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

					Please submit responses to dig-comments@nist.gov by April 14, 2023	-
Organization:		1	IRS			_
Name of Subr	nitter/POC:	1	Varun Lal			_
Email Address	of Submitter/POC:		[REMOVED]			
Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	N/A	N/A	N/A	N/A	NIST should develop a shared responsibility model - responsibilities of CSP vs the agency RP	Create a shared responsibility model (CSP responsibilities vs. agency RP)
-	.,,	.,,	.,,	.,,	Agencies can benefit with guidance from NIST on standardized practices for multi-CSP environment (where an	erence a sinutea responsionally model (doi: responsionales visugency ta)
					agency is using multiple CSPs). How should compliance look? How should agencies handle users with multiple	Provide additional guidance on best practices for a multi-CSP environment. Details should include compliance and
2	N/A	N/A	N/A	N/A	credentials?	how to handle a user with multiple credentials.
3	Base	N/A	N/A	N/A	The identity technology market has not been able to keep up with the requirements in NIST 800-63-3.	NIST should consider the state of the market capabilities and design requirements around those abilities, at least at the lower assurance levels, rather than seek to drive the market to create compliant products.
4	Base	Note to Reviewers 5.1.3 Identify Potential	ii	149	The second to last word on line 149 "Identify" is misspelled.	Update 'identify' to 'identity'
5	Base	Impact Levels	28	1100	Impact Category label missing.	Missing "Loss of sensitive information"
		5.1.3 Identify Potential			The section "Damage to trust and reputation" has two sets of Low, Moderate, High examples, with the second set having reference to [FIPS199]. Was this a mistake in leaving this set in the base document? If not, why doesn't the	
6	Base	Impact Levels	28	1101 - 1109	other impact categories have examples with reference to [FIPS199]?	Clarify if lines 1101-1109 are a different section than lines 1093-1099.
					Why are the xAL diagrams removed from Rev. 4? NIST 800-63-3 has Figures 6-1 Selecting IAL; Figure 6-2 Selecting AAL; and Figure 6-3 Selecting FAL. In Rev. 3 base volume, there is guidance (via a diagram) on selecting xALs; this	
7	Base	N/A 5.2.2.1. Identity	N/A	N/A	is found in Section 6 - Selecting Assurance Levels (p.27, p.30, p.32). In Rev. 4, the diagrams are moved.	Include diagrams in NIST SP 800-63-4?
8	Base	Assurance Level	31	1198	IALO is not listed with its definition.	Add IALO and definition for quick access instead of only being referred to in 63A
9	_	5.2.2.2 Authentication			Line 1213 reads, Proof of possession and control of two different authentication factors. Why not just state MFA	
9	Base	Assurance Level	31	1213	instead of '2 different authenticators'.	Replace '2 different authenticators' with Multi-Factor Authentication (MFA)?
					Lack of understanding for this section, please clarify:	
					<ul> <li>Is this section supposed to tell agencies how to perform the initial impact assessments? There are no defined steps to perform the analysis of the Impact categories against the xALs and how to determine the level needed to</li> </ul>	
					avoid the risk of identity proofing, authentication, or federation.  Is the Initial Impact Assessment process designed to replace the Impact Category section that was in the Decision	
		5.1 Conduct Initial			Trees?  •Table 1 makes no sense on how you can use it to determine the levels (low, moderate, high) and there is no	Section 5.1 is lacking some guidance on how to perform the four steps listed. Can some guidance on how to
10	Base	Impact Assessment	24	965 - 1169	• Lable 1 makes no sense on now you can use it to determine the levels (low, moderate, nigh) and there is no explanation on if when combining the Impact Levels do you use High Water mark method?	Section 5.1 is facking some guidance on now to perform the four steps listed. Can some guidance on now to perform the analysis or defined processes be added?
11	Base	Note to Reviewers	ii	145	Public perception of biometric technology is causing heated debates. (Note: Similar language appears in all volumes.)	Suggest direct engagement with the controversy by including a description of biometrics, its use as a tool, and the importance of agency decisions in managing the risks (both technologically and reputationally) in using this tool.
12	Base	2.3.2 Privacy	8	542	The language states that the Privacy Act established a set of fair information practices. The recommendation is to update the statement to include the actual history of the Privacy Act.	Suggest correcting language to match the actual history of the act: The Privacy act was built on a set of fair information practices
13	Base	5.1.4 Impact Analysis	29	1158	The process of authenticating and passing the authentication attributes bears similar risk of over-collection of data to the identity proofing process.	Suggest including an analysis of the use of excessive information in Authentication, similar to the third bullet in Identity Proofing.
14	Base	5.2.1 Assurance Levels	31	1180	Organizations should consider all potential risks when determing assurance levels.	Suggest removing the exclusive "cybersecurity" from the sentence "based on cybersecurity risk and mission needs."
15	Base	5.2.3 Initial Assurance Level Selection	32	1238	The initial selection of assurance levels must consider all angles of risk.	Suggest removing the exclusive "cybersecurity" from the sentence "These initial selections are primarily based on cybersecurity risk, but will be tailored"
16	Base		N/A	N/A	Agencies can benefit if NIST can provide separate guidance on CSP strategy and additional information what CSPs could obtain for better fraud management.	Provide separate guidance on CSP strategy and additional information what CSPs could obtain for better fraud management.
10	Dase	N/A 5.5 Cyper, Fraud, and Identity Program	N/A	N/A	Both lines are written as SHOULD statements. The recommendation is to change both statements from SHOULD to	management
17	Base	Integrity	39	1493, 1497	SHALL.	Replace "SHOULD" with "SHALL"
		4.3.3 Authentication			Guidance is needed regarding allowing multiple subscriber accounts to the same authenticator (e.g., many	
18	Base	Process	19	N/A	subscriber accounts with the same SMS MFA).	N/A
					The Continuous Evaluation and Improve section contains two SHOULDs which seem insufficient given the number	
19	Base	5.4 Continuously Evaluate & Improve	39	1479 & 1481	and variety of threat actors and their continuously evolving capabilities. In order to ensure a robust risk management framework, consider changing the two SHOULDs to SHALLs.	Replace "SHOULD" with "SHALL"
19	DaSe	Lvaiuate & Improve	37	14/7 & 1401	management is astrework, consider trianging the two StiOULDS to StiALLS.	Provide more guidance around how to manage accounts across multiple CSPs. For instance, guidance on how to
20	63C	N/A	N/A	N/A	Agencies would benefit from more guidance around how to manage accounts across multiple CSPs.	implement a reciprocity schema or how to securely associate new credentials to an existing account that was proofed by another entity.
					The IdP and RP have agreed to participate in a federation transaction with each other for the purposes of logging	
21	63C	4 Federation Assurance Level (FAL)	6	439, 442	in the subscriber to the RP. This can be traced back to a static agreement between the parties or occur implicitly from the connection itself.	What information must the static agreement betwwen the IdP and RP have?
2.1	550	Level (PAL)	3	152, 112	There are multiple questions around Table 1, which references Dynamic and Static for Trusted Agreement &	must the state agreement occurrent the Ital and Italiane
					Registration  •What is the difference for the use of Static & Dynamic in the Trust Agreement versus the Registration?	
					<ul> <li>Under the Registration column of Table 1, is the use of Static or Dynamic related to Knowledge Based</li> </ul>	
					Authentication (KBA)?  If the use of Static or Dynamic for Registration are intended for KBA, why would Static be used on all three and	
					Dynamic used on FAL1 and 2 only when Dynamic is more stringent?  •Why isn't Enhanced Dynamic KBA considered?	
22	63C	4 Federation Assurance Level (FAL)	7	Table 1 - FALs	Should definitions for Static and Dynamic (as it relates to KBA) be included in Appendix A of NIST 800-63-4	Provide more clarity/context on this statement.
22	ośt	Levei (FAL)		rable 1 - FALS	[[ Dabe j :	priovide more darity/context on this statement.

				,		
23	60.0	Assurance Level 2		544.500	G C PRODUCE C LINE PRODUCE PRODUCE C	W. L
23	63C	(FAL2) 4.4. Requesting and	9	514, 539	Confirm correct FIPS 140 reference; should it be FIPS140 or FIPS140-3 Further explain "IdP may indicate no claim is made to IAL or AAL for given federation transaction." How would	Update reference to FIPS140-3 if needed Clairify what this paragraph means by IdP may indicate no claim is made to IAL or AAL for given federation
24	63C	Processing xALS	10	556-560	there be "no IAL?"	transaction.
		4.1. FAL1, 4.2. FAL2, 4.3.				
25	63C	FAL3, 4.4 Requestion and Processing xALs	711	463-587	Each section provides lengthy in depth detail about assertion requirements and recommendations for each of the FAL levels.	Create a process flow to visualize how scores are processed for better understanding if possible.
25	630	and Processing XALS	/11	403-387	FAL levels.	Add in the decision trees or additional guidance about how to select the correct FAL level under given
26	63C	N/A	N/A	N/A	There are no longer decision trees for FAL	circumstances
		,	,		· ·	
						Emphasize importance of data minimization, with language such as:
						The RP and IdP SHALL organize their data exchange agreements to ensure only they exchange only the minimum
					Data minimization is a key privacy consideration in this aspect of the relationship. There should be more emphasis	data necessary to achieve mission needs, maintain security and prevent fraud. These data elements SHALL be
27	63C	5.1 Trust Agreements	14	642	on the importance of data minimization.	reviewed periodically to avoid over-collection or unnecessary exchange of data.
					Commercial organizations have historically chosen to implement their consent basis in an "opt-out" model that	Add language to the paragraph such as:
		5.5 Privacy			defaults to users sharing data, whether they specifically choose to do so or not. A better privacy model is to	When building consent measures, the IdP SHOULD utilize an "opt-in" model that defaults users to a state where
28	63C	Requirements	30	1109-1111	implement an "opt-in" model, where user data is not used, unless specifically approved.	their data is not used for any other service unless they choose to allow it.
		4.1.2 Authenticator &				
		Verifier Requirements				
		5.1.1.2 Memorized Secret Verifiers				
		5.2.12 Connected				
		Authenticators				
		6.1 Authenticator			Is an adversary-in-the-middle (AitM) considered the same as a man-in-the-middle attack (MitM)? V4 removed any	
29	63B	Binding	N/A	N/A	reference to MitM and added AitM.	N/A
			.,,	.,		
		4. Authentication			Line 434 states, [FIPS140] requirements are satisfied by FIPS 140-3 or new versions. Is FIPS 140-3 or higher	
30	63B	Assurance Levels	6	434	revisions the minimum FIPS 140 that is to be implemented?	Update to FIPS140-3 if needed
31	63B	4.1.2 Authenticator and Verifier Requirements	7	469	Confirm correct FIPS 140 reference; should it be FIPS140 or FIPS140-3	Update to FIPS140-3 if needed
31	03.0	4.2.2 Authenticator and	/	407	Commin correct Firs 140 reference, should it be Firs140 of Firs140-3	opuate to FF5140-5 ii needed
32	63B	Verifier Requirements	9	524, 535	Confirm correct FIPS 140 reference; should it be FIPS140 or FIPS140-3	Update to FIPS140-3 if needed
		4.3.2 Authenticator and				
33	63B	Verifier Requirements	11	597, 599, 600	Confirm correct FIPS 140 reference; should it be FIPS140 or FIPS140-3	Update to FIPS140-3 if needed
		Table 1 AAL Summary of		,,		
34	63B	Requirements	13	Table 1, 2nd Row	Confirm correct FIPS 140 reference; should it be FIPS140 or FIPS140-3	Update to FIPS140-3 if needed
		5.1.7.1 Single-Factor		,		
		Cryptographic Device				
35	63B	Authenticators	28	1119	Confirm correct FIPS 140 reference; should it be FIPS140 or FIPS140-3	Update to FIPS140-3 if needed
		5.1.9.1 Multi-Factor Crypotographic Device				
36	63B	Authenticators	30	1206	Confirm correct FIPS 140 reference; should it be FIPS140 or FIPS140-3	Update to FIPS140-3 if needed
50	000	Tattientettors	50	1200		b punc to 11 of 10 of incented
					Table 1 AAL Summary of Requirements does not list Records Rention Policy or Privacy although required at all	
		4.5. Summary of		Table 1 - AAL Summary of	levels. Why was it removed from the table when it allows for easier understanding of AAL requirements at a	
37	63B	Requirements 4.4 Privacy	13	Requirements	glance? The e-Gov Act requires a privacy impact assessment on "informatin technology" that processes information in	Add Records Retention Policy and Policy back into AAL Summary of Requirements table  Suggest a change to the wording on the requirement for a PIA that more closely aligns to the e-Gov Act
38	63B	Requirements	12	653	identifiable form.	requirements.
		1				
					Privacy is important throughout the full lifecycle of the data, as mentioned in the current draft. Much of the requirements are covered in the 63 Base and 63A. With appreciation for the continued inclusion of privacy in 63B,	Update the sentence to read, "These controls cover notices, redress, role-based training, and other important
39	63B	9.2 Privacy Controls	59	2002	there are some other key privacy controls worth mentioning in this context.	considerations for successful and trustworthy deployments."
37	031	7.2 I Tivacy Controls	37	2002	there are some other key privacy condois worth mendoning in this context.	considerations for successful and didstworthy deployments.
					The use of biometrics is an especially sensitive topic. In order for individuals to properly consent to its use there	Include a requirement that the CSP SHALL provide clear notice concerning the collection, use, purpose and options
40	63B	5.2.3 Use of Biometrics	32	1255	must be clear notification of its collection, purpose, use and security.	when applying biometrics as an authentication factor.
					OMB M 10-22 includes requirements for notification of the use of cookies on a government website. Recommend	Include reference to OMB M-10-22, "Guidance for Online Use of Web Measurement and Customization
41	63B	7.1.1 Browser Cookies	49	1865	including OMB M-10-22 reference.	Technologies."
		arenes services				
		1				
		1			63A says in 5.1.8 #2: When collecting and comparing biometrics remotely, the CSP SHALL implement liveness	
					detection capabilities to confirm the genuine presence of a live human being and to mitigate spoofing and	
		1			impersonation attempts. However, 63B says in 5.2.3: The biometric system SHOULD implement presentation attack	
42	63B	5.2.3 Use of Biometrics	32	953 (63A) & 1283 (63B)	detection (PAD). These two sections appear to be inconsistent in approach. Shouldn't both be SHALL statements?	Replace "SHOULD" with "SHALL"
		N ELECTRICAL PROPERTY AND ADDRESS AND ADDR		, , , , , , , , , , , , , , , , , , , ,		
			****		Maybe more emphasis on identity governance? Things like account maintenance, ability to change permissions, etc.	W. C.
43	63A	N/A 4.3.4.1 Evidence	N/A	N/A	This could be more on the 53 side but could be handy in a zero trust approach.	N/A
44	63A	Validation	N/A	N/A	How would a CSP operator confirm evidence is not counterfeit and not tampered with?	N/A
				.,		,
	_	4.3.4.4 Validation			Can you provide examples of each of the source bullet points in this section? Who would be an original source of a	
45	63A	Sources 5.1.7 Requirements for	13	636-654	First Name/Last Name or Address?	Provide examples of each of the source bullet points.
		Notifications of Identity			Why is there from SHALL to SHOULD for sending notifications of proofing and enrollment codes to different	
46	63A	Proofing	22	895-897	validated addresses?	Provide more clarity/context on this statement.
		5.3.3 Evidence and Core			In remote identity proofing of IAL1, how would the CSP validate the genuineness of each piece of FAIR evidence by	,,
47	63A	Attributes Validation	a-		visual inspection by trained personnel in real life workflows? What if an MNO record or credit report accessed by a	W.G.
		Requirements 6.3 Subscriber Account	27	N/A	Phone Number/SSN is used?	N/A
4/	USA			1	I and the second se	
48			35	N/A	Is there any guidance for notification of Subscriber Account Termination by the CSPs?	N/A
	63A	Lifecycle	35	N/A	Is there any guidance for notification of Subscriber Account Termination by the CSPs?	N/A
			35	N/A	In the list of Evidence collection, to be more clear and to match Section 5.3.2.1, suggest adding ", or" after 1. One	N/A
		Lifecycle	35	N/A	In the list of Evidence collection, to be more clear and to match Section 5.3.2.1, suggest adding ", or" after 1. One piece of SUPERIOR EVIDENCE. The section would then read as	N/A
			35	N/A	In the list of Evidence collection, to be more clear and to match Section 5.3.2.1, suggest adding ", or" after 1. One	N/A Suggest adding ", or" after number 1

		2.2 Identity Assurance			Under Section 2.2 Lines 420 and 421 it states for IAL3 "via a supervised remote identity proofing session", however, in section 5.1.9.1 requirements for Trusted Referees on line 995 it only lists IALs 1 and 2. The	
		Levels			supervised remote identity proofing session statement for IAL3 would support the use of a Trusted Referee for	
		5.1.9.1 Requirements for	4 (Section 2.2)	420-421 (Section 2.2)	remote identity proofing for IALs 1, 2, and 3. A Direct to Virtual-in-Person (VIP) process with a Trusted Referee	
50	63A	Trusted Referees	24 (Section 5.1.9.1)	994-995 (Section 5.1.9.1)	should be able to support the ID Proofing process even at IAL3.	Recommend changing line 995 to "proofing at all IALs."
					Added new IALO level where there is no requirement to link the applicant to real life identity (neither validated or	
		2.2. Identity Assurance		408	verified). How does this impact existing applications at the different IAL levels? Does this mean the level is	
51	63A	Levels	4	408	downgraded by one (e.g., from IAL1 to IAL0) There are multiple questions regarding rather from IAL kequirements summary, liven that IAL1 and IAL2 are the	Clarify what this might mean for existing applications at IAL1 and IAL2.
					same,	
					•If IAL2 requires "stronger evidence and a more rigorous process," why is the evidence required the same for IAL1 and IAL2?	
		5.6. Summary of		Table 1 - IAL	•Why was the option of 2 pieces STRONG, or 1 STRONG plus 2 FAIR removed that were previously listed for IAL2	
52	63A	Requirements	33	Requirements Summary	in Rev 3?	Explain reasoning
					Identity proofing may be required for a variety of interactions with individuals. This document currently only	
					specifically identifies online and telephone interactions. Recommendation is to include language that 800-63 series	Suggest adding that the 800-63 series does not include ID-proofing requirements for written or faxed
53	63A	1 Purpose	2	361	does not include ID-proofing requirements for written or faxed correspondence.	correspondence.
54	63A	2 Introduction	3	390	Privacy controls are not optional. They should be noted as "Normative."	Update privacy to "Normative"
		Validation, and				
55	63A	Verification	6	427	Editorial. The current revision says "This section provides and overview"	Correct spelling, the statement should read: "This section provides an overview"
56	63A	4.1 Identity Proofing and Enrollment	7	463	This section outlines expectations for collecting information from applicants, including describing what information must be presented.	Provide guidance to RPs to notify applicants of available choices concerning CSPs, identity document requirements, and related privacy notices.
56	63A	and Enrollment	/	463	must be presented.	and related privacy notices.  Move the example to a point in the document after the definitions immediately below it, so that the example can
57	63A	4.1.1 Process Flow	8	467	This is a good example of the process, but comes before the context being analyzed.	include an analysis of how well it meets those definitions.
						Add context as to why that matters. Include an explanation that, by collecting only the minimum amount of data,
						there is less risk to the applicant and less overhead for the CSP/RP related to storing and protecting unnecessary
58	63A	4.2 Identity Resolution	9	491	The statement sets the expectation to use the smallest set of attributes possible.	information. There may be other worthwhile reasons to notate.
		4.3.1 Characteristics of Acceptable Physical			An informed applicant can help streamline the process and minimize burden for all and contributes to better	Suggest adding a "should" statement for CSPs to describe what is being collected, why, and how to meet the
59	63A	Evidence	9	516	overall privacy protections.	expected evidence requirements, in an order to support a well-informed applicant.
60	63A	4.3.4.4 Validation Sources	14	653	It's important that vendors, contractors and sub-contractors protect data to acceptable standards and that individuals are informed regarding who has access to their information.	Suggest adding guidance that CSPs/RPs "shall" ensure data protections, including all applicable security and privacy controls, are met by any vendor or their tertiary service providers.
00	UJA	5.1.1 Identity Service	11	033	individuals are informed regarding wito has access to their information.	privacy controls, are mee by any venuos of their tertainy service providers.
		Documentation and			The e-Gov Act requires government agencies to publish privacy impact assessments, with limited exceptions. CSPs	
61	63A	Records	16	720	should be expected to support the government PIA, if not contribute directly to it.	Suggest adding guidance about CSP support for PIAs, possibly as a best practice.
		5.1.1.1 Ceasing			Businesses often cease to exist for a variety of reasons. A common reason is being bought out and rolled into	Suggest adding clarity that the "Ceasing Operations" includes any and all cessations, transfers, reorganizations,
62	63A	Operations	17	725	another company.	recharacterizations or other changes to business organization or ownership.
		5.1.1.2 Fraud Mitigation				Suggest adding guidance that CSPS should notify individuals about the use of their information, including fraud mitigation measures. This does not mean exposing specific tactics to the public, but the simple awareness that
63	63A	Measures	17	739	An important element of privacy risk mitigation is notifying individuals about how their information is used.	information they provide may be used to prevent fraud.
		5.1.2.2 Additional				
		Privacy Protective Measures	18 (Section 5.1.2.2)	773 (Section 5.1.2.2)		Suggest adding guidance that CSPs "shall" provide privacy training to employees, contractors, sub-contractors, in conjunction with requirements by the RP. The training "shall" apply to any member of the company or a tertiary
64	63A	5.5.8 Requirements for	32 (Section 5.1.2.2)	1225 (Section 5.1.2.2)	Privacy and security role-based training is critical for an effective workforce.	service provider who has access to any sensitive information in the conveyance of the contract.
		5.1.5 Additional	()	(00000000000000000000000000000000000000	,	, , , , , , , , , , , , , , , , , , , ,
		Requirements for			The e-Gov Act requires a privacy impact assessment on "informatin technology" that processes information in	Suggest a change to the wording on the requirement for a PIA that more closely aligns to the e-Gov Act
65	63A	Federal Agencies	20	842	identifiable form.	requirements.
						Recommend further explination, such as CSPs shall ensure that privacy and security training for employees,
		5.1.9.2 Requirements for			Applicant referees are entitled to the same privacy and security protections as the individuals they are assisting in	especially Trusted Referees, includes an understanding of the need to protect information about the Applicant
66	63A	Applicant References	25	1009	meeting identity proofing requirements.	References as securely as information about the applicant.
		5.3.3 Evidence and Core				
		Attributes Validation				This is another section that should include additional clarification and emphasis on the requirement to ensure
67	63A	Requirements	27	1076	Data must be protected throughout its lifecycle, including when being processed by a vendor.	privacy and security protections in sub-contractor or tertiary service provider systems.
		5.5.3.2 Core Attribute				This is another section that should include additional devisionation and amphasis on the
68	63A	Validation Requirements	30	1182	Data must be protected throughout its lifecycle, including when being processed by a vendor.	This is another section that should include additional clarification and emphasis on the requirement to ensure privacy and security protections in sub-contractor or tertiary service provider systems.
30	-241	7.1 Threat Mitigation	-0	Table 3	, and	y processor and a second processor and a second
69	63A	Strategies	38		Social engineering has become a prevalent attack technique.	Suggest additional detail on how to identify and prevent social engineering attacks.
		6.3 Subscriber Account			Agencies can hanofit if NICT can provide additional detail-/-tf	Provide additional details (stansfrom quests on substitute and the second secon
70	63A	6.3 Subscriber Account Lifecycle	35	N/A	Agencies can benefit if NIST can provide additional details/stepsframework on subsriber account life cycle management - standardized across all CSPs.	Provide additional details/stepsframework on subsriber account life cycle management - standardized across all CSPs.
				.,,,,	9	
		6.3 Subscriber Account			Can OMB/DHS/GSA establish standard framework for CSPs (like a framework) for digital identity and thus be the	Fetablish standard framework for CSDs (like a framework) for digital identity and thus he the continue - which for
71	63A	6.3 Subscriber Account Lifecycle	35	N/A	certifying entity for CSPs? Agencies can benefit from Federal standaridzed requirements (framework) for CSPs.	Establish standard framework for CSPs (like a framework) for digital identity and thus be the certifying entity for CSPs? Agencies can benefit from Federal standaridzed requirements (framework) for CSPs.
	****				, o , o , o , o , o , o , o , o , o , o	0
					Providing Trusted Referees (Sec. 5.1.9.1) explains the CSP shall train its trusted referee to make risk-based	
72	63A	5.1.9.1 Requirements for Trusted Referees	24	993	decisions based on the specific applicant circumstances". Agencies may benefit if NIST can provide specific guidance and details on criteria and what entails "risk-based decision".	The recommendation is to provide specific guidance and details on criteria and what entails "risk-based decsion".
12	OJA	11 usteu Referees	24	393	Burdance and details on Criteria and What entails Tisk-based decsion .	The recommendation is to provide specific guidance and details on criteria and what entails risk-based decsion".
					Based on the below statement, agencies will benefit if NIST/NARA establish strict guidelines/mandates for record	
		6.3.2 Subscriber Account			retention and disposal requirements. "The CSP SHALL delete any personal or sensitive information from the subscriber	
73	63A	Termination	35	1292	account records following account termination in accordance with the record retention and disposal requirements."	Establish strict guidelines/mandates for record retention and disposal requirements.

Base	.3.3 Authentication Proces	19	801	There are unintended consequences from the implementation of facial recognition technology including privacy invasion, public trust, fraud, and use of an emerging technology. A safer less intrusive biometric would be retinal scan which is genetically unique to every individual and equally effective. User cases should demonstrate effective application of specific, measurable, actionable objectives to ensure the benefits outweigh the risk.	Delay use facial recognition until sufficient evidence suggest the option will prove useful. Consider alternatives such as fingerprint and retinal scan first.
63A	N/A	N/A	N/A	Provide a "Track changes" redline document of NIST changes so the whole document does not need review.	Provide a "Track changes" redline document of NIST changes so the whole document does not need review.
63A	4.3.4.4 Validation Sources	13	629-631	Based on the statement below, does this mean that documents visually inspected by a trusted referee would not be required to be authenticated with the authoritative source? Core attributes that are contained on identity evidence that has been validated according to Sec. 4.3.4.1 can be considered validated, in which case no further validation is required.	Provide more clarity/context on this statement.
63A	5.1.1.2 Fraud Mitigation Measures	17	733-736	Consider making the below statement a SHALL statement. The CSP SHOULD obtain additional confidence in identity proofing using fraud mitigation measures (e.g., examining the device characteristics of the applicant, evaluating behavioral characteristics, and checking vital statistic repositories such as the Death Master File ([DMF]).	Update SHOULD to SHALL statement
634	5.1.6 Requirements for	21	N/A	What is the reasoning in allowing an enrollment code to be used to verify identity but not authentication? Line 887 states "5. The enrollment code SHALL NOT be used as an authentication factor." Yet in section 5.3.4 Identity Verification Requirements, the CSP SHALL verify the binding of the applicant to the claimed identity by one of the Following:  Line 1.086 ctars "2" Nerficiation of the applicant's nature of a valid appointment code Sec. 5.16".	Provide more clarity/context on this statement.
0571	Diff officer codes	21	.,,,,	**	1 Totale more clarity/context on this statement.
	5.3.5 Notification of			completion of identity proofing at IAL1, the CSP SHOULD send a notification of proofing to a validated address for	
63A	Proofing Requirement	27	1088-1089	the applicant, as specified in Sec. 5.1.7	Provide more clarity/context on this statement.
63A	6.2 Subscriber Account Access	35	1266-1271	Based on the following statement, is the AAL2 or AAL3 applicable for account access for IAL1 proofed accounts? In order to meet the requirement that accounts containing PII be protected by multi-factor authentication (MFA), the CSP SHALL provide a way for subscribers to access the information in their subscriber account through AAL2 or AAL3 authentication processes using authenticators registered to the subscriber account. The CSP SHALL product the capability for subscribers to change or update the personal information contained in their subscriber account.	Provide more clarity/context on this statement.
63A	5.1.9 Trusted Referees & Applicant Referees	24	977-992	Multiple questions for Section 5.1.9  *Could the concept of an "applicant reference", while increasing accessibility and equity, also potentially increase a fraud vector? (i.e., one fraudster successfully ID proofs himself, and then helps another fraudster "ID proof", for example, as the new "Mrs. HighProfilePerson").  *What strength level is the vouching of an applicant reference considered?  *What potential liability would an applicant reference have if someone they vouched for commits fraud?  *Should CSFs be required to let Relying Parties know that a user was 10 proofed with the aid of an applicant reference (as RPs form trusted partnerships with CSPs, not with an applicant reference)?	Provide more clarity/context on this statement.
	5.3.4 Identity			What is the difference in the first Identity Verification Requirement for IAL1 (Section 5.3.4) and IAL2 (Section	
624	Verification	27	1001	5.4.4)? Additionally, the verification option for Section 5.3.4 is not listed in Table 1 under Verification for IAL1. They	Add clarity on the difference between Section 5.3.4 and Section 5.4.4. If they're meant to be the same, please write them the same.
	4.3.2 Characteristics of Acceptable Digital			Lines 540-541 reads, "If applicable, the presented digital evience can be verified through authentication at an AAL or FAL commensurate with the assessed IAL." Does this mean that if the application assesses at an IALI/AALZ/FALZ that the digital evidence should be verified using the higher level digital evidence for AAL and/or	
63A	Evidence	10	540 - 541	PAL/	Provide more clarity/context on this statement.
63A	N/A	N/A	N/A	Is there a process where IdP's can leverage validation/verification of users registration against other IdP's?	Setting up the ability for an IdP to coordinate with other IdP's to validate/verify a user when registering as a part of the registration process. For example, if John Doe has registered with ID.me and has been validated/verified at IALZ/AALZ/FALZ, and the user is now registering with Login.gov, Login.gov can through a back channel connection with ID.me to save time and validate/verify an individual that has already been vetted and speed up the process, and potentially reduce the potential for fraud. This cross check process can helpful if not already in place.
				person & remote. Should this say "visual comparison" instead, for darity, since the operator won't be physically comparing anything? (the great Wikipedia says "A visual comparison is to compare two or more things by eye.",	Update references of 'physical comparison' to 'visual comparison'. This would provide more clarity as the operator
63A	N/A	N/A	N/A	characteristics of bullets, using tools, in crime labs)	won't be physically comparing anything.
	5.1.1 Identity Service Documentation &				
63A	Records	17	723	There is an extra ; and at the end of the statement	Remove ; and
63A	Assessment	18	771	The word dilligence is spelled incorrectly	The correct spelling is diligence
63B	Verifiers	26	1050	The word authentictor is spelled incorrectly	The correct spelling is authenticator
	5.1.8.1. Multi-Factor				
63B	Authenticators	29	1157	The word requirementss is spelled incorrectly	The correct spelling is requirements
Base	5.5. Cyber, Fraud, and Identity Program Integrity	39	1493-1495	The following statement reads, "Organizations SHOULD establish consistent mechanisms for the exchange of information between critical security and fraud stakeholders". The recommendation is to update this statement from SHOULD to SHALL.	Update SHOULD to SHALL statement
	63A	63A	63A	63A	Sources 19 881  Sources 19 881

		5.5. Cyber, Fraud, and			The following statement reads, "Where supporting service providers, such as CSPs, are external, this may be	
91	Rase	Identity Program Integrity	39	1496-1497	complicated, but SHOULD be considered in contractual and legal mechanisms". The recommendation is to update this statement from SHOULD to SHALL.	Update SHOULD to SHALL statement
91	base	integrity	39	1490-1497	tins statement from Strould to Strald.	The following language is suggested if a 'Data Management' section is added:  Maintaining account creation data, account management records and user end point data in a retrievable and analyzable format is critical to fraud detection and analytics. This data will also be critical to legal process.
		2.3 Enterprise Risk				To facilitate fraud analytics by end user client and legal process by law enforcement authorities, the CSP should be prepared and able to provide unmodified data records for the above-mentioned data types, if requested. This includes a standard data formatting, a data retention policy, ability to securely transfer data and all requisite policies and procedures to maintain these capabilities.
92	Base	Management Requirements and Considerations	6	489	Similar to the 'Security' sub-section under Section 2.3.1, there should be a 'Data Management' sub-section under Section 2.3, to address data management guidelines, and availability requirements.	To facilitate this capability, the CSP must establish and maintain a secure data repository that meets all relevant security standards but maintains the data in an unmodified format upon decryption and is accessible to both the CSP and authorized partners and parties.
93	Base	5.5 Cyber, Fraud, and Identity Program Integrity	39	1484	There should be a section on 'Data Capture Requirements', which should include a baseline (unexhaustive) list of data fields needed for fraud detection and monitoring that the CSPs should capture for internal and/or client fraud detection and response.	Refer to general comments document provided by CFAM.
					Security should also include fraud considerations, particularly fraud analytics for detection, root cause analysis to identify successful threat vectors and remediation strategies and implementation procedures.	
94	Base	5.5 Cyber, Fraud, and Identity Program Integrity	39	1484	Fraud poses as high of a threat to sensitive application processes and data as traditional cyber security threats such as hacking. Through identity theft, social engineering, phishing and other strategies, criminals can pose as one or many identities. These identity owner's personal data, benefits and financial resources are put at grave risk when this happens, as well as the organizations processes and assets.	The recommendation is to provide additional information on the threat posed by insufficient identity protection to emphasize importance of fraud detection and monitoring.
95	Base	5.5 Cyber, Fraud, and Identity Program Integrity	39	1484	Add a requirement for the development of a comprehensive overall fraud detection posture, to be shared with CSP partners.	The CSP should maintain a comprehensive fraud analytics, detection, and response posture. This posture shall include indicator development and monitoring, data analytics-based threat hunting, dedicated fraud analyte personnel and technical access and capability to identify the root cause of successful fraudulent exploitation of the CSP Identity validation process. This posture shall be applied to all log types of record documented in section 2.3.1. Refer to general comments document provided by CFAM.
75	base	5.5 Cyber, Fraud, and	37	1404	partiers.	neter to general comments document provided by Crisis.
96	Base	Identity Program Integrity	39	1484	Level of rigor applied to fraud detection and analytics is tied to the sensitivity of the data delivered by the applications protected. This results in higher IAL processes being the target of the most rigorous detection posture.	Fraud detection posture needs to be tied to the sensitivity of the data delivered by the applications protected.
97	Base	5.5 Cyber, Fraud, and Identity Program Integrity	39	1484	Request the addition of language regarding threat intelligence sharing for fraud detection, and the development of major fraud remediation playbooks. This will allow for CSP partners to quickly respond to new TTPs and rapid implement remediation strategies.	Include language such as: The CSP must inform RPs of accounts detected to be fraudulent. The CSP must maintain secure pathways and procedures to exchange two-way threat intelligence and investigation findings with all clients.
98	Base	5.5 Cyber, Fraud, and Identity Program Integrity	39	1484	CSP must maintain a mechanism for end users to report potential fraudulent activity or account takeover. This mechanism should also allow for the account to be disabled to prevent further harm to the user. Information on this self reported fraudulent activity should be passed along with the account information in order to allow for partners to conduct their own fraud investigation and remediation.	Include language such as: The CSP must maintain a self-reporting mechanism for CSP clients (end users) who believe they have been a victim of fraud along with a function for users to be disabled at both the account, and identity level. Record of these communication and actions shall be documented and shared within account management data.
99	Base	5.5 Cyber, Fraud, and Identity Program Integrity	39	1484	Customer notification is a critical aspect of identity protection; without notification of potential account changes, a customer is particularly vulnerable to account takeovers by bad actors.	Include language such as: The CSP shall maintain a posture of notifying the account owner upon all account management and update actions (e.g. 2FA method update, password reset, account suspension, email update, etc.). The CSP shall inform the identity of the existence of multiple accounts upon login to the CSP.
100	Base	5.5 Cyber, Fraud, and Identity Program Integrity	39	1484	Define Fraud analytics, Root Cause Analysis, & Fraud Activity Remediation within section 5.5. This will provide a common understanding of these activities.	The following definitions are recommended:  Fraud Analytics — Analytics applied to proofing, application, and web transaction data augmented with identity data sources to identify suspicious behavior patterns indicative of fraud activity. Critical data includes but is not limited to, source device and network information, user entered unique values, data validation response codes and internal and taxpayer driven account suspension information.  Root Cause Analysis – Review of identified fraud behaviors in the context of existing identity validation strategy to identify exploitation vectors used by fraudulent actors to gain unauthorized access to accounts and data other than their own.  Fraud Activity Remediation – The modification of Identity Validation process to eliminate a weakness that is being exploited by criminals to gain fraudulent access to accounts or data that are not their own.
		4.2 Enrollment and	37		Currently language on subscriber accounts reads "_subscriber account to uniquely identify each subscriber". The language needs additional clarity requiring that an identity be bound to a single active account. Allowing for an identity to have multiple accounts provides threat actors the ability to potentially proof and create a duplicate	Include language such as: The CSP then establishes a subscriber account to uniquely identify each subscriber and record any authenticators registered (bound) to that subscriber account. An individual identity may only have only
101	Base	Identity Proofing	14	706	account, allowing for actions to be taken without the subscribers knowledge or consent.  The resolution section does not explicitly state the phone number is a required attribute. Later in the verification	one active subscriber account.
400	cn.	444.7	8	450	section (row 483) it's required. The way it's worded in the resolution section, a phone number appears to be optional.	
102	63A 63A	4.1.1 Process Flow 4.1.1 Process Flow	8	470 483	Line 483 references the validated phone number but does not state the phone number should be validated against the identity.	Update the text to explicitly state the phone number is a required attribute.
103	63A	4.1.1 Process Flow	8	483	against the identity.  Should include language to mention that the goal is to confirm that the person proofing is the owner of the lidentity.	Update the text to explicitly state the phone number referenced is validated against the identity.  Include text that explicitly states the goal is to confirm the person proofing is the owner of the identity.
104	0JA		Ü	7/0	identity. Line 590 states, "contains at least one reference number that uniquely identifies and resolves to the person to whom it relates." This is not a strong enough evidence unless the reference number on the document is checked	
105	63A	4.3.3.3 Superior Evidence Requirements	12	590	against an authoritative source.	The true identity should match this identity in an accepted system of record. Gathering data and checking the data gathered must correlate for true identity proofing.
106	63A	5.1.1.2 Fraud Mitigation Measures	17	732	This section only addresses fraud mitigation during the initial proofing and is not relevant to the mitigation of new or emerging threats.	Add fraud detection/mitigation process post account creation based on patterns and connections.
107	63A	5.1.2.1 Privacy Risk Assessment	18	771	Risk assessment measures do not preclude the ability to protect systems and processes from fraudulent activity.	Add language to protect systems and processes from fraudulent activity.
10/	UJA	ASSESSMENT	10	//1	I	rand language to protect systems and protesses from fraudulent activity.

112 6.54 Procedure 29 1996 administrated processors of parameters of the SPECIAL Control OF	From Services 1						T	
Procycles of the control of the cont	Proportions 1			540041155			TO THE STATE OF TH	
Security Content of the process of the content of the process of the content of the process of	Service of the company of the compan							
10 63. S. Happermanenter Company 2 65 M2 season of finding through the set of the CPT and selected home of growth of the CPT and selected home of growth of the CPT and selected home of the C	Section   Company   Comp						use to make authorization decisions." Authorized processing reasons should include detection and mitigation of	
Section of Gloridon (Control Control C	Section of Control o	108	63A	5.1.7 Requirements for	18	773-775	fraud activity.	Add language to include fraud in authorized processing of PII.
111 CAS 17.1 Separation of 17.1	Proceedings			Notifications of Identity				
110 640 Transaction formers 27 97 97 97 98 per desired for special of profession special formers and a final analysis of the company of the c	10 6A Use of Remarkers 11 10 6A Transmitted freedom (1) 10 1 10 1 10 1 10 1 10 1 10 1 10 1	109	63A	Proofing 5.1.8 Requirements for	22	895	IAL2 account notifications should be sent by the CSP to validated home of record address or phone.  Suggest the language here be further refined to ensure the highest data matches both the applicant and the	Incorporate notification language for IAL2.
111 OAA Travelle findered 15 1000 representation of a found desirate pressor with standard religious to the presentation of a found desirate pressor with standard religious to the presentation of a found desirate pressor with standard religious to the presentation of a found desirate pressor with standard religious to the presentation of a found desirate pressor with standard religious to the presentation of a found desirate pressor with standard religious to the presentation of a found desirate pressor with standard presentation of a found desirate prese	11	110	63A	Use of Biometrics	23	952	true identity owner.	Add additional clarity.
12 6.3. A financial state.  13 4 Procession.  13 4 Procession.  13 4 Procession.  14 5 Procession.  15 5 Procession.  16 6 A Procession.  17 5 Procession.  18 6 A Procession.  19 7 Procession.  19 7 Procession.  19 7 Procession.  10 8 A Procession.  10 10 A Procession.  10 10 A Procession.  10 10 A Procession.  10 10 A Procession.  10 A Procession.  10 A Procession.  10 A Procession.  11 A Collection and Data.  11 A Collec	177 0.06 N. H. Amende Anni 20 190 Support season to adult anything the season distance in process on the later improvement of the comment of the season of th	111	63A		25	1002		Add proofing step requirement for trusted referee.
112 6.3.4 Powerton  113 6.5.4 Establishment for the control states of the control	112 GAA Provision 30 1996 estimated at the procession.  113 ASA Structure 4 1997 1997 1997 1997 1997 1997 1997 19							· · · ·
111 6AA Springs 29 1122 Interfere sublished by subtractive sourced of the SUPERIOR criterion and the SUPERIOR criterion and the Superior and t	113 0.34 Proceeding 124 125 Interesting 125 15 Journal of the Company of Table 1 - U. 125 15 Journal of the Company of Table 1 - U. 125 15 Journal of the Company of Table 1 - U. 125 15 Journal of the Company of Table 1 - U. 125 15 Journal of Territorium 126 15 Journal of Territorium 127 0.34 Company of Territorium 127 0.34 Company of Territorium 128 15 Journal of Territorium 129 15 Journal of Territorium 120 15 Journal of	112	63A		28	1096		
111 6AA Springs 29 1122 Interfere sublished by subtractive sourced of the SUPERIOR criterion and the SUPERIOR criterion and the Superior and t	113 0.34 Proceeding 124 125 Interesting 125 15 Journal of the Company of Table 1 - U. 125 15 Journal of the Company of Table 1 - U. 125 15 Journal of the Company of Table 1 - U. 125 15 Journal of the Company of Table 1 - U. 125 15 Journal of Territorium 126 15 Journal of Territorium 127 0.34 Company of Territorium 127 0.34 Company of Territorium 128 15 Journal of Territorium 129 15 Journal of Territorium 120 15 Journal of			E 4 4 1 Romoto Identity			Decommend this he CUREDIOD avidence only (accuming the shange is made that this sating requires unique	
164 O.A. Prevention 29 1148 Suggest the same additions and updates made to M.J. To curried over consistently throughout the document of the propose of prefet that prevention and publishes or prevention of the propose of prefet that prevention and publishes or prevention and publishes	131 OAA Procession 27 Table 1 Magnetic made to ML, To carried our constroating throughout the document.  132 Suggest conducted sharper to Telefonce and Yaddeding of SPTESON 1770AC/FAM.  133 LOGISCON and that 1 Telefonce and Yaddeding facility from the property of Endocation of SPTESON 1770AC/FAM.  134 LOGISCON and that 1 St. Collection and the second street of the property of Endocation of SPTESON 1770AC/FAM.  135 LOGISCON and that 1 St. Collection and the second street of the property of Endocation of SPTESON 1770AC/FAM.  136 LOGISCON and that 1 St. Collection and the second street of the property of Endocation of SPTESON 1770AC/FAM.  137 LOGISCON and that 1 St. Collection and the second street of SPTESON 1770AC/FAM.  138 LOGISCON and that 1 St. Collection and the SPTESON 1770AC/FAM.  139 LOGISCON and that 1 St. Collection and the SPTESON 1770AC/FAM.  140 LOGISCON and that 1 St. Collection and the SPTESON 1770AC/FAM.  141 LOGISCON and that 1 St. Collection and the SPTESON 1770AC/FAM.  142 LOGISCON and that 1 St. Collection and the SPTESON 1770AC/FAM.  143 LOGISCON and that 1 St. Collection and the SPTESON 1770AC/FAM.  144 LOGISCON and that 1 St. Collection and the SPTESON 1770AC/FAM.  145 LOGISCON and that 1 St. Collection and the SPTESON 1770AC/FAM.  145 LOGISCON and that 1 St. Collection and the SPTESON 1770AC/FAM.  145 LOGISCON and that 1 St. Collection and the SPTESON 1770AC/FAM.  145 LOGISCON and the SPTESON 1770AC/FAM.  145 LOGISCON and the SPTESON 1770AC/FAM.  145 LOGISCON and the SPTESON 1770AC/FAM.  146 LOGISCON and the SPTESON 1770AC/FAM.  147 LOGISCON 1770AC/FAM.  147 LOGISCON 1770AC/FAM.  148 LOGISCON and the SPTESON 1770AC/FAM.  149 LOGISCON 1770AC/FAM.  140 LOGISCON 1770AC/FAM.  140 LOGISCON 1770AC/FAM.  140 LOGISCON 1770AC/FAM.  140 LOGISCON 1770AC/FAM.  141 LOGISCON 1770AC/FAM.  141 LOGISCON 1770AC/FAM.  141 LOGISCON 1770AC/FAM.  141 LOGISCON 1770AC/FAM.  142 LOGISCON 1770AC/FAM.  143 LOGISCON 1770AC/FAM.  144 LOGISCON 1770AC/FAM.  144 LOGISCON 1770AC/FAM.  145 LOGISCON 1770AC/FAM.  145 LOGISCO	113	63A		29	1132		Recommend this be SUPERIOR evidence only.
15 SA Superments 16 SA Superments 17 Superments 18 Superments 19 Superments 18 Superme	Total Column   Tota	114	624		20	1140	Suggest the same additions and undates made to IAL 2 he sawied great consistently throughout the desument	Suggest the same additions and undates made to IAL 2 he sawied area sensistantly throughout the degree of
15 GA SUCCESSA Superments 33 Requirements Summy Sugget consistent changes to Dictions and Value of SUCCESSA SUPERIOR ASSTONAÇIARS  15 Colorism and Ratus  16 Colorism and Ratus  18 Colorism and Ratus  19 CASA SUCCESSA SUPERIOR SU	15 CAA STREAM SQUARE AND SQUARE CONTINUES AND SQUAR	114	UJA		29		Suggest the same auditions and updates made to IAL 2 be carried over consistently un oughout the document.	Suggest the same additions and updates made to IAL 2 be carried over consistency diroughout the document.
156   63.A   Termination   157   Revenience adding clause for the user to report an unanabarised account.   158	15 (2.5 Section of Day 15 (Section of Day 15 (Secti	115	63A		33		Suggest consistent changes to Evidence and Validation of SUPERIOR vs STRONG/FAIR	Suggest consistent changes to Evidence and Validation of SUPERIOR vs STRONG/FAIR.
117 634 Minimization 40 1346 Final detection should be conducted only for the purpose of facilitating further account validations processes and final facilities and final facilities and detection and the second of the second o	177 63A Minimistation 40 1146 Proceedings of the purpose of feelinging further account validation processes and for the purpose of feelinging further account validation processes and feelings of the purpose of			6.3.2 Subscriber Account				
117 OSA Minimization 40 1346 fraid defection and pure eventous activative.  118 OSA STATES (Control and PLAS)  119 OSA Minimization 40 1348 Suggest addings clarifying language minimization of PTI to address transis.  119 OSA STATES (Control and PLAS)  120 OSA STATES (Control and PLAS)  121 OSA Minimization 40 1348 Suggest addings clarifying language minimization of PTI to address transis.  120 OSA STATES (Control and PLAS)  121 OSA Minimization 40 142 OSA Mi	117 OSA Melamination 40 136 frau detection and prevention approaches activities.  118 OSA BLOOM Melamination 40 1346 Suggest adding depriving language on minimistation of PIU and approach transport from the Melamination 40 1346 Suggest and institution of PIU and approach transport from the Melamination 40 1346 Suggest and institution of PIU and approach transport from the Melamination 40 1346 Suggest and institution of PIU and approach transport from the Melamination 40 1346 Suggest and institution of PIU and approach transport from the Melamination 40 1346 Suggest and institution of PIU and approach transport from the Melamination 40 1346 Suggest and institution of PIU and approach transport from the Melamination 40 1346 Suggest and institution of PIU and approach transport from the Melamination 40 1346 Suggest and institution of PIU and approach transport from the Melamination 40 1346 Suggest and institution of PIU and approach transport from the Melamination of PIU and approach transport	116	03A		35	1280		Add sen-reporting of unauthorized access.
18 6.1 Giberia and Data 19 1440 Suggested deling electricing lumuage on minimization of Filt to address fraud. 19 6.1 A Association of Security Risk. 10 6.1 A Product State of the Control of Security Risk. 110 6.1 A Product State of Security Risk. 110 6.1 A Security Risk. 110 6.1 A Product State of Security Risk. 110 6.1 A Product State of Security Risk. 110 6.1 A Security	11 Concross and task  12	117	624		40	1246		Add by many to any ife way of DH for found
188 63. Minimatoria 40 1348 Suggest adding cultifug Leguage on minimator of PIT to address Transl.  19 63. By Trivoy Biok.  Associated 42 1459 This section does not the first of MT Day Section does not first of the section of Section Pilots.  120 63. All Facilitation and the Section of Section Pilots.  121 63. All Facilitation and the Section of Section Pilots.  122 63. Benefit and the Section of Section Pilots of	## 19 61A Strongs	11/	03A	Minimization	40	1340	iraud detection and prevention activities.	Add language to specify use of Pil for fraud.
19 6.A Assessment 42 H29 This section does not cle the rise of NOT taking specific copy regarding data collection and its Security Biols.  10 6.A Profits Session 48 Second collection and its Security Biols.  10 6.A Profits Session 48 Second collection and its Security Biols.  10 6.A Profit Session 48 Second collection and its Security Biols.  10 6.B A Profit Session 48 Second collection and its Security Biols.  10 6.B A Profit Session 48 Second collection and its Security Biols.  10 6.B A Profit Session Level 2 Second collection and its Security Biols.  10 6.B Add second collection and its Security Biols.  10 6.B Add second collection and its Security Biols.  10 6.B Add second collection and its Security Biols.  10 6.B Add second collection and its Security Biols.  10 6.B Add second collection and its Security Biols.  10 6.B Add second collection and its Security Biols.  10 6.B Add second collection and its Security Biols.  10 6.B Add second collection and its Security Biols.  10 6.B Add second collection and its Security Biols.  10 6.B Add second collection and its Security Biols.  10 6.B Add second collection and its Security Biols.  10 6.B Add second collection and its Security Biols.  10 6.B Add second collection and its Security Biols.  10 6.B Add second collection and its Security Biols.  10 6.B Add second collection of the second collection o	19 63A Accessment 42 1429 This section does not one the risk of MT Using specific steps regarding data odlection and its Security Bale.  10 63A Profession 48 1641 Security Se							Include additional language in line 1348. Suggested language, "but minimization procedures should be weighted
19 GSA Assessment 42 1429  Recommend ensuring the enrollment code is accompanied by a message that clearly states what the user is John Proofing Section 48 1641 enrollings for - based on CPMs is stoom learned.  19 GSB Assessment Level 2	10 GA Assessment 42 1479  Recumented ensuring the enrollment code is accompanied by a message that clearly states what the user is enrolling part and the second part of the second part	118	63A		40	1348		against valid needs of threat mitigation, fraud detection and security processes when established".
120 63A Proofing Session 48 141 enrolling for - based on CPAM's besons learned.  121 63B Authentication: 8 4091 Add 'decity owner' affer chimant.  122 63B Enrollment 41,42 1582,1617 owner.  123 63B Enrollment 41,42 1582,1617 owner.  124 63B Threats  125 63B Authentication: 8 41,42 1582,1617 owner.  126 63B Authentication: 9 400 Add 'decity owner' affer chimant.  127 63B Authentication: 9 400 Add 'decity owner' affer chimant.  128 63B Authentication: 9 400 Add 'decity owner' affer chimant.  129 63B Authentication: 9 400 Add 'decity owner' affer chimant.  129 63B Authentication: 9 40 Add 'decity owner' affer chimant.  120 63B Authentication: 9 40 Add 'decity owner' affer chimant.  120 63B Authentication: 9 40 Add 'decity owner' affer chimant.  121 63B Authentication: 9 40 Add 'decity owner' affer chimant.  122 63B Authentication: 9 40 Add 'decity owner' affer chimant.  123 63B Authentication: 9 40 Add 'decity owner' affer and previously active attempt by incorporating authoritative source validation.  124 63B Authentication: 9 5 Compromise  125 63B Authentication: 9 5 Compromise  126 63B Authentication: 9 5 Compromise  127 63B Authentication: 9 5 Compromise  128 63B Authentication: 9 5 Compromise  129 63B Authentication: 9 5 Compromise  120 63B Authentication: 9 5 Compromise  120 63B Authentication: 9 5 Compromise  121 63B Authentication: 9 5 Compromise  122 63B Authentication: 9 5 Compromise  123 63B Authentication: 9 5 Compromise  124 65B Authentication: 9 5 Compromise  125 63B Authentication: 9 5 Compromise  126 63B Authentication: 9 5 Compromise  127 63B Authentication: 9 5 Compromise  128 63B Authentication: 9 5 Compromise  129 63B Authentication: 9 5 Compromise  120 63B Authentication: 9 5 Compromise  120 63B Authentication: 9 5 Compromise  121 63B Authentication: 9 5 Compromise  122 63B Authentication: 9 5 Compromise  123 63B Authentication: 9 5 Compromise  124 63B Authentication: 9 5 Compromise  125 63B Authentication: 9 5 Compromise  126 63B Authentication: 9 5 Compromise  127 63B Authentication: 9 5 Com	120 63.6 Proding Section 48 1641 enrolling for - based on CPAN is known kerned.  121 638 4.2 Authentication 8 491 Add accompanying message to a recollection bound to the subscriber account.  122 631 Authentication 8 50 Add accompanying message to a recollection bound to the subscriber account of the absorber account of the product of the absorber account of the account of the absorber account of the account of the absorber account of the ac	119	63A	Assessment	42	1429	8-1	Include additional guidance or specific steps regarding data collection and its Security Risks.
42 Authentication  Ad Junification 2 8 491 Add Identity owner controls  Advantage level 2 8 491 Add Identity owner controls  Authenticator  Browning 12	4.2 Authentication 4.3 Authentication 4.3 Authentication 4.4 Authentic			9.3 Enrollment and			Recommend ensuring the enrollment code is accompanied by a message that clearly states what the user is	
Add identity owner of the subscriber account.	Authenticator   Comment data 27A device cannot be updated or added to account without a separate 27A code validation by the Recommend that 27A device cannot be updated or added to account without a separate 27A code validation by the Recommend that 27A device cannot be updated or added to account without a separate 27A code validation by the Recommend that 27A device cannot be updated or added to account without a separate 27A code validation by the Recommend that 27A device cannot be updated or added to account without a separate 27A code validation by the Recommend that 27A device cannot be updated or added to account without a separate 27A code validation by the Recommend that 27A device cannot be updated or added to account without a separate 27A code validation by the Recommend that 27A device cannot be updated or added to account without a separate 27A code validation by the Recommend that 27A device cannot be updated or added to account without a separate 27A code validation by the Recommend that 27A device cannot be updated or added to account without a separate 27A code validation by the Recommend that 27A device cannot be updated or added to account without a separate 27A code validation by the Recommend that 27A device cannot be updated or added to account without a separate 27A code validation by the Recommend that 27A device cannot be updated or added to account without a separate 27A code validation by the Recommend that 27A device and the account of the Account 2AR device cannot be updated or added to account without a separate 27A code validation by the Account 2AR device and the account 2AR device and the account 2AR device cannot be updated or added to account without a separate 27A code validation by the Recommend 2AR device cannot be updated or added to account without a separate 27A code validation by the Recommend 2AR device and the account 2AR device cannot per account	120	63A	Proofing Session	48	1641	enrolling for - based on CFAM's lessons learned .	Add accompanying message to enrollment code.
Binding decidence on the account, solely to validate this new binding. This would add some mitigation to account factors without direct notification of the account solely to validate this new binding. This would add some mitigation to account factors without direct notification of the account solely to validate this new binding. This would add some mitigation to account factors without direct notification of the account solely to validate this new binding. This would add some mitigation to account factors. The account of the account, solely to validate this new binding. This would add some mitigation to account factors. The account of the account, solely to validate this new binding. This would add some mitigation to account factors. The account of the account, solely to validate this new binding. This would add some mitigation to account factors. The account of the account, solely to validate this new binding. This would add some mitigation to account factors. The account of the account, solely to validate this new binding. This would add some mitigation to account factors. The account of the account, solely to validate this new binding. This would add some mitigation to account factors. The account for the account, solely to validate this new binding and the account factors. The account of the account, solely to validate this new binding and the account factors. The account of the account factors within the account factors. The account of the account factors within the account factors. The account of the account factors within the account factors. The account factors within the account factors within the account factors. The account factors within the account factors within the account factors. The account factors within the account factors within the account factors. The account factors within the account factors within the account factors. The account factors within the account factors within the account factors. The account factors within the account factors within the account factors within the account fa	Binding 6.11. Binding at 1.22 G.38 G.11. Binding at 1.4. 2 1582.16.71 tolowerse, limiting criminal ability to set up persistent account access without direct netification of the account, solely to volidate this new binding. This would add some mitigation to account to the count of the account observe.  1.23 G.38 G.12. Account Recovery 4.4 1.681 Exposed on addresses of record statement by incorporating authoritative source validation.  1.24 G.58 S. 12.2 Account Recovery 5.1. Authoritations 5.2 1.933 1.02. Account Recovery 6.2. Institute the control of the account validation of the acc	121	63B		8	491	Add 'identity owner' after claimant.	
Binding decidence on the account, solely to validate this new binding. This would add some mitigation to account factors without direct notification of the account solely to validate this new binding. This would add some mitigation to account factors without direct notification of the account solely to validate this new binding. This would add some mitigation to account factors without direct notification of the account solely to validate this new binding. This would add some mitigation to account factors. The account of the account, solely to validate this new binding. This would add some mitigation to account factors. The account of the account, solely to validate this new binding. This would add some mitigation to account factors. The account of the account, solely to validate this new binding. This would add some mitigation to account factors. The account of the account, solely to validate this new binding. This would add some mitigation to account factors. The account of the account, solely to validate this new binding. This would add some mitigation to account factors. The account of the account, solely to validate this new binding. This would add some mitigation to account factors. The account for the account, solely to validate this new binding and the account factors. The account of the account, solely to validate this new binding and the account factors. The account of the account factors within the account factors. The account of the account factors within the account factors. The account of the account factors within the account factors. The account factors within the account factors within the account factors. The account factors within the account factors within the account factors. The account factors within the account factors within the account factors. The account factors within the account factors within the account factors. The account factors within the account factors within the account factors. The account factors within the account factors within the account factors within the account fa	Binding 6.11. Binding at 1.22 G.38 G.11. Binding at 1.4. 2 1582.16.71 tolowerse, limiting criminal ability to set up persistent account access without direct netification of the account, solely to volidate this new binding. This would add some mitigation to account to the count of the account observe.  1.23 G.38 G.12. Account Recovery 4.4 1.681 Exposed on addresses of record statement by incorporating authoritative source validation.  1.24 G.58 S. 12.2 Account Recovery 5.1. Authoritations 5.2 1.933 1.02. Account Recovery 6.2. Institute the control of the account validation of the acc							
6.11 Blading at Enrollment 41,42 1582,1617 were.  6.38 6.12.2 Account Recovery.  124 6.38 5.12.2 Account Recovery.  125 6.38 Threats 52 19.33 Incorporate social engineering search of the model of the composition of the execution of the victims device settings by the criminal formation of the victims device settings by the criminal formation of the subscriber source will dealer of the subscriber source. The subscriber source will dealer of the subscriber source will dealer of the subscriber source.  126 6.38 Threats 52 19.33 Incorporate social engineering senaris.  22 Threat Migistro Strategies 57 Compromise C	122 6.38 Enrollment 41,42 1562_1617 owere.  123 6.38 6.12.3 Account Recovery 124 1.681 Expound on 'addresses of record' statement by incorporating authoritative source validation.  125 6.38 0.12.3 Account Recovery 126 6.38 Threats 127 5.2 1923 127 6.38 Threats 128 6.38 Threats 129 6.38 Threats 129 6.38 Threat Mitigation 120 6.38 Strategies 120 6.38 Strategies 121 5.5 Compromise 122 6.38 Threat Mitigation 123 6.38 Threat Mitigation 124 6.38 Threat Mitigation 125 6.38 Threat Mitigation 126 6.38 Strategies 127 6.38 Threat Mitigation 128 6.38 Threat Mitigation 129 6.30 Strategies 129 6.30 Strategies 120 Adheritative 120 6.38 Threat Mitigation 120 6.38 Strategies 120 Adheritative 121 6.38 Threat Mitigation 122 6.38 Threat Mitigation 123 6.38 Threat Mitigation 124 6.38 Threat Mitigation 125 6.38 Threat Mitigation 126 6.38 Strategies 127 6.38 Threat Mitigation 128 6.38 Threat Mitigation 129 6.30 Strategies 120 6.30 Stra							
122   638   Enrollment   41,42   1582, 1617   owner.	122   638   Enrollment   41,42   1582,1617   owner.							
123 6.38 6.1.2.3 Account Recovery 44 16.61 Expond on 'addresses of record' statement by incorporating authoritative source validation.  124 6.38 Threats 52 1933  125 Farment Mitigation 55 Compromise  126 6.38 Strategies 57 Shared Signaling  127 6.38 Threats 52 N/A incorporate social engineering scenario.  128 6.38 Threats 52 N/A incorporate social engineering scenario.  129 6.38 Strategies 57 Shared Signaling  120 6.38 Threats 52 N/A incorporate social engineering scenario.  120 6.38 Threats 52 N/A incorporate social engineering scenario.  121 6.38 Threats 52 N/A incorporate social engineering scenario.  122 6.38 Threats 52 N/A incorporate social engineering scenario.  123 6.36 Threats 52 N/A incorporate social engineering scenario.  124 6.38 Threats 52 N/A incorporate social engineering scenario.  125 8.39 Threats 52 N/A incorporate social engineering scenario.  126 6.38 Threats 52 N/A incorporate social engineering scenario.  127 6.38 Threats 52 N/A incorporate social engineering scenario.  128 6.38 Threats 52 N/A incorporate social engineering scenario.  129 6.30 Stateples 57 Shared Signaling 44 1701 Recommend incorporating language that admonwledges overall risks of using a Federated model.  129 6.30 Stateples 57 Shared Signaling 32, 33 1201,1207 Stateples 57 Shared Signaling 32, 33 1201,1207 State account: Three should be an exception added in the case of fraudulent activity response or legal due process  130 Stateples 32, 33 1201,1207 State, The Idl/RP MAY send a signal reporting for engine prospection on what data attributes are required for federated model via the API.  131 6.30 Stateples 45 Should should be specific on what data attributes are required for federated model via the API.  131 6.31 Stateples 57 Shared Signaling 32, 33 1201,1207 State, The Idl/RP MAY send a signal required for federated model via the API.  132 6.32 Stateples 57 Shared Signaling 32, 33 1201,1207 State, The Idl/RP MAY send a signal required for federated model via the API.	123 638 6.1.2.3 Account Recovery 144 1681 Expound nicedress of record statement by incorporating authoritative source validation. 125 638 Threats 126 638 Threats 127 638 Threats 128 Compromise 129 179.3 Incorporate social engineering scenario. 129 638 Threats 120 638 Th	122	63B	Enrollment	41, 42	1582, 1617		owner. Similar language does exist in line 1636-1642.
124 6.88 Threats 52 1933 Incorporate social engineering scenario.  125 6.88 Threat Mitigation 126 6.38 Threat Mitigation 127 6.38 Threat Mitigation 128 Add text forwarding of SMS code due to modified configuration of the victims device settings by the criminal 129 6.38 Authenticator 120 8.1 Authenticator 121 6.38 Threat Mitigation 122 6.38 Threat Mitigation 123 Authenticator 124 Associal Engineering 125 Robin Threats 125 N/A 126 Robin Threats 127 6.38 Threats 128 6.38 Authenticator 128 6.38 Authenticator 129 6.30 Authenticator Binding 129 6.30 S. Farday Might September 129 1067-1069 States, "All attributes associated with an IP subscriber account teerminated." There should be an exception added in the case of fraudulent activity response or legal due process 130 6.30 Requirements 130 6.30 Requirements 130 6.30 S. Frivacy 131 6.30 S. Frivacy 132 6.30 S. Frivacy 133 Incorporate security consideration for risk assessment 134 6.30 S. Frivacy 135 Frivacy 136 Should be specific on what data attributes are required for federated model with the API. 136 C. S. Frivacy 137 Should be specific on what data attributes are required for federated model with the API. 137 C. S. Frivacy 138 Should be specific on what data attributes are required for federated model with the API. 139 C. S. Frivacy 130 Should be specific on what data attributes are required for federated model with the API. 130 C. S. S. Frivacy 131 C. S. Should be specific on what data attributes are required for federated model with the API. 132 C. S. Should be specific on what data attributes are required for federated model with the API. 133 C. S. Should be specific on what data attributes are required for federated model with the API.	124 638 Threats 52 1933 Incorports social engineering scenario.  125 638 Threat Migation 126 638 St. Authenticator 127 638 Threat Migation 128 St. Threat Migation 129 St. Threat Migation 120 St. Threat Migation 120 St. Threat Migation 121 St. Threat Migation 122 St. Threat Migation 123 St. Authenticator 124 St. St. Threat Migation 125 St. St. Authenticator 126 638 Threat Migation 127 St.	123	63B	6.1.2.3 Account Recovery	44	1681	Expound on 'addresses of record' statement by incorporating authoritative source validation.	records maintained by an authoritative source".
Second Companies   Second Comp	125 638 Threats 55 Compromise Add text forwarding of SMS code due to modified configuration of the victims device settings by the criminal 26 8.2 Threat Mitigation 57 Table 4, Social Engineering 80 Strategies 57 Bow 0 authenticates with CSP name for 'X agency' 10 authenticates with CSP name for 'X	124	63B		52	1033	Incorporate social angineering scenario	
Table 4, Social Engineering Explicitly state the reason for the authentication code delivery in the SMS sent to the user. "This code is being used to authenticate with "CSP name" for "X agency".  Bal Authenticator Threats 52 N/A Incorporate security consideration for risk assessment    127	Table 4, Social Engineering Explicitly state the reason for the authentication code delivery in the SMS sent to the user. "This code is being used to authenticate with 'CSP name' for 'X agency'".  Recommend adding 3rd consideration: The impact to the integrity of the authentication system and user if dat not retained.  Recommend adding 3rd consideration: The impact to the integrity of the authentication system and user if dat not retained.  Recommend adding 3rd consideration: The impact to the integrity of the authentication system and user if dat not retained.  Recommend adding 3rd consideration: The impact to the integrity of the authentication system and user if dat not retained.  Recommend adding 3rd consideration: The impact to the integrity of the authentication system and user if dat not retained.  Recommend adding 3rd consideration: The impact to the integrity of the authentication system and user if dat not retained.  Recommend adding 3rd consideration: The impact to the integrity of the authentication system and user if dat not retained.  Recommend adding 3rd consideration: The impact to the integrity of the authentication system and user if dat not retained.  Recommend adding 3rd consideration: The impact to the integrity of the authentication system and user if dat not retained.  Recommend adding 3rd consideration: The impact to the integrity of the authentication system and user if dat not retained.  Recommend adding 3rd consideration: The impact to the integrity of the authentication system and user if dat not retained.  Recommend adding 3rd consideration: The impact to the integrity of the authentication system and user if dat not retained.  Recommend adding 3rd consideration: The impact to the integrity of the authentication system and user if dat not retained.  Recommend adding 3rd consideration: The impact to the integrity of the authentication system and user if dat not retained.  Recommend adding 3rd consideration: The impact to the integrity of the authentication system and user if dat not			8.1 Authenticator		Table 3 - Endpoint		
126 638 Strategies 57 Row to authenticate with "CSP name" for "X agency"  127 638 Threats 52 N/A Incorporate security consideration for risk assessment  128 638 Authenticator Binding 44 1701 Recommend incorporating language that admowledges overall risks of using a Federated model.  129 63C 5.4.4 Attribute Collection 29 1067-1069 states, "All attributes associated with an RP subscriber account; regardless of their source, SHALL be removed when the RP subscriber account is terminated." There should be an exception added in the case of fraudulent activity response or legal due process.  130 63C Requirements 30 1112-1117 Exponse or legal due process.  131 636 5.7 Shared Signaling 32, 33 1201, 1207 these actions.  132 63C 6.3 Identity APIs 45 1536 Should be specific on what data attributes are required for federated model via the API.  134 63C 6.3 Identity APIs 45 1536 Should be specific on what data attributes are required for federated models via the API.	126 638 Strategies 57 Row to authenticate with 'CSP name' for 'X agency'' and a signal regarding the following changes to the subscriber account.' The recommendation is to change that a signal regarding the following changes to the subscriber account.' The recommendation is to change this specific on what data attributes are required for federated model via the API.  126 638 Strategies 57 Row to authenticate with 'CSP name' for 'X agency'' is being used to authenticate with CSP name' for 'X agency''.  127 638 Threats 52 N/A incorporate security consideration for risk assessment  128 638 Authenticator Binding 44 1701 Recommend incorporating language that advanced legs overall risks of using a Federated model.  129 63C 54.4 Attribute Collection 29 1067-1069 Threat the removed when the RP subscriber account is terminated.' There should be an exception added in the case of fraudulent activity response or legal due process.  129 63C 75.5 Privacy  120 63C Requirements 30 1112-1117 The report of a CSP MUST have their own, in house, cross client, fraud detection, analysis and response posture.  130 63C Requirements 30 1112-1117 The recommendation is to change this to MUST send a signal regarding the following changes to the subscriber account.' The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  131 63C 6.3 Identity APIs 45 1536 Should be specific on what data attributes are required for federated model via the API.  132 63C 6.3 Identity APIs 45 1536 Should be specific on what data attributes are required for federated model via the API.  133 63C 10.2.1 User Perspectives on Online Identity  134 63C 8.5 Identity APIs 45 1536 Should be specific on what data attributes are required for federated model via the API.  135 63C 10.2.1 User Perspectives on Online Identity  136 63C 8.5 Identity APIs 45 1536 Should be specific on what data attributes are required for federated model via the API.  135 63C 10.2.1 User Perspectives on Online Identity  136 63C 8.5 I	125	63B	Threats	55	Compromise	Add text forwarding of SMS code due to modified configuration of the victims device settings by the criminal	Add text forwarding of SMS code due to modified configuration of the victims device settings by the criminal
8.1 Authenticator Threats 52 N/A Incorporate security consideration for risk assessment  8.2 N/A Incorporate security consideration for risk assessment  8.3 Authenticator Ending 4 Incorporate security consideration for risk assessment  8.4 Authenticator Binding 4 Incorporating Inguage that admonwledges overall risks of using a Federated model.  8.5 Privacy  9. 1067-1069  130  130  130  130  131  130  130  13	8.1 Authenticator Threats 52 N/A Incorporate security consideration for risk assessment  8.6 Authenticator Binding Authentication for risk assessment Authentication for risk at another Authentication for risk tax denowledges overall risks of using a Federated model Authenticator Binding Authenticator Bindin							
127 638 Threats 52 N/A Incorporate security consideration for risk assessment    Commended in the case of the case of fraud targeting one agency to proliferate at another stringer data attribute checks for different partners)   Commended in figurage includes:	127 638 Threats 52 N/A Incorporate security consideration for risk assessment  128 638 Authenticator Binding 44 1701 Recommend incorporating language that acknowledges overall risks of using a Federated model.  129 636 5.4. Attribute Collection 29 1067-1069 states, "All attributes associated with an RP subscriber account, regardless of their source, SHALL be removed when the RP subscriber account is terminated." There should be an exception added in the case of further emphasizing the need for a CSP MUST have their own, in house, cross client, fraud detection, analysis and response posture.  130 636 Requirements 30 1112-1117  131 636 5.7 Shared Signalling 32,33 1201,1207 these actions.  132 636 6.3 Identity APIs 45 1536 Should be specific on what data attributes are required for federated model with the Informaccount creation.  133 636 on Online Identity 63 1960 Recommend adding the ability for users to lock their identity from account creation.  134 637 Recommend being more specific on what data attributes are required for federated model with the API.  135 636 On Online Identity on the statement in the case of fraudulent activity response or legal due process.  136 And the case of fraudulent activity response or legal due process.  137 Add an exception to the statement in the case of fraudulent activity response or legal due process.  138 Add an exception to the statement in the case of fraudulent activity response or legal due process.  139 Add an exception to the statement in the case of fraudulent activity response or legal due process.  130 Add an exception to the statement in the case of fraudulent activity response or legal due process.  130 Add an exception to the statement in the case of fraudulent activity response or legal due process.  130 Add an exception to the statement in the case of fraudulent activity response or legal due process.  131 Add an exception to the statement in the case of fraudulent activity response or legal due process.  132 Add an exception to the statement in the case of frau	126	63B		57	Row	to authenticate with 'CSP name' for 'X agency'"	
Recommended language includes: 128 63B Authenticator Binding 44 1701 Recommend incorporating language that acknowledges overall risks of using a Federated model.  Lines 1067-1069 states, "All attributes associated with an RP subscriber account, regardless of their source, SHALL be removed when the RP subscriber account is terminated." There should be an exception added in the case of fraudulent activity response or legal due process.  This paragraph cites that the CSP should discourage tracking of a user across multiple clients. It is recommended further emphasizing the need for a CSP MUST have their own, in house, cross client, fraud detection, analysis and response posture.  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account." The recommended for these account." The recommended for these account. The recommended for the search of the	Recommended tanguage includes: -Including potential for fraud dargeting one agency to proliferate at another -Limitations for CSP to tailor their ID proding strategies based on risks to individual clients (i.e. more stringent data attribute checks for different partners) -Reduced visibility into third party vendor proofing parameters  Lines 1067-1069 states, "All attributes associated with an RP subscriber account; regardless of their source, SHALL - removed when the RP subscriber account is terminated." There should be an exception added in the case of fraudulent activity response or legal due process.  This paragraph cites that the CSP should discourage tracking of a user across multiple clients. It is recommended further emphasizing the need for a CSP MUST have their own, in house, cross client, fraud detection, analysis and response posture.  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal if the client agency requests notification of the search of the client agency requests notification of the search of the client agency requests notification of Lines 1201 und 1207 state, "The IdP/RP MAY send a signal if the client agency requests notification of the search of the client agency requests notification of the search of the client agency requests notification of Lines 1201 und 1207 state, "The IdP/RP MAY send a signal if the client agency requests notification of the search of the client agency requests notification of Lines 1201 and 1207 state, "The IdP/RP MAY send a signal if the client agency requests notification of the search of the client agency requests notification of Lines 1201 and 1207 state, "The IdP/RP MAY send a signal if the client agency requests notification of Lines 1201 and 1207 state, "The IdP/RP MAY send a signal if the client agency requests notification of Lines 1201 and 1207 state, "The IdP/RP MAY send a signal if the client agency requests notification Lines 1201 and 1207 state, "The IdP/RP MAY send a signal if the client agency requests notification Lines 1201 and 1207 state,	127	63B		52	N/A	Incorporate security consideration for risk assessment	
128   63B   Authenticator Binding   44   1701   Recommend incorporating language that acknowledges overall risks of using a Federated model.   Authenticator Binding   44   1701   Recommend incorporating language that acknowledges overall risks of using a Federated model.   Reduced visibility into third party vendor proofing parameters	128 63B Authenticator Binding 44 1701 Recommend incorporating language that acknowledges overall risks of using a Federated model.  129 63C 5.4.4 Attribute Collection 29 1067-1069 states, "All attributes associated with an RP subscriber account; terminated." There should be an exception added in the case of fraudulent activity response or legal due process.  130 63C Requirements 30 1112-1117  131 63C 5.7 Shared Signaling 32,33 1201,1207  132 63C 6.3 Identity APIs 45 1536 Should be specific on what data attributes are required for federated model via the API.  133 63C 0.0 Identity 4 PIs 45 1536 Should be specific on what data attributes are required for federated model via the API.  134 63C 0.0 Identity 4 PIs 45 1536 Should be specific on what data attributes are required for federated model via the API.  135 63C 0.0 Identity 6 Pis valor their 1D proofing strategies based on risks to individual clients (i.e. more stringent data attributes, see during the first source, SHALL be remarked." There should be used in the case of fraudulent activity response or legal due process.  Add an exception to the statement in the case of fraudulent activity response or legal due process.  Add an exception to the statement in the case of fraudulent activity response or legal due process.  Add an exception to the statement in the case of fraudulent activity response or legal due process.  Add an exception to the statement in the case of fraudulent activity response or legal due process.  Add an exception to the statement in the case of fraudulent activity response or legal due process.  Add an exception to the statement in the case of fraudulent activity response or legal due process.  Add an exception to the statement in the case of fraudulent activity response or legal due process client, fraud detection, analysis and response posture.  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account." The recommendation is to change this to MUST send a signal if the client agen					,		
6.12.4. External Authenticator Binding 44 1701 Recommend incorporating language that acknowledges overall risks of using a Federated model. Lines 1067-1069 states, "All attributes associated with an RP subscriber account, regardless of their source, SHALL be removed when the RP subscriber account is terminated." There should be an exception added in the case of fraudulent activity response or legal due process.  This paragraph cites that the CSP should discourage tracking of a user across multiple clients. It is recommended further emphasizing the need for a CSP MUST have their own, in house, cross client, fraud detection, analysis and response posture.  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account." The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  Solved the commendation is to change this to MUST send a signal if the client agency requests notification of these actions.  Solved the commendation is to change this to MUST send a signal if the client agency requests notification of these actions.  Solved the commendation is to change this to MUST send a signal if the client agency requests notification of these actions.  Solved the commendation is to change this to MUST send a signal if the client agency requests notification of these actions.  Solved the commendation is to change this to MUST send a signal if the client agency requests notification of these actions.  Solved the commendation is to change this to MUST send a signal if the client agency requests notification of these actions.  Solved the commendation is to change this to MUST send a signal if the client agency requests notification of the same account." The recommendation is to change this to MUST send a signal if the client agency requests notification of the same account. The commendation is to change this to MUST send a signal if the client agency requests notification of the same account. The commendation	4 Authenticator Binding 44 1701 Recommend incorporating language that acknowledges overall risks of using a Federated model.  Lines 1067-1069 states, "All attributes associated with an RP subscriber account, regardless of their source, SHALL be removed when the RP subscriber account is terminated." There should be an exception added in the case of fraudulent activity response or legal due process.  Add an exception to the statement in the case of fraudulent activity response or legal due process.  This paragraph cites that the CSP should discourage tracking of a user across multiple clients. It is recommended further emphasizing the need for a CSP MUST have their own, in house, cross client, fraud detection, analysis and response posture.  Lines 1021 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account." The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  Lines 1021 and 1207 state, "The IdP/RP MAY send a signal free delication, analysis and response posture.  Lines 1021 and 1207 state, "The IdP/RP MAY send a signal if the client agency requests notification of these actions.  Lines 1021 and 1207 state, "The IdP/RP MAY send a signal if the client agency requests notification of these actions.  Update MAY to MUST statement  Lines 1021 user Perspectives on Online Identity for users to lock their identity from account creation.  Recommend including the ability for users to lock their identity from account creation.  Either in 63A or in Implementation Guidance, there should be defined minimum data attributes, per piece of							Limitations for CSP to tailor their ID proofing strategies based on risks to individual clients (i.e. more stringent)
Lines 1067-1069 states, "All attributes associated with an RP subscriber account, regardless of their source, SHALL be removed when the RP subscriber account is terminated." There should be an exception added in the case of fraudulent activity response or legal due process.  This paragraph cites that the CSP should discourage tracking of a user across multiple clients. It is recommended further emphasising the need for a CSP MUST have their own, in house, cross client, fraud detection, analysis and response posture.  This paragraph cites that the CSP should discourage tracking of a user across multiple clients. It is recommended further emphasising the need for a CSP MUST have their own, in house, cross client, fraud detection, analysis and response posture.  Lines 1021 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account." The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  Should be specific on what data attributes are required for federated model via the API.  Recommend being more specific on what data attributes are required for federated models via the API.	Lines 1067-1069 states, "All attributes associated with an RP subscriber account, regardless of their source, SHALL be removed when the RP subscriber account is terminated." There should be an exception added in the case of fraudulent activity response or legal due process.  This paragraph cites that the CSP should discourage tracking of a user across multiple clients. It is recommended further emphasizing the need for a CSP MUST have their own, in house, cross client, fraud detection, analysis and response posture.  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account". The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  132 63C 6.3 Identity APIs 45 1536 Should be specific on what data attributes are required for federated model via the API.  133 63C 0 100 In Perspectives on Online Identity 63 1960 Recommend adding the ability for users to lock their identity from account creation.  Either in 63A or in Implementation Guidance, there should be defined minimum data attributes, per piece of	100	COD		,,	4504		data attribute checks for different partners)
be removed when the RP subscriber account is terminated." There should be an exception added in the case of fraudulent activity response or legal due process.  Add an exception to the statement in the case of fraudulent activity response or legal due process.  This paragraph cites that the CSP should discourage tracking of a user across multiple clients. It is recommended further emphasizing the need for a CSP MUST have their own, in house, cross client, fraud detection, analysis and response posture.  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account." The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account." The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account." The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account." The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber response posture  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber response posture  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber response posture  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber response posture  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following chang	be removed when the RP subscriber account is terminated." There should be an exception added in the case of fraudulent activity response or legal due process.  This paragraph cites that the CSP should discourage tracking of a user across multiple clients. It is recommended further emphasizing the need for a CSP MUST have their own, in house, cross client, fraud detection, analysis and response posture.  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal fregarding the following changes to the subscriber account." The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  132 63C 6.3 Identity APIs 45 1536 Should be specific on what data attributes are required for federated model via the API.  133 63C 0 no fuller lednity 63 1960 Recommend adding the ability for users to lock their identity from account creation.  Either in 63A or in Implementation Guidance, there should be defined minimum data attributes, per piece of	128	63B	Autnenticator Binding	44	1701		Needuced visibility into third party vendor proofing parameters
129 63C 5.4.4 Attribute Collection 29 1067-1069 fraudulent activity response or legal due process.  This paragraph cites that the CSP should discourage tracking of a user across multiple clients. It is recommended further emphasising the need for a CSP MUST have their own, in house, cross client, fraud detection, analysis and response posture.  130 63C Requirements 30 1112-1117 response or legal due process.  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account". The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  131 63C 5.7 Shared Signaling 32, 33 1201, 1207 these actions.  132 63C 6.3 Identity APIs 1536 Should be specific on what data attributes are required for federated model via the API.  134 Recommend being more specific on what data attributes are required for federated models via the API.	129 63C 5.4.4 Attribute Collection 29 1067-1069 fraudulent activity response or legal due process  This paragraph cites that the CSP should discourage tracking of a user across multiple clients. It is recommended further emphasizing the need for a CSP MUST have their own, in house, cross client, fraud detection, analysis and response posture.  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account." The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  132 63C 5.7 Shared Signaling 32, 33 1201, 1207  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal if the client agency requests notification of these actions.  Update MAY to MUST statement  Update MAY to MUST statement  133 63C 0 no Online Identity 63 1960 Recommend adding the ability for users to lock their identity from account creation.  Either in 63A or in Implementation Guidance, there should be defined minimum data attributes, per piece of							
130 63C Requirements 30 1112-1117 further emphasizing the need for a CSP MUST have their own, in house, cross client, fraud detection, analysis and response posture.  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account". The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  132 63C 6.3 Identity APIs 45 1536 Should be specific on what data attributes are required for federated model via the API.  132 Recommend being more specific on what data attributes are required for federated models via the API.	For the remphasizing the need for a CSP MUST have their own, in house, cross client, fraud detection, analysis and response posture.  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account." The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  132 63C 5.7 Shared Signaling 32, 33 1201, 1207 these actions.  138 63C 6.3 Identity APIs 45 1536 Should be specific on what data attributes are required for federated model via the API.  139 63C 10.2.1 User Perspectives on Online Identity 63 1960 Recommend adding the ability for users to lock their identity from account creation.  Either in 63A or in Implementation Guidance, there should be defined minimum data attributes, per piece of	129	63C	5.4.4 Attribute Collection	29	1067-1069		Add an exception to the statement in the case of fraudulent activity response or legal due process
5.5 Privacy 130 63C Requirements 30 1112-1117 Further emphasizing the need for a CSP MUST have their own, in house, cross client, fraud detection, analysis and response posture.  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account". The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account". The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account". The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account". The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account". The recommendation is to change this to MUST send a signal if the client agency requests notification of Update MAY to MUST statement  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account". The recommendation is to change this to MUST send a signal regarding the following changes to the subscriber account. The recommendation is to change this to MUST send a signal regarding the following changes to the subscriber account."  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account."  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account."  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the f	5.5 Privacy Requirements 30 1112-1117 response posture.  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account." The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  131 63C 5.7 Shared Signaling 32,33 1201,1207 Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account." The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  132 63C 63.1 Identity APIs 120, 1User Perspectives 133 63C 0 no nline Identity 63 1960 Recommend adding the ability for users to lock their identity from account creation. Either in 63A or in Implementation Guidance, there should be defined minimum data attributes, per piece of						This paragraph sites that the CSP should discourage tracking of a user across multiple dients. It is recommended	
130 63C Requirements 30 1112-1117 response posture. response posture  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account". The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  131 63C 5.7 Shared Signalling 32, 33 1201, 1207 these actions.  132 63C 6.3 Identity APIs 45 1536 Should be specific on what data attributes are required for federated model via the API.  102.1 User Perspectives	130 63C Requirements 30 1112-1117 response posture. response posture  Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber account". The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  131 63C 5.7 Shared Signaling 32,33 1201,1207 these actions.  132 63C 6.3 Identity APIs 45 1536 Should be specific on what data attributes are required for federated model via the API. Recommend being more specific on what data attributes are required for federated models via the API 10.2.1 User Perspectives on Online Identity 63 1960 Recommend adding the ability for users to lock their identity from account creation. Recommend including the ability for users to lock their identity from account creation.			5.5 Privacy				Provide more emphasis that a CSP MUST have their own, in house, cross client, fraud detection, analysis and
131 63C 5.7 Shared Signaling 32, 33 1201, 1207 these actions.  132 63C 6.3 Identity APIs 45 1536 Should be specific on what data attributes are required for federated model via the API.  132 Prespectives Should be specific on what data attributes are required for federated model via the API.	account". The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  132 63C 6.3 Identity APIs 45 1536 Should be specific on what data attributes are required for federated model via the API. Recommend being more specific on what data attributes are required for federated models via the API 10.2.1 User Perspectives on Online Identity 63 1960 Recommend adding the ability for users to lock their identity from account creation. Recommend including the ability for users to lock their identity from account creation.	130	63C	Requirements	30	1112-1117	response posture.	response posture
131 63C 5.7 Shared Signaling 32, 33 1201, 1207 these actions.  132 63C 6.3 Identity APIs 45 1536 Should be specific on what data attributes are required for federated model via the API.  132 Prespectives Should be specific on what data attributes are required for federated model via the API.	account". The recommendation is to change this to MUST send a signal if the client agency requests notification of these actions.  132 63C 6.3 Identity APIs 45 1536 Should be specific on what data attributes are required for federated model via the API. Recommend being more specific on what data attributes are required for federated models via the API 10.2.1 User Perspectives on Online Identity 63 1960 Recommend adding the ability for users to lock their identity from account creation. Recommend including the ability for users to lock their identity from account creation.						Lines 1201 and 1207 state, "The IdP/RP MAY send a signal regarding the following changes to the subscriber	
132 63C 6.3 Identity APIs 45 1536 Should be specific on what data attributes are required for federated model via the API. Recommend being more specific on what data attributes are required for federated models via the API 10.2.1 User Perspectives	132 63C 6.3 Identity APIs 45 1536 Should be specific on what data attributes are required for federated model via the API. Recommend being more specific on what data attributes are required for federated models via the API.  10.2.1 User Perspectives on Online Identity 63 1960 Recommend adding the ability for users to lock their identity from account creation. Recommend including the ability for users to lock their identity from account creation  Either in 63A or in Implementation Guidance, there should be defined minimum data attributes, per piece of	121	620	E 7 Chanad Ci	22.22	1201 1207	account". The recommendation is to change this to MUST send a signal if the client agency requests notification of	Hwdata MAV to MHCT statement
10.2.1 User Perspectives	10.2.1 User Perspectives on Online Identity 63 1960 Recommend adding the ability for users to lock their identity from account creation.  Recommend including the ability for users to lock their identity from account creation.  Either in 63A or in Implementation Guidance, there should be defined minimum data attributes, per piece of							
	133 63C on Online Identity 63 1960 Recommend adding the ability for users to lock their identity from account creation. Recommend including the ability for users to lock their identity from account creation  Either in 63A or in Implementation Guidance, there should be defined minimum data attributes, per piece of	132	63C		45	1536	Should be specific on what data attributes are required for federated model via the API.	Recommend being more specific on what data attributes are required for federated models via the API
	Either in 63A or in Implementation Guidance, there should be defined minimum data attributes, per piece of	133	63C		63	1960	Recommend adding the ability for users to lock their identity from account creation.	Recommend including the ability for users to lock their identity from account creation
								7
4.3.4.1 Evidence evidence, that should be required to be validated. This would set a standard across the CSPs on what will be							evidence, that should be required to be validated. This would set a standard across the CSPs on what will be	
	134 63A Validation 12 601 validated on the evidence at each xAL level.	134	63A	Validation	12	601	validated on the evidence at each xAL level.	