the side of the side of the side of the short of the short of the short of the side of the s	
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" to "Associate applications" to "Requires multifactor authentication" to "Requires phishing resistance requirement. Change "Provide phishing resistance" to "Requires phishing resistance requirement. Change "Provide phishing resistance" to "Requires phishing resistance requirement. Change "Provide phishing resistance" to "Requires phishing resistance replication in the place of the tailoring based on their poporation of the passed on their replace all "shall" statements in the 3.4 to "should" replace all "shall" statements in the 3.4 to "should" replace all "shall" statements in the 3.4 to "Requires phishing resistance" to "Requires phishing resistance replace all "shall"	38 63-Rasa	3 3 2 1 35		Add a hullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities ar
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. 63-Base 3.4 39 1505 Standard recommends (should) the tailoring process for the xALs, but then requires (shall) pieces of 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. 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. 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.	00 00 000			Change "Support multifactor authentication" to "Requires multifactor authentication" or "Enforces"
63-Base 3.4 39 1505 Standard recommends (should) the tailoring process for the xALs, but then requires (shall) pieces of the replace all "shall" statements in the 3.4 to "should" tailoring documentation. This assumes that the CSP committing to the tailoring based on their population of Fis 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. 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. 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.				
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. 63-Base 3.4.1 42 1581-1591 Consideration of "known threats" based on current set of TTPs negates the opportunity for continued threat seessments for an evolving threat landscape. 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.				
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. 63-Base 3.4.1 42 1581-1591 Consideration of "known threats" based on current set of TTPs negates the opportunity for continued threat sessements for an evolving threat landscape. 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.	63-Base	3.4 39 1505		replace all "shall" statements in the 3.4 to "should"
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. 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. 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.				
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. 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. 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.				
41 with the CSP. 63-Base 3.4.1 42 1581-1591 Consideration of "known threats" based on current set of TTPs negates the opportunity for continued threats specific, known, and potential threats threat assessments for an evolving threat landscape. 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.				
63-Base 3.4.1 42 1581-1591 Consideration of "known threats" based on current set of TTPs negates the opportunity for continued threat sessesments for an evolving threat landscape. 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.				
threat assessments for an evolving threat landscape. 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.	41 63 B	2.4.4		and the language and a should bloom to
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.		3.4.1 42 1581		specific, known, and potential threats
(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.	63-Base	3.4.4 44 1648		
			(RP) to a CSP, additional compensating controls need to be identified based on xALs for that RP. This is	
"initially assessed xALs" are required in a DIAS, which is required to be created by a CSP. This	43		an added burden to the RPs seeking to integrate with the CSP.	
initially assessed Anta- are required in a bind, which is required to be distated by a col. This			"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				
				Remove requirements for CSPs to create aDIAS; keep the requirement to aid RPs in creating their DIAS
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	63-Base	3.5 45 1686		snouia
organizations, especially those supported by II systems governed by HisMa 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.				
45	45		0 · 0 · · · · · · · · · · · · · · · · ·	

		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	
46	63-Base		3.1			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 IALO (no proofing), not IAL1.	Change IAL1 to IAL0
						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	
49	63C	3.1.2		11	688-689	for mDLs).	Remove either the presentation of an activation factor and/or of subscriber-controlled wallets in Section 3
						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"	
50	63C		3.4	17	896-897	requirements?	Remove or change to a SHOULD statement
						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	
51	. 63C		3.4	17			Suggest changing SHALL to SHOULD
	63C	3.5.2		22		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.	
52	1						
	63C	3.11.2		32	1408-1422	Should a digital-wallet, considered an IdP in some transactions, be held to the same requirements set	Include clarifying language in digital wallet section around the attribute bundles similar to these requirements when the
53						forth in 3.11.2 for derived attributes?	wallet is acting as the IdP to some degree.
						How would an RP know that the assertion has a "phishing resistant" authenticator when technology	
54	63C		3.14	37	1568-1569	vendors do not transmit that level of veracity on authentication assertions?	Create a new AAL - AALO, which would be for single factor authenticators; AAL1 would be for MFA phishable, AAL2 would be N
							2297 - Remove this item from the 'SHOULD' list and change to:
						It is critical that RPs and IdPs be informed when either suspects that an account has been	"The IdP SHALL send a signal or other notification regarding any subscriber account suspected of being compromised."
55	63C	-	4.8	62			2306 - "The RP SHALL send a signal or other notification regarding any subscriber account suspected of being compromised."
						There are instances in these guidelines where phishing resistant authenticators are required, yet they	
56	63C	-	4.9	64		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
						An activation factor should always be required before any operation that is using a wallet's signing keys	
57	63C		5.1	69	2507	is involved.	change SHOULD to SHALL