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

Please submit responses to dig-comments@nist.gov by October 7, 2024.

Organization:	1Kosmos
Name of Submitter/POC:	Christine Owen
Email Address of Submitter/POC:	

Section Sect	Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	# Line #	Comment (Include rationale for comment)	Suggested Change
Oth 137 1.3 3-14 transplanment or processing and compared to proceed and the processing of the							
Supplied Company Com				7			
Compared to "Cisir for administration of the process and a single and a		63A	1.3.2	6	5 53	4 typographical error	remove space after Organizations
Sign 13 at 13 confirmed and applicants in separation and security and equation in the part of the security and application of the part of the security and applications and and applica							
28.5 24.1 0.1 0.2 Expression to the second profession and special profesion and special profession and special profession and special pro		63A	213	8	61		
SA 1.1.1 1.2 19 10 for the tips algorithms one perform fault comparisons more accurately and equalitarity their horses. SA 1.1.2 19 10 for the tips algorithms can be profited to the second of the comparison of		••••		11			
50. 1.5.1 1.7. 29 an against related by proceded as affect and a agreement companion during an in person propriet groups. 50. 1.1.1.2 1.5. 1.5. 1.5. 1.5. 1.5. 1.5.		03A	2.4.1.1	11	. 07	4 typographical circi	The list Contains two number 1 items
50. 1.5.1 1.7. 29 an against related by proceded as affect and a agreement companion during an in person propriet groups. 50. 1.1.1.2 1.5. 1.5. 1.5. 1.5. 1.5. 1.5.						Cinca the ten algorithms now perform facial comparisons more accurately and equitably then hymans	Add this contains "Optionally the photo on the identity avidence can be seemed and algorithmically compared to a photo of the
\$1.12 29 Organization should continuously monotory performance or do not of disputate performance or do allow of efficiency and the performance of the performance		624	2.5.4				
Old 13.22 1 13 300 for infectiveness. Old 13.22 1 10 20 for size of the common of the	-	63A	2.5.1	14	/9		applicant taken by the proofing agent.
Signate highly direct direct prices preserving rectionages, such as exception on basinery, exists an exception of possible and processing and acceptance of the prices of the direct possible and the processing of the prices of the direct possible and the processing of a starting, as should only be explicitly, existed and the processing of a starting, as should only be explicitly, existed and the processing of a starting, as should only be explicitly, existed and instruction according of the cancellance of projection in provinces the left by the processing of a starting, as should only be explicitly, existed and instruction according to the cancellance of projection in provinces the left by the processing of a starting, as should be reported. 13 27 67 670 garden featurement that a product of a starting and according to the proposition of the product of a starting and according to the product of according to the product of a starting and according to the product of according to the product of a starting and according to the product of according to		504					
SA 13.23 22 130 of raises	-	63A	3.1.2.1	19	93		
Explained users may five benefite to desting profiling for example, where good of address is required a phone from example, and under the profiling for example and phone. Since a type of above for the individuo projection. It is described recovered under the contept of a phone for the projection of the individuo projection. It is described to expect of a phone for the projection of the projection of the individuo projection. It is described to project the projection of the individuo projection of th							
sa is fast prevention measure. In this will cross a barrier to a homeless individual with a pre-good place. Bits as 1 specified or produce of a barrier, so should only the equility clied out if there is reduced or projection in prevention is designed. 2 2 39 3 2 39 3 2 39 3 2 39 3 2 39 3 2 30 3 2 30 3 2 30 3 2 30 3 2 30 3 2 30 3 2 30 3 2 30 3 3 2 30 3 3 2 30 3 3 2 30 3 3 2 30 3 3 2 30 3 3 2 30 3 3 2 30 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3		63A	3.1.3.2	22	103		
bone. Biss is a type of harm that involves proplace. It is therefore covered and or the concept of a barries, so should not be equilibly read of if projudice in government identity provides a part of the services of the services. If you projudice existed that would be a service in the services of the							1
same, so should only be explicitly called out if there is evidence of projection in government identity to profile grosses. Such projection section that would be a related to the world be a related to the extended to the world be a related to delect deceleration and segar for the world believe to the							
oponed processes. If such projudice sites of hat would be a sorrous issue, no fifteen is evidence opened processes. If such projudice is the other provided in processes and by agencies. It is understandable that usually issues on the a barrier to some involvable processes and by agencies. It is understandable that usually issues on the a barrier to some involvable processes and the properties of the pr						phone. Bias is a type of barrier that involves prejudice. It is therefore covered under the concept of a	
SSA 3 2 29 599 Society completes should be provided. It is understanded be that sabelity issues can be a barrier to some individuals presenting an authenticator successfully, for example, submeritator apps may change numbers too quickly for some control of the provided						barrier, so should only be explicitly called out if there is evidence of prejudice in government identity	
a understandable that usability issues can be a barrier to some individuals precenting an authentication stay, authentication span, with the control of the stay of the control of the history of the control of the history of the control of the history of the evolution of the history of the control of the history of the evolution of the history of the control of the history of the evolution of the history of the control of the history of the evolution of the history of the control of the history of the evolution of the evolution of the history of the evolution of						proofing processes. If such prejudice existed that would be a serious issue, so if there is evidence	
a the understandable that usability sous can be a barrier to once individuals precenting an authenticator says who they may change numbers to quickly for some users to successfully, ever them as a second factor, thewever, what 'bas's or prejudice could be styll a submitted to may could be a submitted to the property of the property		63A	3	23	95	9 specific examples should be provided.	Remove the phrase "including biases" which implies that prejudice is part of the identity proofing processes used by agencies.
authenticator auccendully. For example, authenticator apps may change numbers too quickly for some ourset to successfully enter them as extended from the extended of the play of the policy of the spoil of the property of the policy of the spoil of the policy of the policy of the spoil of the policy of the policy of the spoil of the policy of the spoil of the policy o							
users to accessfully where them as a second factor. However, what 'ba's' or prejudics coals as a play during a field as altherections to that the ovidening of an authenticator may applicate "and like authenticator may a second feel and the integer of the claimed dentity to the applicant of the second of the s							
during a field authentication attemp? Not mentioned is that the outliability of an authenticator may Replace "including bases" with "including availability." ### A proofing agent is also making a determination of the linkage of the claimed identity to the paginant for the claimed identity of the paginant for the paginant for the claimed identity of the paginant for the paginant fo							
Replace 'Including blased' with 'Including availability' 1 a proprieting agest to some storage agest as also making adetermination of the inlarge of the claimed identity to the applicant in similarly. Sec. 2.5.11, then the agent should also be trained to detect deception and signs of social regimenting; similarly. Sec. 3.1.21, incrept profine agents to detect deception and signs of social regimenting; similarly. Sec. 3.1.21, incrept profine agents to detect deception and signs of social regimenting. Signal 2.1.2 7, 555.558 regiment them to be trained to detect deception and for such detects. Girch the regiment is not sense as a such asu							
fa proofing agent is also making a determination of the linkage of the claimed identity to the applicant (Sec 2.5.1), then the agent hand also be trained to detect deception and flag suspected events, which means their frault craiming should be more compatible with trusted reason and (Sec 2.5.1). The proofing agent to detect deception and fraud. 2.12 7535558 requires them to be trained only, not remove and (Sec 4.1.7) Experimental to the string should be more considerable with trusted referee and (Sec 4.1.7) Experimental to the string should be not considerable with trusted referee and (Sec 4.1.7) Experimental to the string should be considerable and (Sec 4.1.7) Experimental to the string should be considerable with the string should be not set the string should be removed that the should be afficially to return a confirmation of the string should be acceptable for full, as that level of susmeriment of Supprice evidence, release the securities of evidence to prove that the applicant is more than likely than not the claimed identity at ILA 20 rILA; it could be acceptable for full, as that level of susmeriment on Coale in one strange cough price continues of the subject participate in an onsite attended enrollment		504					
Sec 2.5.1, then he agent should also be trained to detect deception and signs of section and signs used events, similarly, Sec. 3.1.2.1 gentle profiling agent to detect deception and figs suspected events, which means their fraud training should be more compatible with fusused referees and (Sec. 4.1.7) Sec. 3.1.2.1 gentle better to be trained to detect deception and figs. 4.1.2 (Sec. 3.1.2) and the section of deep size that cold and the cold section for the considerable with the section of th	-	63A	3	23	964-96		, ,
similarly, (Sec. 3.1.2.1) requires proofing agent to detect indication of fraul and flag suspected events, which means their fraud training should be more compatible with the referees and flex. 4.1.77 (sys-5580 requires them to be trained to detect deception and fraud. The reference of designation to be trained to detect deception and fraud. Experiment should be onsite attended only, not remote attended, for superior evidence. Given the rise of designation to be trained to detect deception and fraud. Experiment should be onsite attended only, not remote attended, for superior evidence, Given the rise of designation and socially only of the control of the proofing agent to runted referee to designation and social to the proofing agent to runted referee to the evidence in the proofing agent to runted referee to the proofing agent to runted referee to designation and social to the proofing agent to runted referee to designation and social to the proofing agent to runted referee to designation and social to a superior evidence, reference to prove that the applicant is more than likely than not the claimed identity at IA.2 or IA.3.1 (and be acceptable for IA.1 as that level of social control and social to the proofing agent to the proofing agent to trusted referee and flex. The proofing agent to trusted referee the evidence is physical? The issuing source had the subject participate in an onsite attended enrollment" The issuing source had the subject participate in an onsite attended enrollment							
which means their fraud training should be more compatible with trusted referees and fisc. 4.1.7) 7 555-558 (register bitm to be trained to detect deception and fraud. 7 555-558 (register bitm to be trained to detect deception and fraud. 8 2 4.1.3 (12 72-72) and how easy it is for bad actors to impensate their victims and socially engineer line service desk workers, superior evidence, should only be given to those people who must to see of desplate technology and how easy it is for bad actors to impensate their victims and socially engineer line service desk workers, superior evidence should only be given to those people who must to service desk workers, superior evidence should only be given to those people who must should not be considered expected. 8 2 4.1.3 (12 72-72) be difficult to reproduce regardless of vehether it is physical or not. While there is show a cryptographic requirement for Superior devidence, etc. and the subject participate in an onsite attended enrollment" 8 2 4.1.3 (12 72-72) be difficult to reproduce regardless of vehether it is physical or not. While there is show a cryptographic requirement for Superior should on the need that reproductions should an expension of the subject participate in an onsite attended enrollment" 8 3 4 2.1.3 (12 72-72) be difficult to reproduce regardless of vehether it is physical or not. While there is show a cryptographic requirement for Superior should an expension of the subject participate in an onsite attended enrollment" 8 4 2.1.3 (12 72-72) be difficult to reproduce regardless of whether it is physical or not. While there is show a cryptographic requirement for superior should an expension of the subject participate in an onsite attended enrollment							
GSA 2.1.2 7 555-558 requires them to be trained to detect deception and fraud.							
Forvillment should be onsite attended only, not remote attended, for superior evidence. Given the rise of depetate technology and how asys it is for bad actors to its for bad actors to rise for bad bad socially enjineer live service desk workers, superior evidence, related only by given to those people who must relate the evidence (e.g., DMP, PV) office, etc.) 1 2 720-721, go onate to Obtain the evidence (e.g., DMP, PV) office, etc.) 1 2 720-722, by onate to Obtain the evidence (e.g., DMP, PV) office, etc.) 2 3 2 729-720, be difficult repardless of whether it is physical or not. While there is shown a cryptographic or evidence, relating the need that reproduction should be acceptable for high and the claimed identity at IAL2 or IAL3; account to a comparison of the publicant is more than likely than not the claimed identity at IAL2 or IAL3; account to a comparison of the publicant is more than likely than not the claimed identity at IAL2 or IAL3; actor or more "method, this evidence alone should not be considered enough to verify the linkage of the applicant to evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect potential fraud, ask the applicant is flaud, ask the applicant is flaud ask the applicant is a considered enough in social engineering to							
of deeptake technology and how easy it is for bad actors to impersonate their victims and socially engineer lives existing source desk workers, superior evidence should be giben to those people who must represent the evidence desk workers superior evidence should be giben to those people who must be difficult to reproduce regardless of whether it is physical or not. While there is also a cryptographic requirement for Superior evidence, relievating the need that reproduction should a 12 729-730 be difficult regardless of redential type is not too repetitive. The ability to return a confirmation code is not a strong enough piece of evidence to prove that the applicant is more than likely than not the claimed identity. Or IAL1, as that level of assurance is considerably weaker. Because the section requires "one or more" method, this evidence alone should not be considered enough to verify the linkage of the applicant to exhaust facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect potential fraud, as the applicant store to exhaust ending and the ability to biometrically compare the photographic evidence, a supplicant fiscal movements to detect possible fraudient activities. This would not be available in unattended sessions, and whom the ability to biometrically compare the photographic evidence, a supplicant fiscal image comparison. The trusted referee fee comment above on necessity of social engineering training of the proofing agent from this section. 13.1 293.085-981 the more of the internal control of a CPI horing an assessment should be made available to any and all RPs that are customers, proteinal extensions and associated militage to supplications provided and associated militage comparison. The trusted referee fee comment above on necessity of social engineering training of the proofing agent from this section. 13.1 33.1 33.1 33.1 33.1 33.1 33.1 3		63A	2.1.2	7	555-55	8 requires them to be trained to detect deception and fraud.	Either increase the level of training of the proofing agent or change Sec. 2.5.1, pg. 14, line 799-808, from proofing agent to trusted referee.
engineer live service desk workers, superior evidence should only be given to those people who must 12 720-720; go norste to obtain the evidence (e.g., DM, PV) office, e.g., DM, PV) office, e.g., DM, PV office, e.g., DM						Enrollment should be onsite attended only, not remote attended, for superior evidence. Given the rise	
SaA 2.4.13 12 720-723, go notise to obtain the evidence (e.g., DMV, PW Chife, etc.) The evidence should be difficult reproduce regardless of whether it is physical or not. While there is also a cryptographic requirement for Superior evidence, reterating the evidence should be difficult requirement for Superior evidence, reterating the evidence should be difficult requirement for Superior evidence, reterating the evidence should be difficult requirement for Superior evidence, reterating the evidence to prove that the policiant is more than likely than not the claimed indentity of evidence to prove that the applicant to more whether the should be acceptable for NA.1, as that level of assurance is considerably weaker. Because the section requires "one or more" method, this evidence alone should not be considered enough to verify the linkage of the applicant to more enough in social engineering to be able to detect possible fraudulent activities. This would not be available in unattended essissions, and without the ability to biometrical fland, ask the ability to accompliate value of the applicant to a						of deepfake technology and how easy it is for bad actors to impersonate their victims and socially	
The evidence should be difficult to reproduce regardless of whether it is physical or not. While there is also a cytograph crequirement for Superior evidence freelesting the need that reproduction should also a cytographic requirement for Superior evidence for Sup						engineer live service desk workers, superior evidence should only be given to those people who must	
The evidence should be difficult to reproduce regardless of whether it is physical or not. While there is also a cryotographic requirement for Superior evidence for Superior ev		63A	2.4.1.3	12	720-72	go onsite to obtain the evidence (e.g., DMV, PIV office, etc.)	"The issuing source had the subject participate in an onsite attended enrollment"
also a cryptographic requirement for Superior evidence, reliterating the need that repoduction should 2793-730 be difficult regardless of credental type is not to expetitive 18							
Facility to repart each of the continue of the size of the continue of the conti							
the ability to return a confirmation code is not a strong enough piece of evidence to prove that the applicant is more than likely than not the calinethity at IAL2 or IAL3; it could be acceptable for IAL1, as that level of assurance is considerably weaker. Because the section requires "one or more" method, this evidence alone should not be considered enough to verify the linkage of the applicant to method, this evidence alone should not be considered enough to verify the linkage of the applicant to the devidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect potential fraging to be able to trained able to the potential value fraging to be able to trained able		634	2 / 1 3	12	729-73		Remove "If the evidence is physical"
applicant is more than likely than not the claimed identity at IAL2 or IAL3; it could be acceptable for IAL1, as that level of assurance is considerably weaker. Because the section requires "one or more" method, this evidence alone should not be considered enough to verify the linkage of the applicant to Remove these lines A visual facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions, only). Proofing agents need to be trained enough in social engineering to be able to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a policy applicant facial imovements to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a remove thread sessions, and without the ability to biometrically compare the photographic evidence, a remove thread sessions, and without the ability to biometrically compare the photographic evidence, a remove thread sessions, and without the ability to biometrically compare the photographic evidence, a remove thread sessions, and without the ability to biometrically compare the photographic evidence, a remove thread sessions, and observe the applicant to unattended sessions, and without the ability to biometrically compare the photographic evidence, a remove thread sessions, and observe the applicant to unattended sessions, and without the ability to compare the photographic evidence, a remove thread sessions, and observe the applicant to the applicant to a session of the proofing agent to remove proofing agent form this section is unattended. Bemove these lines Remove these lines		03A	2.4.1.3	- 12	125 /5		nemove in the evidence is physical
Al.1, as that level of assurance is considerably weaker. Because the section requires "one or more" method, this evidence alone should not be considered enough to verify the linkage of the applicant to the defect of the identity of the							
method, this evidence alone should not be considered enough to verify the linkage of the applicant to A visual facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect potential fraud, ask the applicant questions, and observe the applicants facial movements to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a regimenting to be able to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a regimenting to be able to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a regimenting to be able to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a regimenting to determine the photographic evidence, a regimenting to determine the photographic evidence, a regimenting to regiment and provided in the applicant of the proofing agent in section 7.12 or remove proofing agent from this section. While the results of an equity assessment should be made available to any and all RPs that are customers of a CSP, having an assessment and associated mitigations publicly suggest limiting the availability to RPs When not validated, the passport is on par with a driver's license (Sec. 42.4). Keep the passport in a fact a regiment of the proofing agent in section 2.1.2 or remove proofing agent from this section. The shall statement begins with "when setting allows for it, suggest removing that and changing the change shall to should, remove "when the setting allows for itevents)" "assessed and certified" means a trai							
A visual facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect optomital fraud, ask the applicant questions, and observe the applicants facial movements to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a 63A 2.5.1 14 799-808 deep fake could easily pass a produce after capture. 63A 3.2.11 18 936-938 The amount of training required in this section is more than required in 2.1.2 Either increase the level of training of the proofing agent in section 2.1.2 or remove proofing agent from this section. While the results of an equity assessment and associated mitigations publicly could invite bad actors to find the ability to commit fraud against the CSPs. 63A 3.1.4 23 1085-18 available could invite bad actors to find the ability to commit fraud against the CSPs. 63A A 2 Table 5 78 2728 SUPENIOR only when NFC chip is read. 63A 3.1.12 31 1336-13 1315-13 and 1325-13 entire statement to should. Reads onger that way. 63A 3.1.12 31 1336-13 have to spend additional money for certification bodies to certify employees. 63A 3.1.12 31 1336-13 have to spend additional money for certification bodies to certify employees.							
A visual facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect possible fraud, ask the applicants facial image enterprises. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a applicants facial image and applicants facial image comparison. The (trusted referee (see comment above on necessity of social engineering training fit is the proof of the proofing agent in section 2.1.2 are seen to should be made available to any and all RPs that are customers? Potential customers for potential customers assessment and associated mitigations publicly available could invite bad actors to find the ability to commit fraud against the CSPs. When not validated, the passport is on par with a driver's license (Sec. 4.2.4). Keep the passport in Add Passport to "STRONG", when only visual inspection is used. The shall statement begins with "when setting allows for it", suggest removing that and changing the statement to should. Rest tonger that way. assessed and certified" means a training and a certificate, of which there is none for proofing agents from the setting allows for itevents)" Add Passport to "STRONG", when only visual inspection is used. The shall statement begins with "when setting allows for it", suggest removing that and changing the change shall to should; remove "when the setting allows for itevents)" assessed and certified" means a training and a certificate, of which there is none for proofing agents/frusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/frusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/frusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/frusted referees today. This requirement puts undue burden on the CSPs and RPs, who					.		l
evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a applicants facial movements to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a unattended sessions, and without the ability to biometrically compare the photographic evidence, a deep fake could easily pass a proofing agent who reviews the evidence after capture. 63A 3.2.1.1 18 936-938 The amount of training required in this section is more than required in 2.1.2 Either increase the level of training of the proofing agent in section 2.1.2 or remove proofing agent from this section. While the results of an equity assessment should be made available to any and all RPs that are customers / potential customers of a CSP, having an assessment and associated mitigations publicly sailable could invite back tost to find the ability to commit fraud against the CSPs. When not validated, the passport is on par with a driver's license (Sec. 4.2.4). Keep the passport in Suggest limiting the availability to RPs When not validated, the passport is on par with a driver's license (Sec. 4.2.4). Keep the passport in The shall statement begins with "when setting allows for it", suggest removing that and changing the change shall to should; remove "when the setting allows for itevents)" 63A 3.1.12 30 1325-13 entire statement to should. Reads stronger that way. agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents and certified with at least annual evaluations"		63A	2.5.1	14	784-78	36 the identity	Remove these lines
evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a applicants facial movements to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a unattended sessions, and without the ability to biometrically compare the photographic evidence, a deep fake could easily pass a proofing agent who reviews the evidence after capture. 63A 3.2.1.1 18 936-938 The amount of training required in this section is more than required in 2.1.2 Either increase the level of training of the proofing agent in section 2.1.2 or remove proofing agent from this section. While the results of an equity assessment should be made available to any and all RPs that are customers / potential customers of a CSP, having an assessment and associated mitigations publicly sailable could invite back tost to find the ability to commit fraud against the CSPs. When not validated, the passport is on par with a driver's license (Sec. 4.2.4). Keep the passport in Suggest limiting the availability to RPs When not validated, the passport is on par with a driver's license (Sec. 4.2.4). Keep the passport in The shall statement begins with "when setting allows for it", suggest removing that and changing the change shall to should; remove "when the setting allows for itevents)" 63A 3.1.12 30 1325-13 entire statement to should. Reads stronger that way. agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents and certified with at least annual evaluations"					1		
engineering to be able to detect potential fraud, ask the applicant questions, and observe the applicants facial movements to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a unattended sessions, and without the ability to biometrically compare the photographic evidence, a least of the photographic evidence, and so the proposition of the proof of the					1		
applicants facial movements to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a 14 799-808 deep fake could easily so a proofing agent who reviews the evidence after capture. 63A 2.5.1 18 936-938 The amount of training required in this section is more than required in 2.1.2 Either increase the level of training of the proofing agent in section 2.1.2 or remove proofing agent from this section. While the results of an equity assessment should be made available to any and all RPs that are customers / potential customers of a CSP, having an assessment and associated mitigations publicly solved in the ability to commit fraud against the CSPs. When not validated, the passport is on par with a driver's license (Sec. 4.2.4). Keep the passport in 16 Add Passport to "STRONG", when only visual inspection is used. The shall statement begins with "when setting allows for it", suggest removing that and changing the 16 agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will 6 assessed and certified with at least annual evaluations"					1	evidence (so for attended sessions only). Proofing agents need to be trained enough in social	
unattended sessions, and without the ability to biometrically compare the photographic evidence, a 63A 2.5.1 14 799-808 deep fake could easily pass a proofing agent who reviews the evidence after capture. 63A 3.2.1.1 18 936-938 The amount of training required in this section is more than required in 2.1.2 While the results of an equity assessment should be made available to any and all RPs that are customers / potential customers of a CSP, having an assessment and associated mitigations publicly 63A 3.1.4 23 1085-18 available could invite ballity to commit fraud against the CSPs. When not validated, the passport is on par with a driver's license (Sec. 4.2.4). Keep the passport in 63A A.2 Table 5 78 2728 SUPFRIOR only when NFC chip is read. The shall statement begins with "when setting allows for it", suggest removing that and changing the entire statement to should. Reads stronger that way. 63A 3.1.12 31 1336-13 have to spend additional money for certification bodies to certify employees. Remote (Attended) visual facial image comparison. The (trusted referee (see comment above on necessity of social engineering training fe Either increase the level of training of the proofing agent in section 2.1.2 or remove proofing agent from this section. Suggest limiting the availability to RPs Add Passport to "STRONG", when only visual inspection is used. Add Passport to "STRONG", when only visual inspection is used. Change shall to should; remove "when the setting allows for itevents)" **Comment of the proofing agent from this section 2.1.2 or remove proofing agent from this section. Suggest limiting the availability to RPs Add Passport to "STRONG", when only visual inspection is used. Change shall to should; remove "when the setting allows for itevents)" **Comment of the proofing agent in section 2.1.2 or remove proofing agent from this section. **Comment of the proofing agent in section 2.1.2 or remove proofing agent in section 2.1.2 or remove proofing agent in section 2.1.2 or remove proofing agent					1	engineering to be able to detect potential fraud, ask the applicant questions, and observe the	
unattended sessions, and without the ability to biometrically compare the photographic evidence, a 63A 2.5.1 14 799-808 deep fake could easily pass a proofing agent who reviews the evidence after capture. 63A 3.2.1.1 18 936-938 The amount of training required in this section is more than required in 2.1.2 While the results of an equity assessment should be made available to any and all RPs that are customers / potential customers of a CSP, having an assessment and associated mitigations publicly 63A 3.1.4 23 1085-18 available could invite ballity to commit fraud against the CSPs. When not validated, the passport is on par with a driver's license (Sec. 4.2.4). Keep the passport in 63A A.2 Table 5 78 2728 SUPFRIOR only when NFC chip is read. The shall statement begins with "when setting allows for it", suggest removing that and changing the entire statement to should. Reads stronger that way. 63A 3.1.12 31 1336-13 have to spend additional money for certification bodies to certify employees. Remote (Attended) visual facial image comparison. The (trusted referee (see comment above on necessity of social engineering training fe Either increase the level of training of the proofing agent in section 2.1.2 or remove proofing agent from this section. Suggest limiting the availability to RPs Add Passport to "STRONG", when only visual inspection is used. Add Passport to "STRONG", when only visual inspection is used. Change shall to should; remove "when the setting allows for itevents)" **Comment of the proofing agent from this section 2.1.2 or remove proofing agent from this section. Suggest limiting the availability to RPs Add Passport to "STRONG", when only visual inspection is used. Change shall to should; remove "when the setting allows for itevents)" **Comment of the proofing agent in section 2.1.2 or remove proofing agent from this section. **Comment of the proofing agent in section 2.1.2 or remove proofing agent in section 2.1.2 or remove proofing agent in section 2.1.2 or remove proofing agent					1	applicants facial movements to detect possible fraudulent activities. This would not be available in	
63A 2.5.1 14 799-808 deep fake could easily pass a proofing agent who reviews the evidence after capture. "Remote (Attended) visual facial image comparison. The (trusted referee (see comment above on necessity of social engineering training facility facility for this section is more than required in 2.1.2 Either increase the level of training of the proofing agent in section 2.1.2 or remove proofing agent from this section. While the results of an eavailable to any and all RPs that are customers / potential customers of a CSP, having an assessment and associated mitigations publicly 3.1.4 23 1085-18 available could invite bad actors to find the ability to commit fraud against the CSPs. When not validated, the passport is on par with a driver's license (Sec. 4.2.4). Keep the passport in 63A A.2 Table 5 78 2728 SUPERIOR only when NFC chip is read. The shall statement begins with "when setting allows for it", suggest removing that and changing the 63A 3.1.12 30 1325-13 entire statement to should. Reads stronger that way. "assessed and certified" means a training and a certificate, of which there is none for proofing agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will 63A 3.1.12 31 1336-13 have to spend additional money for certification bodies to certify employees. Remove "and be assessed and certified with at least annual evaluations"						unattended sessions, and without the ability to biometrically compare the photographic evidence, a	
63A 3.2.1.1 18 936-938 The amount of training required in this section is more than required in 2.1.2 Either increase the level of training of the proofing agent in section 2.1.2 or remove proofing agent from this section. While the results of an equity assessment should be made available to any and all RPs that are customers / potential customers of a CSP, having an assessment and associated mitigations publicly sold in the shall state the case of the proofing agent in section 2.1.2 or remove proofing agent from this section. While the results of an equity assessment should be made available to any and all RPs that are customers / potential customers of a CSP, having an assessment and associated mitigations publicly sold according to the proofing agent in section 2.1.2 or remove proofing agent from this section. While the results of an equity assessment should be made available to any and all RPs that are customers / potential customers of a CSP, having an assessment and associated mitigations publicly Suggest limiting the availability to RPs When not validated, the passport is on par with a driver's license (Sec. 4.2.4). Keep the passport in The shall statement begins with "when setting allows for it", suggest removing that and changing the sagessed and certified means a training and a certificate, of which there is none for proofing agent from this section. Add Passport to "STRONG", when only visual inspection is used. Add Passport to "STRONG", when only visual inspection is used. Change shall to should; remove "when the setting allows for itevents)" "assessed and certified means a training and a certificate, of which there is none for proofing agent from this section. Bither increase the level of training of the proofing agent from this section. Add Passport to "STRONG", when only visual inspection is used. Change shall to should; remove "when the setting allows for itevents)" "assessed and certified means a training and a certificate, of which there is none for proofing agent from this		63A	251	14	799-80		"Remote (Attended) visual facial image comparison. The (trusted referee (see comment above on necessity of social engineering training fr
While the results of an equity assessment should be made available to any and all RPs that are customers / potential customers of a CSP, having an assessment and associated mitigations publicly 63A 3.1.4 23 1085-18 available to could invite abd actors to find the ability to commit fraud against the CSPs. When not validated, the passport is on par with a driver's license (Sec. 4.2.4). Keep the passport in Add Passport to "STRONG", when only visual inspection is used. The shall statement begins with "when setting allows for it", suggest removing that and changing the entire statement to should. Reads stronger that way. "assessed and certified" means a training and a certificate, of which there is none for proofing agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will Remove "and be assessed and certified with at least annual evaluations"							
customers / potential customers of a CSP, having an assessment and associated mitigations publicly 3.1.4 23 1085-18 available could invite bad actors to find the ability to commit fraud against the CSPs. When not validated, the passport is on par with a driver's license (Sec. 4.2.4). Keep the passport in When not validated, the passport is on par with a driver's license (Sec. 4.2.4). Keep the passport in Add Passport to "STRONG", when only visual inspection is used. The shall statement begins with "when setting allows for it", suggest removing that and changing the 3.1.12 30 1325-13 entire statement to should. Reads stronger that way. "assessed and certified" means a training and a certificate, of which there is none for proofing agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will 63A 3.1.12 31 1336-13 have to spend additional money for certification bodies to certify employees. Remove "and be assessed and certified with at least annual evaluations"	h	03/1	J.E.I.I.I	10	, 550 50		enter increase the lever of training of the proofing agent in section 2.2.2 of remove proofing agent from this section.
63A 3.1.4 23 1085-18 available could invite bad actors to find the ability to commit fraud against the CSPs. Suggest limiting the availability to RPS When not validated, the passport is on par with a driver's license (Sec. 4.2.4). Keep the passport in Add Passport to "STRONG", when only visual inspection is used. The shall statement begins with "when setting allows for it", suggest removing that and changing the safe and passport to "STRONG", when only visual inspection is used. The shall statement to should. Reads stronger that way. assessed and certified" means a training and a certificate, of which there is none for proofing agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will 63A 3.1.12 31 1336-13 have to spend additional money for certification bodies to certify employees. Remove "and be assessed and certified with at least annual evaluations"					1		
When not validated, the passport is on par with a driver's license (Sec. 4.2.4). Keep the passport in Add Passport to "STRONG", when only visual inspection is used. The shall statement begins with "when setting allows for it", suggest removing that and changing the 3.1.12 30 1325-13 entire statement to should. Reads stronger that way. "assessed and certified" means a training and a certificate, of which there is none for proofing agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will 63A 3.1.12 31 1336-13 have to spend additional money for certification bodies to certify employees. Remove "and be assessed and certified with at least annual evaluations"		634	2.4.4		1,005		Course de limitaire a de a considerativa de PD
63A A.2 Table 5 78 2728 SUPERIOR only when NFC chip is read. The shall statement begins with "when setting allows for it", suggest removing that and changing the active statement to should. Reads stronger that way. 63A 3.1.12 30 1325-13 entire statement to should. Reads stronger that way. 83Sessed and certified" means a training and a certificate, of which there is none for proofing agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will applied to accompany to a company to	 	DOM	3.1.4	23	1085-1		Suggest inniting the availability to RPS
The shall statement begins with "when setting allows for it", suggest removing that and changing the change shall to should; remove "when the setting allows for itevents)" Sassessed and certified" means a training and a certificate, of which there is none for proofing agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will 63A 3.1.12 31 1336-13 have to spend additional money for certification bodies to certify employees. Remove "and be assessed and certified with at least annual evaluations"					1		1
63A 3.1.12 30 1325-13 entire statement to should. Reads stronger that way. change shall to should; remove "when the setting allows for itevents)" "assessed and certificat" means a training and a certificate, of which there is none for proofing agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will 63A 3.1.12 31 1336-13 have to spend additional money for certification bodies to certify employees. Remove "and be assessed and certified with at least annual evaluations"		63A	A.2 Table 5	78	272		Add Passport to "STRONG", when only visual inspection is used.
"assessed and certified" means a training and a certificate, of which there is none for proofing agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will 63A 3.1.12 31 1336-13 have to spend additional money for certification bodies to certify employees. Remove "and be assessed and certified with at least annual evaluations"					1		
agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will 63A 3.1.12 31 1336-13 have to spend additional money for certification bodies to certify employees. Remove "and be assessed and certified with at least annual evaluations"		63A	3.1.12	30	1325-1		change shall to should; remove "when the setting allows for itevents)"
63A 3.1.12 31 1336-13 have to spend additional money for certification bodies to certify employees. Remove "and be assessed and certified with at least annual evaluations"	1			1	1	"assessed and certified" means a training and a certificate, of which there is none for proofing	
	1				1	agents/trusted referees today. This requirement puts undue burden on the CSPs and RPs, who will	
63A 3.1.13.1 31 1358 This language implies that entire categories of individuals will find identity proofing challenging. Change "such individuals and demographic groups includes:" to "such individuals may include"	1 1	63A	3.1.12	31	1336-1	l have to spend additional money for certification bodies to certify employees.	Remove "and be assessed and certified with at least annual evaluations"
		63A	3.1.13.1	31	135	8 This language implies that entire categories of individuals will find identity proofing challenging.	Change "such individuals and demographic groups includes:" to "such individuals may include"

					The service of the se	
63.		3.1.13.1	31	12	Individuals with no access to online services to not need to be identity proofed since they will not be identity proofed since they will not be	Change "individuals with little or no access to online services" to "individuals with limited access to online services"
63.	SA .	3.1.13.1	31	. 13	"train and certify" - means a training and a certificate, of which there is none for trusted referees	Change individuals with little or no access to online services to individuals with limited access to online services
					today. This requirement puts undue burden on the CSPs and RPs, who will have to spend additional	
63.	tΔ	3.1.13.1	32	13	8 money for certification bodies to certify employees.	Remove "and certify"
03.	<i>I</i> A	5.1.15.1	32	15	money for certification bodies to certify employees.	nemove and certary
					"annual recertification of the trusted referee's capabilities" - means a training and a certificate, of	
					which there is none for trusted referees today. This requirement puts undue burden on the CSPs and	
63.	BA	3.1.13.1	32	13	9 RPs, who will have to spend additional money for certification bodies to certify employees.	Remove "annual recertification of the trusted referee's capabilities"
05.	,,,	5.1.15.1		1 10	Jan 3, who was not to spend additional money for certained to a bodies to certain employees.	The state of the s
					A visual facial image comparison should only be conducted at the time the person presents the	
					evidence (so for attended sessions only). Proofing agents need to be trained enough in social	
					engineering to be able to detect potential fraud, ask the applicant questions, and observe the	
					applicants facial movements to detect possible fraudulent activities. This would not be available in	
					unattended sessions, and without the ability to biometrically compare the photographic evidence, a	
63.	3A	4.1.6	37	1561-	15 deep fake could easily pass a proofing agent who reviews the evidence after capture.	Remove "or an asynchronous process (i.e., visual comparison made by a proofing agent at a different time)"
					While we agree that anyone who is overseeing the video sessions should have extensive fraud training,	
					but we are now unsure what the actual difference between a proofing agent and a trusted referee is,	
63.	BA	4.1.7	38	1576-	15 considering they need the same amount of fraud training	Review the other comments on proofing agents/trusted referees; think about removing proofing agents from the guidelines altoge
63.	BA	4.1.7	38	15	0 typographical error	"records the session"
					While we agree that anyone who is overseeing the onsite sessions should have extensive fraud	
					training, but we are now unsure what the actual difference between a proofing agent and a trusted	
63.	BA	4.1.8	39	1600-	1.6 referee is, considering they need the same amount of fraud training	Review the other comments on proofing agents/trusted referees; think about removing proofing agents from the guidelines altoge
63.	3A	4.1.10	40	16	7 typographical error	"Return of a confirmation"
						Either require biometrics for IAL2 or split IAL2 so that the use of biometrics during identity proofing is clearly captured and transmit
						to all RPs so they can make a decision on its use or absence, and make sure the pathways are clearly marked such as IAL2-B (biomet
						and IAL2-O (other). These two pathways are not equivalent from a security and fraud-deterrence perspective. The non-biometric
						pathway is highly vulnerable to attack by family members, caregivers, and acquaintances, which can lead to devastating financial a
						consequences for disabled beneficiaries and the elderly who rely on their benefits. Capturing the facial image of the individual who
						applying for benefits is a strong deterrent to impersonation, particularly for individuals who are personally acquainted with a victim
					Biometrics improve security. Requiring the capture of a facial image during identity proofing is a	There is no equivalent deterrent in the non-biometric pathway. Individuals with common names are also highly vulnerable to attack
					powerful deterrent for community and family-level bad actors. If biometrics are optional at IAL2 then	when address verification is used for proofing without sufficient additional controls. Records may show that a number, email addre
					an agency that requires biometrics for security reasons will not be able to accept an IAL2 credential	home address is strongly associated with a James Smith, for example. There are 38,313 James Smith's in the United States. This is a
					that was established by an agency with a higher risk tolerance. This breaks the consistency and trust	common attack that is happening at scale today. https://www.statista.com/statistics/279713/frequent-combinations-of-first-and-la
63.	BA	4.2	40	16	8 that enables federation.	name-in-the-us/
					These options DO have different security and assurance outcomes, which effectively waters down the	Acknowledge that these pathways are not equivalent from a security and assurance perspective and rank them, perhaps: IAL2-High
					security of IAL2 to the least security option. Also, digital evidence will either be part of the biometric or	(biometrics), IAL2-Moderate (non-biometrics), IAL-low(?).
					non-biometric pathway. Why create a third pathway just for digital evidence? Wouldn't it really need	Otherwise, trust and interoperability and therefore the ability to leverage federated credentials will break - an agency that requires
63.	3A	4.2	40	1649-	6 to be four pathways in that case? Digital non-biometric and digital biometric?	Otherwise, trust and interoperability and therefore the ability to leverage federated credentials will break - an agency that requires with biometrics will not be able to accept an IAL2 credential that originated with another agency.
63.	\$A	4.2	40	1649-	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-	
03.					6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on	with biometrics will not be able to accept an IAL2 credential that originated with another agency.
63. 63.		4.2 4.2.6.1			6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-	
03				1716-	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on	with biometrics will not be able to accept an IAL2 credential that originated with another agency.
03.				1716-	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on 17 a STRONG or SUPERIOR piece of evidence is required.	with biometrics will not be able to accept an IAL2 credential that originated with another agency.
03.				1716- 1720- 1724	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on 17 a STRONG or SUPERIOR piece of evidence is required.	with biometrics will not be able to accept an IAL2 credential that originated with another agency.
63.	SA.	4.2.6.1	42	1716- 1720- 1724- 1730-	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on 7 a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence
03.	SA.		42	1716- 1720- 1724	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on 17 a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading.	with biometrics will not be able to accept an IAL2 credential that originated with another agency.
63.	SA.	4.2.6.1	42	1716- 1720- 1724- 1730-	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on 17 a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP.	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence
63.	SA.	4.2.6.1	42	1716- 1720- 1724- 1730-	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence
63.	iA	4.2.6.1	42	1720- 1724- 1730- 1734- 1734-	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While this could prevent unknown bad actors from committing fraud, it does not prevent family members or	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence Add a sentence that indicates that these are not equivalent in terms of fraud prevention.
63.	iA	4.2.6.1	42	1720- 1724- 1730- 1734- 1734-	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence
63.	iA	4.2.6.1	42	1720- 1724- 1730- 1734- 1734-	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While this could prevent unknown bad actors from committing fraud, it does not prevent family members or close friends from committing fraud.	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence Add a sentence that indicates that these are not equivalent in terms of fraud prevention.
63.	iA	4.2.6.1	42	1720- 1724- 1730- 1734- 1734-	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While this could prevent unknown bad actors from committing fraud, it does not prevent family members or 17 close friends from committing fraud. A visual facial image comparison should only be conducted at the time the person presents the	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence Add a sentence that indicates that these are not equivalent in terms of fraud prevention.
63.	iA	4.2.6.1	42	1720- 1724- 1730- 1734- 1734-	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on 17 a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While this could prevent unknown bad actors from committing fraud, it does not prevent family members or 17 close friends from committing fraud. A visual facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions only). Proofing agents need to be trained enough in social	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence Add a sentence that indicates that these are not equivalent in terms of fraud prevention.
63.	iA	4.2.6.1	42	1720- 1724- 1730- 1734- 1734-	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While this could prevent unknown bad actors from committing fraud, it does not prevent family members or 7 close friends from committing fraud. A visual facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect potential fraud, ask the applicant questions, and observe the	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence Add a sentence that indicates that these are not equivalent in terms of fraud prevention.
63.	iA	4.2.6.1	42	1720- 1724- 1730- 1734- 1734-	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While this could prevent unknown bad actors from committing fraud, it does not prevent family members or 17 close friends from committing fraud. A visual facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect potential fraud, ask the applicant questions, and observe the applicants facial movements to detect possible fraudulent activities. This would not be available in	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence Add a sentence that indicates that these are not equivalent in terms of fraud prevention.
63.	iA	4.2.6.1 4.2.6.1	42	1720- 1724- 1730- 1734- 1734- 1734-	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on 17 a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While this could prevent unknown bad actors from committing fraud, it does not prevent family members or 17 close friends from committing fraud. A visual facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect potential fraud, ask the applicant questions, and observe the applicants facial movements to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence Add a sentence that indicates that these are not equivalent in terms of fraud prevention. Remove the requirement for STRONG/SUPERIOR evidence
63.	iA	4.2.6.1	42	1720- 1724- 1730- 1734- 1734- 1734-	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While this could prevent unknown bad actors from committing fraud, it does not prevent family members or 7 close friends from committing fraud. A visual facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect potential fraud, ask the applicant questions, and observe the applicants facial movements to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a 17 deep fake could easily pass a proofing agent who reviews the evidence after capture.	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence Add a sentence that indicates that these are not equivalent in terms of fraud prevention.
63.	iA	4.2.6.1 4.2.6.1	42	1720- 1724- 1730- 1734- 1734- 1734-	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While this could prevent unknown bad actors from committing fraud, it does not prevent family members or 17 close friends from committing fraud. A visual facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect potential fraud, ask the applicant questions, and observe the applicants facial movements to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a 7 deep fake could easily pass a proofing agent who reviews the evidence after capture. What is meant by a 'validated account'? Does it need to be an account owned by someone with the	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence Add a sentence that indicates that these are not equivalent in terms of fraud prevention. Remove the requirement for STRONG/SUPERIOR evidence
63.	iA	4.2.6.1 4.2.6.1	42	1720- 1724- 1730- 1734- 1734- 1734-	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on 17 a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While this could prevent unknown bad actors from committing fraud, it does not prevent family members or 17 close friends from committing fraud. A visual facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect potential fraud, ask the applicant questions, and observe the applicants facial movements to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a 17 deep fake could easily pass a proofing agent who reviews the evidence after capture. What is meant by a 'Validated account'? Does it need to be an account owned by someone with the same name? That is not sufficiently granular for someone with a common name. Does it need to be an	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence Add a sentence that indicates that these are not equivalent in terms of fraud prevention. Remove the requirement for STRONG/SUPERIOR evidence
63.	iA	4.2.6.1 4.2.6.1	42	1720- 1724- 1730- 1734- 1734- 1734-	FAIR evidence doesn't require facial images, and therefore should not require biometric or non- biometric methods to verify the evidence. However, a verification method to match the facial image on 3 STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While this could prevent unknown bad actors from committing fraud, it does not prevent family members or close friends from committing fraud. A visual facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect potential fraud, ask the applicant questions, and observe the applicants facial movements to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a deep fake could easily pass a proofing agent who reviews the evidence after capture. What is meant by a 'Validated account'? Does it need to be an account owned by someone with the same name? That is not sufficiently granular for someone with a common name. Does it need to be an account associated with someone's name and SSN? Does length of ownership matter? Note:	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence Add a sentence that indicates that these are not equivalent in terms of fraud prevention. Remove the requirement for STRONG/SUPERIOR evidence
63.	iA iA	4.2.6.1 4.2.6.1 4.2.6.1	42 42 42	1716- 1720- 1724- 1730- 1734- 1734- 1727-	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While this could prevent unknown bad actors from committing fraud, it does not prevent family members or 17 close friends from committing fraud. A visual facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect potential fraud, ask the applicant questions, and observe the applicants facial movements to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a 17 deep fake could easily pass a proofing agent who reviews the evidence after capture. What is meant by a 'validated account'? Does it need to be an account owned by someone with the same name? That is not sufficiently granular for someone with a common name. Does it need to be an account associated with someone's name and SSN? Does length of ownership matter? Note: Association with an address is insufficient. Bad actors can provide a target's legitimate home address	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence Add a sentence that indicates that these are not equivalent in terms of fraud prevention. Remove the requirement for STRONG/SUPERIOR evidence Remove "or an asynchronous process (i.e., visual comparison made by a proofing agent at a different time)"
63.	iA iA	4.2.6.1 4.2.6.1	42	1716- 1720- 1724- 1730- 1734- 1734- 1727-	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While this could prevent unknown bad actors from committing fraud, it does not prevent family members or close friends from committing fraud. A visual facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect potential fraud, ask the applicant questions, and observe the applicants facial movements to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a 17 deep fake could easily pass a proofing agent who reviews the evidence after capture. What is meant by a 'Validated account'? Does it need to be an account owned by someone with the same name? That is not sufficiently granular for someone with a common name. Does it need to be an account associated with someone's name and SSN? Does length of ownership matter? Note: Association with an address is insufficient. Bad actors can provide a target's legitimate home address 5 and then opt to only receive communications via email.	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence Add a sentence that indicates that these are not equivalent in terms of fraud prevention. Remove the requirement for STRONG/SUPERIOR evidence
63.	iA iA	4.2.6.1 4.2.6.1 4.2.6.1	42 42 42	1716- 1720- 1724- 1730- 1734- 1734- 1727-	FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While this could prevent unknown bad actors from committing fraud, it does not prevent family members or 17 close friends from committing fraud. A visual facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect potential fraud, ask the applicant questions, and observe the applicants facial movements to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a 17 deep fake could easily pass a proofing agent who reviews the evidence after capture. What is meant by a 'validated account'? Does it need to be an account owned by someone with the same name? That is not sufficiently granular for someone with a common name. Does it need to be an account associated with someone's name and SSN? Does length of ownership matter? Note: Association with an address is insufficient. Bad across can provide a target's legitimate home address and then opt to only receive communications via email. AAL3/FAL2 is too onerous of an authentication protocol. Looking ahead to digital passports which will	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence Add a sentence that indicates that these are not equivalent in terms of fraud prevention. Remove the requirement for STRONG/SUPERIOR evidence Remove "or an asynchronous process (i.e., visual comparison made by a proofing agent at a different time)"
63.	iA iA	4.2.6.1 4.2.6.1 4.2.6.1	42 42 42	1716- 1720- 1724- 1730- 1734- 1734- 1727-	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While this could prevent unknown bad actors from committing fraud, it does not prevent family members or 17 close friends from committing fraud. A visual facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect potential fraud, ask the applicant questions, and observe the applicants facial movements to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a 17 deep fake could easily pass a proofing agent who reviews the evidence after capture. What is meant by a 'validated account'? Does it need to be an account owned by someone with the same name? That is not sufficiently granular for someone with a common name. Does it need to be an account associated with someone's name and SSN? Does length of ownership matter? Note: Association with an address is insufficient. Bad actors can provide a target's legitimate home address is found then opt to only receive communications via email. AAL3/FAL2 is too onerous of an authentication protocol. Looking ahead to digital passports which will include cryptographic elements within a TPM on the phone that wil	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence Add a sentence that indicates that these are not equivalent in terms of fraud prevention. Remove the requirement for STRONG/SUPERIOR evidence Remove "or an asynchronous process (i.e., visual comparison made by a proofing agent at a different time)"
63.	iA iA	4.2.6.1 4.2.6.1 4.2.6.1	42 42 42	1716- 1720- 1724- 1730- 1734- 1734- 1727-	6 to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While this could prevent unknown bad actors from committing fraud, it does not prevent family members or 17 close friends from committing fraud. A visual facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect potential fraud, ask the applicant questions, and observe the applicants facial movements to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a 17 deep fake could easily pass a proofing agent who reviews the evidence after capture. What is meant by a 'validated account' Does it need to be an account owned by someone with the same name? That is not sufficiently granular for someone with a common name. Does it need to be an account owned by someone with the same name? That is not sufficiently granular for someone with a common name. Does it need to be an account owned by someone with the same name? That is not sufficiently granular for someone with a common name. Does it need to be an account owned by someone with the same name? That is not sufficiently granular for someone with a common name. Does it need to be an account owned by some	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence Add a sentence that indicates that these are not equivalent in terms of fraud prevention. Remove the requirement for STRONG/SUPERIOR evidence Remove "or an asynchronous process (i.e., visual comparison made by a proofing agent at a different time)"
63. 63. 63.	iA iA	4.2.6.1 4.2.6.1 4.2.6.1 4.2.6.2	422	1716- 1720- 1724- 1730- 1734- 1734- 1727- 1733-	FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While this could prevent unknown bad actors from committing fraud, it does not prevent family members or 7, close friends from committing fraud. A visual facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a 7 deep fake could easily pass a proofing agent who reviews the evidence after capture. What is meant by a 'Validated account'? Does it need to be an account owned by someone with the same name? That is not sufficiently granular for someone with a common name. Does it need to be an account associated with someone's name and SSN? Does length of ownership matter? Note: Association with an address is insufficient. Bad across can provide a target's legitimate home address 5 and then opt to only receive communications via cerail. AAL3/FAL2 is too onerous of an authentication protocol. Looking ahead to digital passports which will include cryptographic elements within a TPM on the phone that will be able to be validated by the CSP, an applicant will more likely be utilizing an AAL2 authenticator over an AAL3 authenticator, as the protocol to unlock the digital passport will lik	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence Add a sentence that indicates that these are not equivalent in terms of fraud prevention. Remove the requirement for STRONG/SUPERIOR evidence Remove "or an asynchronous process (i.e., visual comparison made by a proofing agent at a different time)" Provide guidance, or a reference to guidance.
63.	iA iA	4.2.6.1 4.2.6.1 4.2.6.1	422	1716- 1720- 1724- 1730- 1734- 1734- 1727- 1733-	Go to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While this could prevent unknown bad actors from committing fraud, it does not prevent family members or 17 close friends from committing fraud. A visual facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect potential fraud, ask the applicant questions, and observe the applicants facial movements to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a 17 deep fake could easily pass a proofing agent who reviews the evidence after capture. What is meant by a 'validated account'? Does it need to be an account owned by someone with the same name? That is not sufficiently granular for someone with a common name. Does it need to be an account associated with someone's name and SSN? Does length of ownership matter? Note: Association with an address is insufficient. Bad actors can provide a target's legitimate home address 5 and then opt to only receive communications via email. AAL3/FAL2 is too onerous of an authentication protocol. Looking ahead to digital passports which will include cryptographic elements within a TPM on the phone that will b	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence Add a sentence that indicates that these are not equivalent in terms of fraud prevention. Remove the requirement for STRONG/SUPERIOR evidence Remove "or an asynchronous process (i.e., visual comparison made by a proofing agent at a different time)"
63. 63. 63.	iA iA	4.2.6.1 4.2.6.1 4.2.6.1 4.2.6.2	422	1716- 1720- 1724- 1730- 2 1734- 1727- 1733- 1733-	FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While this could prevent unknown bad actors from committing fraud, it does not prevent demands the strong ability to link the applicant to the facial image on the evidence. While this could prevent unknown bad actors from committing fraud, it does not prevent family members or 17 close friends from committing fraud. A visual facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect potential fraud, ask the applicant questions, and observe the applicants facial movements to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a 17 deep fake could easily pass a proofing agent who reviews the evidence after capture. What is meant by a 'validated account'? Does it need to be an account owned by someone with the same name? That is not sufficiently granular for someone with a common name. Does it need to be an account with an address is insufficient. Bad actors can provide a target's legitimate home address and then opt to only receive communications via email. AAL3/FAL2 is too onerous of an authentication protocol. Looking ahead to digital passports which will include cryptographic elements within a TPM on the phone that will be a	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence Add a sentence that indicates that these are not equivalent in terms of fraud prevention. Remove the requirement for STRONG/SUPERIOR evidence Remove "or an asynchronous process (i.e., visual comparison made by a proofing agent at a different time)" Provide guidance, or a reference to guidance.
63. 63. 63.	iA iA	4.2.6.1 4.2.6.1 4.2.6.1 4.2.6.2	42 42 42 43	1716- 1720- 1724 1730- 1730- 1734 1727- 1733- 1773- 1757-	Go to be four pathways in that case? Digital non-biometric and digital biometric? FAIR evidence doesn't require facial images, and therefore should not require biometric or non-biometric methods to verify the evidence. However, a verification method to match the facial image on a STRONG or SUPERIOR piece of evidence is required. The likelihood of a successful impersonation varies significantly between these options, but they are listed as though they provide comparable security, which can be misleading. A confirmation code is not only an onerous process for the applicant, but it is also onerous on the CSP. This does not provide a strong ability to link the applicant to the facial image on the evidence. While this could prevent unknown bad actors from committing fraud, it does not prevent family members or 17 close friends from committing fraud. A visual facial image comparison should only be conducted at the time the person presents the evidence (so for attended sessions only). Proofing agents need to be trained enough in social engineering to be able to detect potential fraud, ask the applicant questions, and observe the applicants facial movements to detect possible fraudulent activities. This would not be available in unattended sessions, and without the ability to biometrically compare the photographic evidence, a 17 deep fake could easily pass a proofing agent who reviews the evidence after capture. What is meant by a 'validated account'? Does it need to be an account owned by someone with the same name? That is not sufficiently granular for someone with a common name. Does it need to be an account associated with someone's name and SSN? Does length of ownership matter? Note: Association with an address is insufficient. Bad actors can provide a target's legitimate home address 5 and then opt to only receive communications via email. AAL3/FAL2 is too onerous of an authentication protocol. Looking ahead to digital passports which will include cryptographic elements within a TPM on the phone that will b	with biometrics will not be able to accept an IAL2 credential that originated with another agency. Remove the requirement for FAIR evidence Add a sentence that indicates that these are not equivalent in terms of fraud prevention. Remove the requirement for STRONG/SUPERIOR evidence Remove "or an asynchronous process (i.e., visual comparison made by a proofing agent at a different time)" Provide guidance, or a reference to guidance.

Why does In LL actuated regular FAM with an image? It is the cody IRRN produces not require to an image? It is the cody IRRN produces not require to the cody of the produces and the cody of the cody	
The couple go on 19 Nat Court in the to committed by a significant out or 19 Nation. Court in the second of the couple of the co	
SSM 97 70 30 310 Material environmental materials in simple condition and status. SSM 97 80 310 Material environmental materials in simple conditions are status. SSM 97 80 310 Materials environmental materials in simple conditions are status. SSM 97 80 310 Materials environmental materials in simple conditions are status. SSM 97 80 310 Materials environmental materials in simple conditions are status. SSM 97 80 310 Materials environmental materials are status in simple conditions. SSM 99 87 30 Materials environmental materials are status in simple conditions. The status in simple conditions are status in simple conditions. The status in simple conditions are status in simple conditions. The status in simple conditions are status in simple conditions. The status in simple conditions are status in simple conditions. The status in simple conditions are status in simple conditions. The status in simple conditions are status in simple conditions. The status in simple conditions are status in simple conditions. The status in simple conditions are status in simple conditions. The status in simple conditions are status in simple conditions. The status in simple conditions are status in simple conditions. The status in simple conditions are status in simple conditions. The status in simple conditions are status in simple conditions. The status in simple conditions are status in simple conditions. The status in simple conditions are status in simple conditions. The status in simple conditions are status in simple conditions. The status in simple conditions are status in simple conditions. The status in simple conditions are status in simple conditions. The status in simple conditions are status in simple conditions. The status in simple conditions are status in status in simple conditions. The status in simple conditions are status in simple conditions. The status in simple conditions are status in status in simple conditions. The status in simple conditions are status in simple conditions. The status in simple con	
SIX 7. 20 311 Montes are transposed to the highly expendent contents of particular to the compact of the contents of the conte	
Seal	
GIA 7- 3 2 212 handed on other inhance the changed or \$100.00 cm but independ of shorthly writing sectionally independent on the changed or \$100.00 cm or sectionally independent on the changed or \$100.00 cm or sectionally independent on the changed or \$100.00 cm or sectionally independent on the changed or \$100.00 cm or sectionally independent on the changed or \$100.00 cm or sectionally independent on the changed or \$100.00 cm or sectionally independent on the changed or \$100.00 cm or sectionally independent on the changed or \$100.00 cm or sectionally independent on the changed or \$100.00 cm or sectionally independent on the changed or \$100.00 cm or sectionally independent on the changed or \$100.00 cm or sectionally independent on the changed or \$100.00 cm or \$1	ng applicant complaints or problems"
this is an every livraed and innocurate statement of the landcaspe of decitivy vetting technology body. The state of the	
while GAS** A byps and dually of performance and equality of commercial remote instructive with extending season and extending from the extending season in the extending season in the extending season in the extending season and extending from the extending season and extending from the extending season and extending seaso	
technologies arose demagraphin ² of first that all the functionages but one "sever equilable arose and demagraphin ² of the seed before of the seed of the seed before of the seed of	
mod internegative, with [a few] suspeption, "and that on the thindings "was equalled across children's description of the company of the comp	
GSA 9.3 72 57552 discorption groups the part of the pattern of the	
Sea suggested a brint "is a highly optical term that only the gardy uses, but the first of the Guidelines to Oldings" from autgested at brint" to "sea". Other "sea suggested at brint" is a highly optical term that only the gardy theme, suggest for the growing to just "sea". Other "sea suggested at brint" to "sea". For every thomas, suggest with the gardy and compression approximation accordance in part and the gardy and	
53. 9. 72 507 Law executive party rhange, suggest changing to just "ser" 53. 9. 17 6, 307 2,	y to capture certain skin tones or facial features of sufficient quality to p
61A 9.2 72 8.727.8 4 minor animal material security of the control of a material security of the control of the	
63.4 9.3 72.8 2 9 12.7 8. Page of the control only in 1.1 matches, but also in 1.N matches. Suggest charging the large property of the control of the suppose highly, especially give the fermi "based doct comparison algorithms" in an off street suppose highly, especially give the fermi "based doct comparison algorithms" in an off street suppose of the control of th	-
CSA 9.3 73 Log-2-2 Stated against against against against and security of the committee of	
63A 9.3 72 5297-25 loaded against algorithms. 63A 9.3 72 5299 algorithms algorithms. 63A 9.3 72 5299 loaded against algorithms. 63A 9.3 72 5297-25 thought to prove that they are indicated in destript their centre are extremely unequitable roam matches are as unequitable result of poorly trained algorithms, identify their due to the rise of deep false and social congenering are an even worser routil perion in an animal road hardbay and the animal road hardbay and the social dependence on the companion technology are inherently biased and wholly inadequate false and social dependence on the animal road hardbay and the social dependence on the animal road hardbay and the social dependence on the animal road animal r	
9.3 73 2928 (mighty et people who are unique former to accurate feath verifications are previously as a second of the process	
S3A 9.3 73 2598 (implying that people who are unable to accurately perform veriflications are prejudeed. Replace "Bases" with "limitations" Replace "Bases" Replace "Ba	inology, there could be a false non-match result."
In the Guidelines discussion of equity, it assumes that not giving access to a suer is the only non-equitable result, whereas the reality of final and identity, their creates an extremely unquitable result for those who need public hearists but cannot because their identity, was closely. While false non-matches are an inequipitable result of poorly trained algorithms, desirely their due to the result of poorly trained algorithms, desirely their due to the result of poorly trained algorithms, desirely their due to the result of poorly trained algorithms, desirely their due to the result of poorly trained algorithms, and perform facial verifications more accessed with their trained training to prove that thray as, indeed their training to prove that thray as, indeed their training to prove that thray as, indeed their training to the poorly as accurately the training to prove that thray as, indeed their training to their training to the poorly as accurately the section of the poorly as a province of the contraction of the poorly as accurately their training to the training to the desired fall the desired of province and their training to their training to the desired fall the desired of province." SAA 2.1.2 7, 555-57. SAA 2.1.3 8, 595 me of the self-contraction of the province of the subsection of the result of the province and the province of the provi	
courtable result, whereas the reality of fraud and identity theft creates an extremely unqualible result. for those who end public heavist but cannot because their identity was stock. While fails non-matches are an unequitable result of poorly trained algorithms, identity their due to the rive of deep face and social engineering are an even worse result, when the amount of histority has person has to go belief that facial image comparison technology are inherently blased and wholly inadequate the complete that the complete that facial image comparison technology are inherently blased and wholly inadequate the complete that the complete that facial image comparison technology are inherently blased and wholly inadequate the complete that facial image comparison technology are inherently blased and wholly inadequate the complete that facial image comparison technology are inherently blased and wholly inadequate the complete that facial image comparison technology are inherently blased and wholly inadequate the complete that facial image comparison technology are inherently blased and wholly inadequate the complete that facial image comparison technology are inherently blased and wholly inadequate the complete that facial image comparison technology are inherently blased and wholly inadequate the complete that facial image comparison technology are inherently blased and wholly inadequate the complete that facial image comparison technology are inherently blased and wholly inadequate and the complete that facial image comparison technology are inherently blased and wholly inadequate and the complete that facial image comparison technology are inherently blased and wholly inadequate and the complete that facial image comparison that the complete that facial image comparison the through the complete the complete that facial image comparison to the real facial or all an advantage of the complete that facial image comparison to the complete that facial image comparison to the complete that facial image comparison to the	
equitable result, whereas the reality of fraud and identity their croates an extremely unequalishe result for brown end public benefits but cannot because their identity was stored. While fails non-matches are an unequalable result of poorly trained algorithms, identity their due to the rise of deep fails and social engineering are an even worse result, when the amount of harbships a person has to go belief that facial image companion technology are inherently blased and wholly inadequate their completed in the facial image companion technology are inherently blased and wholly inadequate their completed in the facial image companion technology are inherently blased and wholly inadequate their completed in the facial image companion technology are inherently blased and wholly inadequate their completed in the facial image companion technology are inherently blased and wholly inadequate their completed in the facial image companion technology are inherently blased and wholly inadequate their completed in the facial image companion technology are inherently blased and wholly inadequate their completed in the facial image companion technology are inherently blased and wholly inadequate their completed in the facial image companion technology are inherently blased and wholly inadequate their completed in the facial image companion technology are inherently blased and wholly inadequate the individual who have a problem that the facial image companion to the real problems of the process individual who have a problem that in a problem in the problems problems in the problems proposed by the algorithm of the process individual who have a report to the process individual who have a problem to the problems of the process individual who have a problem to the problems of the process individual who have a problem to the problems of the process individual who have a problem to the problems of the	
for those who need public benefits but cannot because their identity was stolen. While the due to the rise of deep interest of pondy framed agointhms, identified due to the rise of deep faces are an unequitable hardships of the process are not provided and growthms, and an experimental provided in the process are not provided and growthms, and the process are not provided and growthms, and the process are not provided and growthms, and the provided and pro	
matches are an inequitable result of poorly trained algorithms, identity theft due to the rise of deep faces. 53A 9.3 72 595-59 through to prove that they are, indeed, their own identity, and so continuing a many own of the provided and within the provided and so continuing a many own of the provided and within the provided and provid	
63A 9.3 72 j259725 frough to prove that they are, indeed, their own identity. 63A 9.3 172 j259725 frough to prove that they are, indeed, their own identity. 63A 9.3 173 j259725 frough to prove that they are, indeed, their own identity. 63A 9.3 173 j25972 frough to prove that they are, indeed, their own identity. 63A 9.3 175 j25972 feed all end in the providing an automated option for individuals who have accurately than trained human agents. 50, providing an automated option for individuals who have the option for applicants to have a photo taken which will be algorithmically compared to the option for applicants to have a photo taken which will be algorithmically compared to the option for applicants to have a photo taken which will be algorithmically compared to the option for applicants to have a photo taken which will be algorithmically compared to the option for applicants to have a photo taken which will be algorithmically compared to the option for applicants to have a photo taken which will be algorithmically compared to the option for applicants to have a photo taken which will be algorithmically compared to the option for applicants to have a photo taken which will be algorithmically compared to the option for applicants to have a photo taken which will be algorithmically compared to the option of the process under the option of the process of the process of the process of the process under the option of the process of t	
When high quality images are used, best of breed algorithms now perform facial verifications more accurately than trained human agents. So, providing an automation for individuals who have been declared to the more concisely vacuately than trained human agents. So, providing an automation for individuals who have evolence." 834 9.3 72 2011 falled verification by a human would reduce false non-matches. 855 21 detection skills. 858 21.2 755572 detection skills. 858 21.3 859 2572 detection skills. 859 21.3 859 2572 detection skills. 850 21.3 859 2572 detect	sed and wholly inadequately untrained, and therefore allowing for a
accurately than trained human agents. So, providing an automated option for individuals who have evidence." A 9.3 72 2001 false everification by a human would reduce false non-matches evidence. " More clearly state the difference between a trusted referee and a proofing agent: the trusted referee." More clearly state the difference between a trusted referee and a proofing agent: the trusted referee." S 9.3 72 2001 false everification shills. More clearly state the difference between a trusted referee and a proofing agent: the trusted referee." More clearly state the difference between a trusted referee and a proofing agent: the trusted referee." Add language about training to end of proofing agent definition. Add language about devia with the process underded. That fits with the language at the end of this subsection but is not clear in the definition. Also state that if any part is attended, the second sentence: "Some parts of the process may still be automated. If any portion of the control of the part of the process may still be automated. If any portion of the control of the part of the process may still be automated. If any portion of the control of the part of the process may still be automated. If any portion of the control of the part of the process may still be automated. If any portion of the control of the part of the process may still be automated. If any portion of the control of the part of the process may still be automated. If any portion of the control of the part of the process may still be automated. If any portion of the control of the part of the process may still be automated. If any portion of the control of the part	
63A 2.1.2 7 555-571 [detection skills. 63A 2.1.3 8 593 and detection but not clearly state the defference between a trusted reference and a proofing agent: the trusted reference sevenowered by the CSP to make deviations from the required evidenced following pre-established guidelines. Yes, there may be some difference in training, but need from the other wholly attended. For instance, if the applicant struggles with noty the selfle, they can do the rest of the process unattended. That fits with the language at the end of this subsection but is not clear in the definitions. Also state that if any part is attended, the 58A 2.1.3 8 593 and def "by the applicant" [The definitions and devices used by the applicant in the proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language the center of the proofin structure in the proofing as a definition and devices with the department of the proofing add second sentence: "Some part of the process may still be automated in a proofinition and devices used by the applicant in the proofing process are not controlled to the proofinition and devices used by the applicant in the proofining proofining and de	
More Clearly state the difference between a trusted referee and a proofing agent: the trusted referee sempowered by the CSP to make devalors from the requirement of substance of the CSP to make devalors from the requirement of the control of the	intrimically compared to the portrait on their strongest piece of
sempowered by the CSP to make deviations from the required evidence following pre-established guidelines. Yes, there may be some difference in training, but both need fraud and social engineering. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of proofing agent definition. Add language about training to end of this subscience in the definition. Add language about training to end of this subscience in the definition. Add language at the end of this subscience in the definition and devices used by the applicant in the proofing process are not controlled to the proof add add the proof add the proof add add th	
S3A 2.1.2 7 555-57 detection skills Indicate that the session does not have to be wholly attended. For instance, if the applicant struggles with only the selfic, they can do the rest of the process unattended. That fits with the language at the end of this subsection but is not clear in the definitions. Also state that if any part is attended, the old second sentence: "Some parts of the process may still be automated. If any portion of the location and devices used by the applicant" Indicate that if any part is attended, the old second sentence: "Some parts of the process may still be automated. If any portion of the location and devices used by the applicant in the proofing process are not controlled by the control of the location and devices used by the applicant in the proofing process are not controlled by the control of the location and devices used by the applicant in the proofing process are not controlled by the control of the location and devices used by the applicant in the proofing process are not controlled by the control of the location and devices used by the applicant in the proofing process are not controlled by the control of the location and devices used by the applicant in the proofing process are not controlled by the control of the location and devices used by the applicant in the proofing process are not controlled by the control of the location and devices used by the applicant in the proofing process are not controlled by the control of the proofing process are not controlled by the control of the proofing process are not controlled by the control of the proofing process are not controlled by the control of the proofing process are not controlled by the control of the proofing proofing and the proofing proofing and the proofing process are not controlled by the control of the proofing process are not controlled by the control of the proofing proofing and the proofing proof	
midicate that the session does not have to be wholly attended. For instance, if the applicant struggles with only the selfic, they and not fit is subsection but is not clear in the definitions. Also state that if any part is attended, the add second sentence: "Some parts of the process may still be automated." The first with the language at the end of this subsection but is not clear in the definitions. Also state that if any part is attended, the add second sentence: "Some parts of the process may still be automated. If any portion of 163A 2.1.1 11 674 Immbering issue. Two 91s. It's confusing now we say the document uses valid to not refer to expired but then parenthetically in the location and devices used by the applicant in the proofing process are not controlled by the specific of the process of the process may still be automated. If any portion of 163A 2.1.1 17 873 defines valid as unexpired. Can this language be cleare? It's confusing now we say the document uses valid to not refer to expired but then parenthetically in the location and devices used by the applicant in the proofing process are not controlled by the specific of the process may still be automated. If any portion of the location and devices used by the applicant in the proofing process are not controlled by the specific of the process may still be automated. If any portion of the location and devices used by the applicant in the proofing process are not controlled by the specific of the process may still be automated. If any portion of the location and devices used by the applicant in the proofing process are not controlled by the proofing process are not con	
with only the selfle, they can do the rest of the process unstanted. That fits with the language at the end of this subsection but is not clear in the definitions. Also state that if any part is attended, the 353 at 2.1.3 8 593 and add "by the applicant" The location and devices used by the applicant in the proofing process are not controlled by 15 containing how we say the document uses valid to not refer to expired but then parenthetically 15 containing how we say the document uses valid to not refer to expired but then parenthetically 16 containing how we say the document uses valid to not refer to expired but then parenthetically 17 containing how we say the document uses valid to not refer to expired but then parenthetically 18 containing how we say the document uses valid to not refer to expired but then parenthetically 18 containing how we say the document uses valid to not refer to expired but then parenthetically 18 containing how we say the document uses valid to not refer to expired but then parenthetically 18 containing how we say the document uses valid to not refer to expired but then parenthetically 18 containing how the say the document uses valid to not refer to expired but then parenthetically 18 containing how the say the document uses valid to not refer to expired but then parenthetically 18 containing how the say the document uses valid to not refer to expired but then parenthetically 18 containing how the say the document uses valid to not refer to expired but then parenthetically 18 containing how the say the document uses valid to not refer to expired but then parenthetically 18 containing how the say the document uses valid to not refer to expired but then parenthetically 18 containing how the say the document uses valid to not refer to expired but then parenthetically 18 containing how the say the document uses valid to not refer to expired but then parenthetically 18 containing how the say the document uses valid to not refer to expired but then parenthetically 18 containing how the s	Add language about deviations to definition of trusted referee. Change n
end of this subsection but is not clear in the definitions. Also state that if any part is attended, the add second sentence: "Some parts of the process may still be automated. If any portion of 63A 2.1.3 8 595 entire process should be considered attended. 63A 2.4.1 1 10 674 numbering size. Two 91S. 63A 2.4.1 1 17 674 numbering size. Two 91S. 63A 2.4.1 1 17 674 numbering size. Two 91S. 63A 2.4.1 1 17 674 numbering size. Two 91S. 63A 3.1.1 17 675 defines valid as unexpired. Can this language be clearer? 63A 3.1.1 17 675 defines valid as unexpired. Can this language be clearer? 63A 3.1.1 17 875 defines valid as unexpired. Can this language be clearer? 63A 3.1.2 18 888 fraudsters if they were known 63A 3.1.2.1 18 997 servers, predictive analytics 63A 3.1.2.1 18 997 servers, predictive analytics 63A 3.1.2.1 19 939 continuous monitoring has a specific meaning that perhaps is not intended here (though it is the ideal) 63A 3.1.2 19 945 should only request the core, except for these or collect additional attributes, even if the RP 63A 3.1.2 19 954 should only request the core, except for these or collect additional attributes, even if the RP 63A 3.1.3 1 22 1023 individual? 63A 3.1.4 23 1067 typo "are be" 63A 3.1.5 25 1162 they be probably forgotten. It only adds risk of sufficient as an option as well 63A 3.1.9 26 1164 this check the finding and correlated and propriate AAL is sufficient as an option as well 63A 3.1.9 26 1174 By which the chock the finding and correlated and propriate AAL is sufficient as an option as well 63A 3.1.9 26 1174 By which the chock and propriate AAL is sufficient as an option as well 63A 3.1.9 2.114 the cattern and the find an org. could they see it? Walt fit the end user is an option as well 63A 3.1.9 26 1174 By which the chock and the find an org. could they see it? Walt fit the end user is an option as wel	
S3A 2.1.3 8 559; entire process should be considered attended. 3 359 and add 559 and 3 2.1.3 8 593 and 3 559 and 3 2.1.3 8 593 and 3 2.1.3 1 2 2 2 3 3 3 3 3 3 3	
63A 2.4.1 11 674 numbering issue. Two #1s. 15 674 numbering issue. Two #1s 15 674 numb	compated. If any portion of the process involves a proofing agent, it is cons
63A 2.4.11 11 674 numbering issue. Two #1s.	
Ets confusing how we say the document uses valid to not refer to expired but then parenthetically	Access are not controlled by the corr.
S3A 3.1.1 17 875 Add 15. Fraud management practices to align with 3.1.2.1(1) Be more precise about what capabilities should be included in the practice statements. While the market certainly needs additional anasperncy, some of these are trade secrets or would advantage and the specific capabilities and details of this program SHALL be documented within their CSP consider including other fraud check techniques: device fingerprinting and correlation, VPNs and proxy servers, predictive analytics servers, predictive analytics is the intended here (though it is the ideal) Change continuous to continual is this intended to imply CSPs cannot collect additional attributes to support fraud mitigation? I think that would be limiting. May need to clarify that the CSP can collect additional attributes, even if the RP should only request the core, except for these fraud exceptions in this clause Add similar language to 3.1.2.1	
Be more precise about what capabilities should be included in the practice statements. While the market certainly needs additional transparency, some of these are trade secrets or would advantage sale fraudsters if they were known to consider including other fraud check techniques: device fingerprinting and correlation, VPNs and proxy consider including other fraud check techniques: device fingerprinting and correlation, VPNs and proxy some of these are trade secrets or would advantage to consider including other fraud check techniques: device fingerprinting and correlation, VPNs and proxy some of these are trade secrets or would advantage to consider including other fraud check techniques: device fingerprinting and correlation, VPNs and proxy some of these are trade secrets or would advantage and the secrets or would advantage to consider including other fraud check techniques: device fingerprinting and correlation, VPNs and proxy some of these are trade secrets or would advantage and the secrets of the secrets or would advantage and the secrets of the secrets or would advantage and the secrets or would advantage and	
market certainly needs additional transparency, some of these are trade secrets or would advantage 3.1.2.1 18 888 fraudsters if they were known consider including other fraud check techniques: device fingerprinting and correlation, VPNs and proxy servers, predictive analytics 63A 3.1.2.1 19 939 continuous monitoring has a specific meaning that perhaps is not intended here (though it is the ideal) is this intended to imply CSPs cannot collect additional attributes to support fraud mitigation? I think that would be limiting. May need to clarify that the CSP can collect additional attributes, even if the RP 63A 3.1.2.2 19 954 should only request the core, except for these fraud exceptions in this clause More clearly define what we mean by organization. Is that just RPs or something else? If an end user (subscriber) is an org or is acting on behalf of an org, could they see it? What if the end user is an individual? 63A 3.1.4 23 1067 typo "are be" Be more specific about results. Raw data? Summary reports? Making all mitigations public may advantage attackers—and may do so in a way that undermines the very groups we hope to benefit from Limit what is publicly available and more comprehensive results available only to RPs, regulations 24 hours is too long or email. In reality if someone doesn't confirm an email within a few minutes, Lower 24 hours to 1 hours 63A 3.1.9 26 1164 make clear that authentication at an appropriate AAL is sufficient as an option as well Authentication at a corresponding AAL or higher is sufficient to obviate the need for a cont forms.	.2.1
63A 3.1.2.1 18 888 fraudsters if they were known 63A 3.1.2.1 18 907 consider including other fraud check techniques: device fingerprinting and correlation, VPNs and proxy 63A 3.1.2.1 19 909 continuous monitoring has a specific meaning that perhaps is not intended here (though it is the ideal) 63A 3.1.2.1 19 909 continuous monitoring has a specific meaning that perhaps is not intended here (though it is the ideal) 63A 3.1.2.2 19 954 should only request the core, except for these fraud exceptions in this clause 63A 3.1.2.2 19 954 should only request the core, except for these fraud exceptions in this clause 63A 3.1.3.1 22 1023 individual? 63A 3.1.4 23 1067 typo "are be" 8 more specific about results. Raw data? Summary reports? Making all mitigations public may advantage attackers—and may do so in a way that undermines the very groups we hope to benefit from 13A 3.1.4 23 1067 typo "are be" 8 be more specific about results. Raw data? Summary reports? Making all mitigations public may advantage attackers—and may do so in a way that undermines the very groups we hope to benefit from 15A 3.1.4 23 1067 typo "are be" 8 be more specific about results. Raw data? Summary reports? Making all mitigations public may advantage attackers—and may do so in a way that undermines the very groups we hope to benefit from 15A 3.1.4 23 1067 typo "are be" 15A 1062 they very probably forgotten. It only adds risk 15A 3.1.9 26 1162 they've probably forgotten. It only adds risk 15A 3.1.9 26 1174 [By which methods can the CSP deliver the code? Validated address? Just in session?	
consider including other fraud check techniques: device fingerprinting and correlation, VPNs and proxy servers, predictive analytics 63A 3.1.2.1 19 939 continuous monitoring has a specific meaning that perhaps is not intended here (though it is the ideal) is this intended to imply CSPs cannot collect additional attributes to support fraud mitigation? I think that would be limiting. May need to clarify that the CSP can collect additional attributes, even if the RP 63A 3.1.2.2 19 954 should only request the core, except for these fraud exceptions in this clause More clearly define what we mean by organization. Is that just RPs or something else? If an end user (subscriber) is an org or is acting on behalf of an org, could they see it? What if the end user is an 63A 3.1.4 23 1067 typo "are be" Be more specific about results. Raw data? Summary reports? Making all mitigations public may advantage attackers—and may do so in a way that undermines the very groups we hope to benefit from 24 hours is too long or email. In reality if someone doesn't confirm an email within a few minutes, 63A 3.1.8 26 1162 they've probably forgotten. It only adds risk Lower 24 hours to 1 hours 63A 3.1.9 26 1174 By which methods can the CSP deliver the code? Validated address? Just in session?	umanted within their CCD practice statement with sufficient detail to an
63A 3.1.2.1 18 907 servers, predictive analytics 63A 3.1.2.1 19 939 continuous monitoring has a specific meaning that perhaps is not intended here (though it is the ideal) 63A 3.1.2.1 19 939 continuous monitoring has a specific meaning that perhaps is not intended here (though it is the ideal) 63A 3.1.2.2 19 954 should only request the core, except for these fraud exceptions in this clause 63A 3.1.3.1 22 1023 individual? 63A 3.1.4 23 1067 typo "are be" 63A 3.1.4 23 1067 typo "are be" 63A 3.1.4 23 1067 typo "are be" 63A 3.1.8 26 1085 the mitigations 24 hours is too long or email. In reality if someone doesn't confirm an email within a few minutes, 63A 3.1.9 26 1174 By which methods can the CSP deliver the code? Validated address? Just in session?	amented within their CSP practice statement with sufficient detail to ap
3.1.2.1 19 939 continuous monitoring has a specific meaning that perhaps is not intended here (though it is the ideal) Statis intended to imply CSPs cannot collect additional attributes to support fraud mitigation? I think that would be limiting. May need to clarify that the CSP can collect additional attributes, even if the RP Add similar language to 3.1.2.1 Statis intended to imply CSPs cannot collect additional attributes, even if the RP Add similar language to 3.1.2.1 More clearly define what we mean by organization. Is that just RPs or something else? If an end user (subscriber) is an org or is acting on behalf of an org., could they see it? What if the end user is an (subscriber) is an org or is acting on behalf of an org., could they see it? What if the end user is an (subscriber) is an org or is acting on behalf of an org., could they see it? What if the end user is an (subscriber) is an org or is acting on behalf of an org., could they see it? What if the end user is an (subscriber) is an org or is acting on behalf of an org., could they see it? What if the end user is an (subscriber) is an org or is acting on behalf of an org., could they see it? What if the end user is an organization. It is a subscriber is an organization is an organization. It is a subscriber is an organization is an organization. It is a subscriber is an organization at an appropriate AAL is sufficient as an option as well is an organization. It is the intended here (though it is the ideal) (change continuous to continual (change continuous to end think the RP Add similar language to 3.1.2.1 Add similar language to 3.1.2.1	
Is this intended to imply CSPs cannot collect additional attributes to support fraud mitigation? I think that would be limiting. May need to clarify that the CSP can collect additional attributes, even if the RP 54 should only request the core, except for these fraud exceptions in this clause 4dd similar language to 3.1.2.1 More clearly define what we mean by organization. Is that just RPs or something else? If an end user (subscriber) is an org or is acting on behalf of an org, could they see it? What if the end user is an (subscriber) is an org or is acting on behalf of an org, could they see it? What if the end user is an (change to RP 3.1.4 23 1007 typo "are be" 3re to be? Be more specific about results. Raw data? Summary reports? Making all mitigations public may advantage attackers—and may do so in a way that undermines the very groups we hope to benefit from 5.4 3.1.4 23 1085 the mitigations 24 hours is too long or email. In reality if someone doesn't confirm an email within a few minutes, 24 hours is too long or email. In reality if someone doesn't confirm an email within a few minutes, 24 hours to 1 hours 3.1.9 26 1164 make clear that authentication at an appropriate AAL is sufficient as an option as well 4 Authentication at a corresponding AAL or higher is sufficient to obviate the need for a cont 3.1.9 26 1174 By which methods can the CSP deliver the code? Validated address? Just in session?	
that would be limiting. May need to clarify that the CSP can collect additional attributes, even if the RP 3.1.2.2 19 954 should only request the core, except for these fraud exceptions in this clause More clearly define what we mean by organization. Is that just RPs or something else? If an end user is an (subscriber) is an org or is acting on behalf of an org, could they see it? What if the end user is an 63A 3.1.3.1 22 1023 individual? 63A 3.1.4 23 1067 typo "are be" Be more specific about results. Raw data? Summary reports? Making all mitigations public may advantage attackers—and may do so in a way that undermines the very groups we hope to benefit from 63A 3.1.4 23 1085 the mitigations 24 hours is too long or email. In reality if someone doesn't confirm an email within a few minutes, 63A 3.1.8 26 1162 they've probably forgotten. It only adds risk 63A 3.1.9 26 1174 By which methods can the CSP deliver the code? Validated address? Just in session? Limit what is publicly available and more comprehensive results available only to RPs, regul adventure of the completion of the completion of the code? Validated address? Just in session?	
63A 3.1.2.2 19 954 should only request the core, except for these fraud exceptions in this clause More clearly define what we mean by organization. Is that just RPs or something else? If an end user is an (subscriber) is an org or is acting on behalf of an org, could they see it? What if the end user is an (subscriber) is an org or is acting on behalf of an org, could they see it? What if the end user is an (subscriber) is an org or is acting on behalf of an org, could they see it? What if the end user is an (change to RP) 63A 3.1.4 23 1067 typo "are be" Be more specific about results. Raw data? Summary reports? Making all mitigations public may advantage attackers—and may do so in a way that undermines the very groups we hope to benefit from Limit what is publicly available and more comprehensive results available only to RPs, reguling they've probably forgotten. It only adds risk 63A 3.1.8 26 1162 they've probably forgotten. It only adds risk 63A 3.1.9 26 1174 By which methods can the CSP deliver the code? Validated address? Just in session?	
More clearly define what we mean by organization. Is that just RPs or something else? If an end user (subscriber) is an org or is acting on behalf of an org, could they see it? What if the end user is an 63A 3.1.4 23 1067 typo "are be" are to be? Be more specific about results. Raw data? Summary reports? Making all mitigations public may advantage attackers—and may do so in a way that undermines the very groups we hope to benefit from 63A 3.1.4 23 1085 the mitigations 24 hours is too long or email. In reality if someone doesn't confirm an email within a few minutes, 63A 3.1.8 26 1162 they've probably forgotten. It only adds risk Lower 24 hours to 1 hours 63A 3.1.9 26 1174 By which methods can the CSP deliver the code? Validated address? Just in session?	
(subscriber) is an org or is acting on behalf of an org, could they see it? What if the end user is an 63A 3.1.3.1 22 1023 individual? 63A 3.1.4 23 1067 typo "are be" Be more specific about results. Raw data? Summary reports? Making all mitigations public may advantage attackers—and may do so in a way that undermines the very groups we hope to benefit from Limit what is publicly available and more comprehensive results available only to RPs, regulations. 24 hours is too long or email. In reality if someone doesn't confirm an email within a few minutes, 63A 3.1.8 26 1162 they've probably forgotten. It only adds risk 63A 3.1.9 26 1174 By which methods can the CSP deliver the code? Validated address? Just in session?	
63A 3.1.3.1 22 1033 individual? Change to RP 63A 3.1.4 23 1067 typo "are be" 8 more specific about results. Raw data? Summary reports? Making all mitigations public may advantage attackers—and may do so in a way that undermines the very groups we hope to benefit from 63A 3.1.4 23 1085 the mitigations 24 hours is too long or email. In reality if someone doesn't confirm an email within a few minutes, 63A 3.1.8 26 1162 they've probably forgotten. It only adds risk 63A 3.1.9 26 1174 by which methods can the CSP deliver the code? Validated address? Just in session? Change to RP are to be? Limit what is publicly available and more comprehensive results available only to RPs, regul Limit what is publicly available and more comprehensive results available only to RPs, regul Lower 24 hours to 1 hours Authentication at a corresponding AAL or higher is sufficient to obviate the need for a cont 63A 3.1.9 26 1174 by which methods can the CSP deliver the code? Validated address? Just in session?	
63A 3.1.4 23 1067 typo "are be" Be more specific about results. Raw data? Summary reports? Making all mitigations public may advantage attackers—and may do so in a way that undermines the very groups we hope to benefit from 63A 3.1.4 23 1085 the mitigations 24 hours is too long or email. In reality if someone doesn't confirm an email within a few minutes, 63A 3.1.8 26 1162 they've probably forgotten. It only adds risk Lower 24 hours to 1 hours 63A 3.1.9 26 1164 make clear that authentication at an appropriate AAL is sufficient as an option as well Authentication at a corresponding AAL or higher is sufficient to obviate the need for a cont 63A 3.1.9 26 1174 By which methods can the CSP deliver the code? Validated address? Just in session?	
Be more specific about results. Raw data? Summary reports? Making all mitigations public may advantage attackers—and may do so in a way that undermines the very groups we hope to benefit from Limit what is publicly available and more comprehensive results available only to RPs, regul 24 hours is too long or email. In reality if someone doesn't confirm an email within a few minutes, Lower 24 hours to 1 hours 15 hours 26 hours 16 hours 26 hours 27 hours 28 hours 16 hours 28 hours 16 hours 29 hou	
63A 3.1.4 23 1085 the mitigations Limit what is publicly available and more comprehensive results available only to RPs, regular 24 hours is too long or email. In reality if someone doesn't confirm an email within a few minutes, 63A 3.1.8 26 1162 they've probably forgotten. It only adds risk 63A 3.1.9 26 1164 make clear that authentication at an appropriate AAL is sufficient as an option as well 63A 3.1.9 26 1174 By which methods can the CSP deliver the code? Validated address? Just in session?	
24 hours is too long or email. In reality if someone doesn't confirm an email within a few minutes, 63A 3.1.8 26 1162 they've probably forgotten. It only adds risk 63A 3.1.9 26 1164 make clear that authentication at an appropriate AAL is sufficient as an option as well 63A 3.1.9 26 1174 By which methods can the CSP deliver the code? Validated address? Just in session? Authentication at a corresponding AAL or higher is sufficient to obviate the need for a cont	
63A 3.1.8 26 1162 they've probably forgotten. It only adds risk Lower 24 hours to 1 hours 63A 3.1.9 26 1164 make clear that authentication at an appropriate AAL is sufficient as an option as well 63A 3.1.9 26 1174 By which methods can the CSP deliver the code? Validated address? Just in session?	vailable only to RPs, regulators, etc.
63A 3.1.9 26 1164 make clear that authentication at an appropriate AAL is sufficient as an option as well Authentication at a corresponding AAL or higher is sufficient to obviate the need for a cont 63A 3.1.9 26 1174 By which methods can the CSP deliver the code? Validated address? Just in session?	
63A 3.1.9 26 1174 By which methods can the CSP deliver the code? Validated address? Just in session?	buints the pood for a continuation or -!-
	wate the need for a continuation code
Define "explicit biometric consent." Does this mean a separate consent from that for the service, or	
63A 3.1.11 27 1226 that the terms contain an explicit statement. explicitly state consent for biometric collection before collecting	
What does live capture mean here? I understand it in the context of DL or passport, but it sounds like I	
63A 3.1.12 29 1295 can't upload an image of fair evidence; I have to have a physical copy of it to scan in-session live capture applies to STRONG and above evidence. Alternatively, the entire section only a	, the entire section only applies to STRONG and above

					Trusted referees are only necessary when an RP wants to accept based on its risk determinations. It's	
					not up to a CSP, particularly a 3rd party CSP, to determine if a trusted referee process is sufficient. This	
					could lead to problematic incentives for CSPs. It could also disadvantage small CSPs and make market	
	63A	3.1.13	31	1 13	49 entry difficult	change SHALL to SHOULD, when requested by the RP
					Subscribers should have to authenticate at the AAL that corresponds to the upgraded identity, not the	
	63A	3.2	35	5 14	90 highest. If you're going from IAL1 to IAL2, you don't need to authenticate at AAL3.	Authenticate at an AAL at or higher than the upgraded IAL
	63A	4.1.10	39		25 the authenticators can also be bound prior to the proofing event	before, at the time of, or after the proofing event
 	USA	4.1.10	3:	J 10	23 the authenticators can also be bound prior to the probling event	before, at the time of, or after the probing event
					If you do retain the possibility of an asynchronous process, it needs more explanation and a clearer	
					description of the requirements around it. A still photo is not sufficient. At minimum, a still would need	
	63A	4.1.6(5)	37	7 1	61 to be captured with liveness. Ditto this comment for other mentions of a synch comparison	
					Are there unintended consequences with requiring "each subscriber as a unique identity"? For instance	
					sole proprietorships may have an individual account and a business account, both with the same	
	63A	5.1	50	10	27 identity. This is also not specific to an IAL, so it could apply to pseudonymous applications.	change identity to entity or persona
-	03/1	5.2		-	The type of proofing should be for each piece of evidence and step in the process as proofing may be	enange technique of persona
	504					
<u> </u>	63A	5.1	50) 19	41 multi-modal (got stuck on selfie)	Type of proofing for each type of identity evidence
	63A	5.2	51	1 19	58 not just PII	change PII to personal information
l I		1	1	1	Reference WCAG. Accessibility challenges should be mitigated consistent with federal requirements.	
L I	63A	9.3	3 74	4 20	27 Consider making this normative	
ı İ					Consider adding a column for allowable proofing type. For instance, is SSN acceptable if remote so long	
l l	63A	A.1	78	8 2	28 as it's presented as an image of a card and not just the number?	
\vdash		· · -	†	1 -		1
[1		This is an averagehing comment for 620: In its introduction, NICT recommends "analises"	.
1		1	1		This is an overarching comment for 63B: In its introduction, NIST recommends "applications assessed a	` I
[1		AAL1 offer" MFA, which suggests that AAL1 is barely a "basic confidence" assurance level. More	
					strongly, NIST requires "[a]applications assessed at AAL2 must offer a phishing-resistant authentication	
					option." While this is a great mandate, if an application has both phishable and phishing resistant	
					authenticator options, the application continues to be phishable and the phishing-resistant option	
					mandate loses its purpose - to effectively protect against phishing attacks. Additionally, federation	
					assertions don't always assert whether an authenticator was phishing resistant or not, just that it was	
					MFA/2FA, so adding an additional AAL would create a need for vendors to insert greater veracity in	
					their assertions. As such, phishable MFA should become AAL1, AAL2 should be phishing resistant and	
	63B	Ι	1 & 2	400	113 an AALO should be created to allow for single factor authentication scenarios.	Create an AALO that is a low assurance and allows for single factor; AAL1 should become phishable MFA, whereas AAL2 should be phishin
<u> </u>	638		1 1 & 2	403-		Create an AALU that is a low assurance and allows for single factor; AALI should become phishable MFA, whereas AALZ should be phishing
					This is an overarching comment for 63B: All cryptographic authenticators are technically syncable, but	
					the type of authenticator NIST is referencing is actually synched authenticators - those that	
ı	63B	3.1.7.4			11 affirmatively decided to synch and remove its device-bound status	Change all "syncable" references to "synced"
	63B 63B	3.1.7.4 3.2.2	28		11 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts.	Change all "syncable" references to "synced" Suggest reducing the amount of attempts to below 100.
					11 affirmatively decided to synch and remove its device-bound status	
			28	8 1	11 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts.	
	63B	3.2.2	28	8 17	11 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 24 users pick their second factor doesn't make sense.	Suggest reducing the amount of attempts to below 100.
	63B 63B	3.2.2	28	8 12 3 2463 6 2554	11 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 24 users pick their second factor doesn't make sense.	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate.
	63B 63B 63B	3.2.2	28	8 12 3 2463 6 2554	11 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 2d users pick their second factor doesn't make sense. 2555 59 change agencies to organizations, as throughout this section you discuss "organizations"	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma.
	63B 63B 63B 63-Base	3.2.2	28	3 2463 6 2554 1 3	11 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing users pick their second factor doesn't make sense. 2555 50 change agencies to organizations, as throughout this section you discuss "organizations" It's unclear what a "culturally appropriate" option would be for individuals, considering every identity	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations
	63B 63B 63B 63-Base 63-Base	8.2.2 8.4 9.1	28 1 73 0 76 1 1	8 12 3 2463 6 2554 1 3	11 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 24 users pick their second factor doesn't make sense. 2555 59 change agencies to organizations, as throughout this section you discuss "organizations" It's unclear what a "culturally appropriate" option would be for individuals, considering every identity 79 needs to be vetted to the appropriate assurance level.	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference.
	63B 63B 63-Base 63-Base 63-Base	8.2.2 8.4 9.1	28 1 73 9 76 1 1	8 12 3 2463 6 2554 1 3	11 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 24 users pick their second factor doesn't make sense. 2555 256 Change agencies to organizations, as throughout this section you discuss "organizations" it sunclear what a "culturally appropriate" option would be for individuals, considering every identity needs to be vetted to the appropriate assurance level. 262 Evpographical error	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization"
	63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.4 5 1 1 1 2.3	28 1 73 9 76 1 1 1 2 1 1	8 12 3 2463 6 2554 1 3 2 3 1 3	11 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing users pick their second factor doesn't make sense. 2555 Change agencies to organizations, as throughout this section you discuss "organizations" It's unclear what a "culturally appropriate" option would be for individuals, considering every identity 79 needs to be vetted to the appropriate assurance level. 2 typographical error 46 typographical error	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.4 5 1 1 2.1 2.1	28 73 76 76 76 76 76 76 76 76 76 76 76 76 76	8 12 3 2463 6 2554 1 3 2 3 1 3 0 6	11 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 124 users pick their second factor doesn't make sense. 12555 Schange agencies to organizations, as throughout this section you discuss "organizations" 11's unclear what a "culturally appropriate" option would be for individuals, considering every identity 179 needs to be vetted to the appropriate assurance level. 180 typographical error	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash
	63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.4 5 1 1 1 2.3	28 73 76 76 76 76 76 76 76 76 76 76 76 76 76	8 12 3 2463 6 2554 1 3 2 3 1 3 0 6	11 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 24 users pick their second factor doesn't make sense. 255 255 26 change agencies to organizations, as throughout this section you discuss "organizations" 18 t's unclear what a "culturally appropriate" option would be for individuals, considering every identity needs to be vetted to the appropriate assurance level. 26 typographical error 46 typographical error 47 typographical error 48 typographical error 49 typographical error	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party"
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.4 5 1 1 2.1 2.1	28 73 76 76 76 76 76 76 76 76 76 76 76 76 76	8 12 3 2463 6 2554 1 3 2 3 1 3 0 6	11 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing users pick their second factor doesn't make sense. 2555 change agencies to organizations, as throughout this section you discuss "organizations" It's unclear what a "culturally appropriate" option would be for individuals, considering every identity 79 needs to be vetted to the appropriate assurance level. 20 typographical error 40 typographical error 40 typographical error 40 typographical error 41 typographical error 42 typographical error 43 typographical error 44 typographical error 45 typographical error 46 typographical error 47 typographical error 48 typographical error 49 typographical error 40 typographical error	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party"
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.4 5 1 1 2.1 2.1	28 73 76 76 76 76 76 76 76 76 76 76 76 76 76	8 12 3 2463 6 2554 1 3 2 3 1 3 0 6	11 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 24 users pick their second factor doesn't make sense. 255 255 26 change agencies to organizations, as throughout this section you discuss "organizations" 18 t's unclear what a "culturally appropriate" option would be for individuals, considering every identity needs to be vetted to the appropriate assurance level. 26 typographical error 46 typographical error 47 typographical error 48 typographical error 49 typographical error	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party"
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.4 5 1 1 2.1 2.1	28 73 76 76 76 76 76 76 76 76 76 76 76 76 76	8 12 3 2463 6 2554 1 3 2 3 1 3 0 6	11 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing users pick their second factor doesn't make sense. 2555 change agencies to organizations, as throughout this section you discuss "organizations" It's unclear what a "culturally appropriate" option would be for individuals, considering every identity 79 needs to be vetted to the appropriate assurance level. 20 typographical error 40 typographical error 40 typographical error 40 typographical error 41 typographical error 42 typographical error 43 typographical error 44 typographical error 45 typographical error 46 typographical error 47 typographical error 48 typographical error 49 typographical error 40 typographical error	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party"
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.4 5 1 1 2.1 2.1	28 73 76 76 76 76 76 76 76 76 76 76 76 76 76	8 12 3 2463 6 2554 1 3 2 3 1 3 0 6	Il affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 24 users pick their second factor doesn't make sense. 2555 555 15 change agencies to organizations, as throughout this section you discuss "organizations" lt's unclear what a "culturally appropriate" option would be for individuals, considering every identity needs to be vetted to the appropriate assurance level. 16 typographical error 16 typographical error 17 typographical error 18 typographical error 19 typographical error 10 typographical error 19 typographical error 10 typographical error 10 typographical error 10 t	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party"
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.4 5 1 1 2.1 2.1	28 73 76 76 76 76 76 76 76 76 76 76 76 76 76	8 12 3 2463 6 2554 1 3 2 3 1 3 0 6	11 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. 16 enerally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 17 users pick their second factor doesn't make sense. 18 change agencies to organizations, as throughout this section you discuss "organizations" 18 it's unclear what a "culturally appropriate" option would be for individuals, considering every identity 19 needs to be vetted to the appropriate assurance level. 10 typographical error 10 typographical error 11 typographical error 12 typographical error 13 typographical error 14 typographical error 15 typographical error 16 typographical error 16 typographical error 17 typographical error 18 typographical error 18 typographical error 19 typographical error 19 typographical error 19 typographical error 20 typographical error 21 typographical error 22 typographical error 23 typographical error 24 typographical error 25 typographical error 26 typographical error 27 typographical error 28 typographical error 29 typographical error 20 typographical error 21 typographical error 22 typographical error 23 typographical error 24 typographical error 25 typographical error 26 typographical error 27 typographical error 28 typographical error 29 typographical error 20 typographical error 21 typographical error 22 typographical error 23 typographical error 24 typographical error 25 typographical error 2	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party"
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.4 5 1 1 2.1 2.1	28 73 76 76 76 76 76 76 76 76 76 76 76 76 76	8 12 3 2463 6 2554 1 3 2 3 1 3 0 6	11 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing users pick their second factor doesn't make sense. 2555 change agencies to organizations, as throughout this section you discuss "organizations" It's unclear what a "culturally appropriate" option would be for individuals, considering every identity 10 reads to be vetted to the appropriate assurance level. 11 typographical error 12 typographical error 13 typographical error 14 typographical error 15 typographical error 16 typographical error 16 typographical error 17 while CSPs absolutely must help their RP clients with risk assessments and the DIRM process, requiring them to also create a DIRM is excessive work. While there are many paths to get to IAL2, alongside many risks and exceptions process, ultimately the onerous is on the RP to understand the CSP's process, ask for enhancements, and accept the risk obtained from the original process alongside the enhancements.	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party"
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.2 5 1 1 2.1 2.1 2.1	28 73 76 76 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	8 13 3 2463 6 2554 1 3 2 3 1 3 0 0 0	111 affirmatively decided to synch and remove its device-bound status 116 100 attempts is very high; suggest reducing the attempts. 117 Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 118 Jesers pick their second factor doesn't make sense. 119 Change agencies to organizations, as throughout this section you discuss "organizations" 118 It's unclear what a "culturally appropriate" option would be for individuals, considering every identity needs to be vetted to the appropriate assurance level. 119 Jesers pick their second factor doesn't make sense. 110 Jesers pick their second factor doesn't make sense. 110 Jesers pick their second factor what is considering every identity needs to be vetted to the appropriate assurance level. 110 Jesers pick their second factor doesn't bypographical error typographical error 111 Jesers pick pick pick pick pick pick pick pick	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party" Remove requirements for CSPs to create DIRMs; keep the requirement to aid RPs in creating their DIRMs
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.4 5 1 1 2.1 2.1	28 73 76 76 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	8 13 3 2463 6 2554 1 3 2 3 1 3 0 0 0	11 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. 16 enerally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 17 users pick their second factor doesn't make sense. 18 change agencies to organizations, as throughout this section you discuss "organizations" 18 it's unclear what a "culturally appropriate" option would be for individuals, considering every identity 19 needs to be vetted to the appropriate assurance level. 10 typographical error 10 typographical error 10 typographical error 11 typographical error 12 typographical error 13 typographical error 14 typographical error 15 typographical error 16 typographical error 16 typographical error 17 typographical error 18 typographical error 18 typographical error 19 typographical error 19 typographical error 19 typographical error 20 typographical error 20 typographical error 21 typographical error 22 typographical error 23 typographical error 24 typographical error 25 typographical error 26 typographical error 27 typographical error 28 typographical error 29 typographical error 20 typographical error 21 typographical error 22 typographical error 23 typographical error 24 typographical error 2	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party"
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.2 5 1 1 2.1 2.1 2.1	28 73 76 76 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	8 13 3 2463 6 2554 1 3 2 3 1 3 0 0 0	11 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing users pick their second factor doesn't make sense. 2555 change agencies to organizations, as throughout this section you discuss "organizations" It's unclear what a "culturally appropriate" option would be for individuals, considering every identity 79 needs to be vetted to the appropriate assurance level. 20 typographical error 21 typographical error 22 typographical error 23 typographical error 24 Utypographical error 25 typographical error 26 While CSPs absolutely must help their RP clients with risk assessments and the DIRM process, requiring them to also create a DIRM is excessive work. While there are many paths to get to IAL2, alongside many risks and exceptions process, ultimately the onerous is on the RP to understand the CSP's process, ask for enhancements, and accept the risk obtained from the original process alongside the enhancements. 28 It's unclear what a "culturally responsive" communication alternative would be and whether that 8 description actually enhances this section of the guidelines 29 Scale of impact is a critical missing element from the user group discussion, which focuses exclusively	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party" Remove requirements for CSPs to create DIRMs; keep the requirement to aid RPs in creating their DIRMs
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.6 5 1 1 2.1 2.1 2.1	28 73 76 76 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	8 13 3 2463 6 2554 1 3 2 3 1 3 0 0 0	111 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. 16 Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 12	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party" Remove requirements for CSPs to create DIRMs; keep the requirement to aid RPs in creating their DIRMs than values transmitted in clear text or full attribute values
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.6 5 1 1 2.1 2.1 2.1	28 73 76 76 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	8 13 3 2463 6 2554 1 3 2 3 1 3 0 0 0	11 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing users pick their second factor doesn't make sense. 2555 change agencies to organizations, as throughout this section you discuss "organizations" It's unclear what a "culturally appropriate" option would be for individuals, considering every identity 79 needs to be vetted to the appropriate assurance level. 20 typographical error 21 typographical error 22 typographical error 23 typographical error 24 Utypographical error 25 typographical error 26 While CSPs absolutely must help their RP clients with risk assessments and the DIRM process, requiring them to also create a DIRM is excessive work. While there are many paths to get to IAL2, alongside many risks and exceptions process, ultimately the onerous is on the RP to understand the CSP's process, ask for enhancements, and accept the risk obtained from the original process alongside the enhancements. 28 It's unclear what a "culturally responsive" communication alternative would be and whether that 8 description actually enhances this section of the guidelines 29 Scale of impact is a critical missing element from the user group discussion, which focuses exclusively	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party" Remove requirements for CSPs to create DIRMs; keep the requirement to aid RPs in creating their DIRMs than values transmitted in clear text or full attribute values
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.6 5 1 1 2.1 2.1 2.1	28 73 76 76 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	8 13 3 2463 6 2554 1 3 2 3 1 3 0 0 0	111 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. 16 Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 12	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party" Remove requirements for CSPs to create DIRMs; keep the requirement to aid RPs in creating their DIRMs than values transmitted in clear text or full attribute values
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.6 5 1 1 2.1 2.1 2.1	28 73 76 76 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	8 13 3 2463 6 2554 1 3 2 3 1 3 0 0 0	111 affirmatively decided to synch and remove its device-bound status 112 100 attempts is very high; suggest reducing the attempts. 113 2100 attempts is very high; suggest reducing the attempts. 114 2100 attempts is very high; suggest reducing the attempts. 115 210 attempts is very high; suggest reducing the attempts. 116 210 attempts is very high; suggest reducing the attempts. 117 210 attempts is very high; suggest reducing the attempts. 118 210 attempts is very high; suggest reducing the attempts. 119 210 attempts is very high; suggest reducing the very identity its unclear what a "culturally appropriate" option would be for individuals, considering every identity in process to be vetted to the appropriate assurance level. 119 210 attempts in a considering every identity in process to be vetted to the appropriate assurance level. 110 210 210 210 210 210 210 210 210 210	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party" Remove requirements for CSPs to create DIRMs; keep the requirement to aid RPs in creating their DIRMs than values transmitted in clear text or full attribute values
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.6 5 1 1 2.1 2.1 2.1	28 73 76 76 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	8 13 3 2463 6 2554 1 3 2 3 1 3 0 0 0	111 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. 16 Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 12	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party" Remove requirements for CSPs to create DIRMs; keep the requirement to aid RPs in creating their DIRMs than values transmitted in clear text or full attribute values
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.6 5 1 1 2.1 2.1 2.1	28 73 76 76 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	8 13 3 2463 6 2554 1 3 2 3 1 3 0 0 0	111 affirmatively decided to synch and remove its device-bound status 112 15 100 attempts is very high, suggest reducing the attempts. 113 15 100 attempts is very high, suggest reducing the attempts. 114 21 100 attempts is very high, suggest reducing the attempts. 115 100 attempts is very high, suggest reducing the attempts. 115 100 attempts is very high, suggest reducing the attempts. 116 110 attempts is very high, suggest reducing the attempts. 117 110 attempts is very high, suggest reducing the very side of the pairing, therefore in an "ideal" situation allowing users pick their second factor doesn't make sense. 117 110 attempts is very identity appropriate assurance level. 118 119 110 attempts is very identity appropriate assurance level. 119 110 attempts is very identity appropriate assurance level. 110 110 attempts is very identity appropriate assurance level. 110 110 110 attempts in a considering every identity in page attempts in a considering every identity in a considering	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party" Remove requirements for CSPs to create DIRMs; keep the requirement to aid RPs in creating their DIRMs than values transmitted in clear text or full attribute values
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.4 5 1 1 2.1 2.1 2.1 3.1	288	8 13 3 2463 6 2554 1 3 2 3 1 3 0 0 0	11 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. 16 enerally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 17 users pick their second factor doesn't make sense. 18 change agencies to organizations, as throughout this section you discuss "organizations" 18 it's unclear what a "culturally appropriate" option would be for individuals, considering every identity 19 needs to be vetted to the appropriate assurance level. 19 typographical error 10 typographical error 10 typographical error 10 typographical error 10 typographical error 11 typographical error 12 typographical error 13 typographical error 14 typographical error 15 typographical error 16 typographical error 16 typographical error 17 typographical error 18 typographical error 19 typographical error 10 typographical error 11 typographical error 12 typographical error 13 typographical error 14 typographical error 14 typographical error 15 typographical error 16 typographical error 16 typographical error 17 typographical error 18 typographical error 19 typographical error 20 typographical error 21 typographical error 22 typographical error 23 typographical error 24 typographical error 25 typographical error 26 typographical error 27 typographical error 28 typographical error 29 typographical error 20 typographical error 21 typographical error 21 typographical error 2	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party" Remove requirements for CSPs to create DIRMs; keep the requirement to aid RPs in creating their DIRMs than values transmitted in clear text or full attribute values
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.2 1 1 2.1 2.1 2.1 3.3	288	1 1 2 2 3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	111 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. 16 Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 12	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party" Remove requirements for CSPs to create DIRMs; keep the requirement to aid RPs in creating their DIRMs than values transmitted in clear text or full attribute values
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.4 5 1 1 2.1 2.1 2.1 3.1	288	1 1 2 2 3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	111 affirmatively decided to synch and remove its device-bound status 126 100 attempts is very high, suggest reducing the attempts. 127 Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 128 users pick their second factor doesn't make sense. 128 Change agencies to organizations, as throughout this section you discuss "organizations" 129 It's unclear what a "culturally appropriate" option would be for individuals, considering every identity 120 needs to be vetted to the appropriate assurance level. 121 typographical error 122 typographical error 123 typographical error 124 typographical error 125 typographical error 126 typographical error 127 While CSPs absolutely must help their RP clients with risk assessments and the DIRM process, requiring them to also create a DIRM is excessive work. While there are many paths to get to IAL2, alongside many risks and exceptions process, ultimately the onerous is on the RP to understand the CSP's process, ask for enhancements, and accept the risk obtained from the original process alongside the enhancements. 128 unclear what a "culturally responsive" communication alternative would be and whether that description actually enhances this section of the guidelines 129 Scale of impact is a critical missing element from the user group discussion, which focuses exclusively on role. For example, the successful impersonation of a tax preparer who has a handful of small business as clients will not have the same impact as the successful impersonation of a tax preparer who has a handful of small business as clients will not have the same impact as the successful impersonation of a tax preparer who has a handful of small business as clients will not have the same impact as the successful impersonation of a tax preparer who has a handful of small business as clients will not have the same impact as the successful impersonation of a tax preparer who has a handful of small business as clients will not have the same impact as the succ	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party" Remove requirements for CSPs to create DIRMs; keep the requirement to aid RPs in creating their DIRMs than values transmitted in clear text or full attribute values
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.2 1 1 2.1 2.1 2.1 3.3	288	1 1 2 2 3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	111 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. 26 Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 27 28 users pick their second factor doesn't make sense. 28 users pick their second factor doesn't make sense. 29 tange agencies to organizations, as throughout this section you discuss "organizations" 18 unclear what a "culturally appropriate" option would be for individuals, considering every identity needs to be vetted to the appropriate assurance level. 20 typographical error 21 typographical error 22 typographical error 23 typographical error 24 typographical error 25 typographical error 26 typographical error 27 typographical error 28 the Socreate a DIRM is excessive work. While there are many paths to get to IAL2, alongside many risks and exceptions process, ultimately the onerous is on the RP to understand the CSP's process, ask for enhancements, and accept the risk obtained from the original process alongside the enhancements. 28 tris unclear what a "culturally responsive" communication alternative would be and whether that the description actually enhances this section of the guidelines Scale of impact is a critical missing element from the user group discussion, which focuses exclusively on role. For example, the successful impersonation of a tax preparer who has a handful of small business as clients will not have the same impact as the successful impersonation of a tax preparer who handles the accounts for Walmart and Wells Fargo. Similarly, the impacts on the organization/application itself also needs to be assessed, as well as any other impacted entities. For example, beneficiaries, but should nevertheless be considered since their information would be exposed if a DI error were to occur. 20 typographical error	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party" Remove requirements for CSPs to create DIRMs; keep the requirement to aid RPs in creating their DIRMs than values transmitted in clear text or full attribute values
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.2 1 1 2.1 2.1 2.1 3.3	288	1 1 2 2 3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	111 affirmatively decided to synch and remove its device-bound status 126 100 attempts is very high, suggest reducing the attempts. 127 Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 128 users pick their second factor doesn't make sense. 128 Change agencies to organizations, as throughout this section you discuss "organizations" 129 It's unclear what a "culturally appropriate" option would be for individuals, considering every identity 120 needs to be vetted to the appropriate assurance level. 121 typographical error 122 typographical error 123 typographical error 124 typographical error 125 typographical error 126 typographical error 127 While CSPs absolutely must help their RP clients with risk assessments and the DIRM process, requiring them to also create a DIRM is excessive work. While there are many paths to get to IAL2, alongside many risks and exceptions process, ultimately the onerous is on the RP to understand the CSP's process, ask for enhancements, and accept the risk obtained from the original process alongside the enhancements. 128 unclear what a "culturally responsive" communication alternative would be and whether that description actually enhances this section of the guidelines 129 Scale of impact is a critical missing element from the user group discussion, which focuses exclusively on role. For example, the successful impersonation of a tax preparer who has a handful of small business as clients will not have the same impact as the successful impersonation of a tax preparer who has a handful of small business as clients will not have the same impact as the successful impersonation of a tax preparer who has a handful of small business as clients will not have the same impact as the successful impersonation of a tax preparer who has a handful of small business as clients will not have the same impact as the successful impersonation of a tax preparer who has a handful of small business as clients will not have the same impact as the succ	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party" Remove requirements for CSPs to create DIRMs; keep the requirement to aid RPs in creating their DIRMs than values transmitted in clear text or full attribute values
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.2 1 1 2.1 2.1 2.1 3.3	288	1 1 2 2 3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	111 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. 26 Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 27 28 users pick their second factor doesn't make sense. 28 users pick their second factor doesn't make sense. 29 tange agencies to organizations, as throughout this section you discuss "organizations" 18 unclear what a "culturally appropriate" option would be for individuals, considering every identity needs to be vetted to the appropriate assurance level. 20 typographical error 21 typographical error 22 typographical error 23 typographical error 24 typographical error 25 typographical error 26 typographical error 27 typographical error 28 the Socreate a DIRM is excessive work. While there are many paths to get to IAL2, alongside many risks and exceptions process, ultimately the onerous is on the RP to understand the CSP's process, ask for enhancements, and accept the risk obtained from the original process alongside the enhancements. 28 tris unclear what a "culturally responsive" communication alternative would be and whether that the description actually enhances this section of the guidelines Scale of impact is a critical missing element from the user group discussion, which focuses exclusively on role. For example, the successful impersonation of a tax preparer who has a handful of small business as clients will not have the same impact as the successful impersonation of a tax preparer who handles the accounts for Walmart and Wells Fargo. Similarly, the impacts on the organization/application itself also needs to be assessed, as well as any other impacted entities. For example, beneficiaries, but should nevertheless be considered since their information would be exposed if a DI error were to occur. 20 typographical error	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party" Remove requirements for CSPs to create DIRMs; keep the requirement to aid RPs in creating their DIRMs than values transmitted in clear text or full attribute values
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.2 1 1 2.1 2.1 2.1 3.3	288	1 1 2 2 3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	111 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high, suggest reducing the attempts. 16 200 attempts is very high, suggest reducing the attempts. 17 3 24 description actually appropriate assurance level. 18 2555 18 2555 28 2555 28 2555 28 2555 28 2556 28 2556 28 2556 28 2556 28 2557 29 2557 29 2	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party" Remove requirements for CSPs to create DIRMs; keep the requirement to aid RPs in creating their DIRMs than values transmitted in clear text or full attribute values
	63B 63B 63B 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	3.2.2 8.4 5.5 1 1 2.1 2.1 2.1 3.1 3.1	288	1 1 2 2 3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	111 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high; suggest reducing the attempts. 16 Generally biometrics will unlock a private/public key pairing, therefore in an "ideal" situation allowing 17 24 users pick their second factor doesn't make sense. 18 2555 19 change agencies to organizations, as throughout this section you discuss "organizations" 18 the unclear what a "culturally appropriate" option would be for individuals, considering every identity needs to be vetted to the appropriate assurance level. 16 typographical error 17 typographical error 18 typographical error 19 typographical error 20 typographical error 21 typographical error 22 typographical error 23 typographical error 24 typographical error 25 typographical error 26 typographical error 26 typographical error 27 typographical error 28 typographical error 29 typographical error 20 typographical error 21 tr's unclear what a "culturally responsive" communication alternative would be and whether that the enhancements. 20 tr's unclear what a "culturally responsive" communication alternative would be and whether that the description actually enhances this section of the guidelines 20 Scale of impact is a critical missing element from the user group discussion, which focuses exclusively on role. For example, the successful impersonation of a tax preparer who has a handful of small business as clients will not have the same impact as the successful impersonation of a tax preparer who has a handful of small business as clients will not have the same impact as the successful impersonation of a tax preparer who has a handful of small business as clients will not have the same impact as the successful impersonation of a tax preparer who has a handful of small b	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party" Remove requirements for CSPs to create DIRMs; keep the requirement to aid RPs in creating their DIRMs than values transmitted in clear text or full attribute values Update impact review "At a minimum, agencies shall document all impacted entities when conducting their impact"
	63B 63B 63B 63-Base	3.2.2 8.2 1 1 2.1 2.1 2.1 3.3	288	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	111 affirmatively decided to synch and remove its device-bound status 16 100 attempts is very high, suggest reducing the attempts. 16 200 attempts is very high, suggest reducing the attempts. 17 3 24 description actually appropriate assurance level. 18 2555 18 2555 28 2555 28 2555 28 2555 28 2556 28 2556 28 2556 28 2556 28 2557 29 2557 29 2	Suggest reducing the amount of attempts to below 100. suggest removing the sentence or noting that most uses of biometrics will be to unlock a cryptographic certificate. remove reference to sexual exploitation, as it is a type of trauma. change agencies to organizations Remove "culturally appropriate" reference. Change "considerations and organization "to considerations an organization" make identity provider lower case Remove the hyphen after the em-dash should be "relying party" not "relying party" Remove requirements for CSPs to create DIRMs; keep the requirement to aid RPs in creating their DIRMs than values transmitted in clear text or full attribute values

		_	_		
				It would be impossible for a CSP to perform risk assessments on user groups, given a particular user can	
				be a part of different types of user groups in different RPs. For example, a police officer might have	
				administrative access within their own organization, read only rights to law enforcement sensitive	
				documents in other, federated organizations, the need for benefits for IRS/SSA, a Global Entry	
				participant for State and TSA, as well as a FOIA requester at GSA. This user's changing groups would	
63-Base	3.2.3	22	1200	-12 create different levels of risk, all of which each individual RP needs to accept or decline.	Demonstrating the CCDs to exact DIDMs lean the requirement to aid DDs in exacting their DIDMs
63-Base	3.2.3	33	1290		Remove requirements for CSPs to create DIRMs; keep the requirement to aid RPs in creating their DIRMs
				How does an organization come to an "overall impact score" for each user group? What goes into the	
63-Base	3.2.4	34	1 1	321 score? How does the score translate to assurance levels?	Clarify what an impact score is and how to calculate it, or remove it from Base.
				"initially assessed xALs" are required in a DIAS, which is required to be created by a CSP. This	
				requirement doesn't make sense for CSPs, as CSPs should not be assessing what the xAL should be for a	
				given RP. While the CSP can help the RP create the xAL assessment, CSPs must create workflows to	
				meet their customer's needs, which means their assessed xALs, tailored xALs, and compensating	
63-Base	3.4.4	44	1	controls will be determined by their customers - the RPs - not by the CSPs themselves.	Remove requirements for CSPs to create aDIAS; keep the requirement to aid RPs in creating their DIAS
ĺ		1	1		
63-Base	3.8	50	1	The term "biased outputs" when describing AI/ML results is biased against the technology.	change to "disparate outcomes or outputs," as the adjective "disparate" encompasses the issue - which is that algorithms that are not v
				The RP is the customer, and the CSP is a shared/managed service that is providing the customer with	
				services, including data about potential fraudulent activities, extensive activity logs, etc., to provide the	
63-Base	3.7			-18 RP with a broader, more holistic view of its cybersecurity landscape and threats.	change shall to should
63-Base	2.1	. 10)	46 you'll want an apostrophe here	relying' party
				the system might already be implemented but it's risks are still part of DIRM. This will reflect DIRM as a	
63-Base	3	22	,	322 continuous process. Consider flowthrough changes.	Replace "might be addressed" with "addressed." Replace "to be implemented" with "itself"
			1		ment de dedicased with dedicased. Replace to be implemented with itself
				The first dimension is defined earlier as "risks to the online service that might be addressed by an	replace might be addressed. With dadressed, replace to be imprenented. With risen
	2.3			The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is	
63-Base	3.2	28		The first dimension is defined earlier as "risks to the online service that might be addressed by an	remove the parenthetical, replace "and seeks to identify" with "by identifying"
	3.2			The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is 27 consistent	
	3.2			The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not	
	3.2			The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is 27 consistent	
	3.2			The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is	
	3.2			The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is 27 consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not	
63-Base				The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to	
	3.2 general			The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion	
63-Base				The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there	
63-Base				The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is 27 consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and	remove the parenthetical, replace "and seeks to identify" with "by identifying"
63-Base				The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there	remove the parenthetical, replace "and seeks to identify" with "by identifying"
63-Base				The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is 27 consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and	remove the parenthetical, replace "and seeks to identify" with "by identifying"
63-Base			3 1	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency,	remove the parenthetical, replace "and seeks to identify" with "by identifying"
63-Base 63-Base	general	28	3 1	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is 27 consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, organization, and RP seem interchangeable, which adds confusion	remove the parenthetical, replace "and seeks to identify" with "by identifying"
63-Base 63-Base	general	28	3 1	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, 56 organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think	remove the parenthetical, replace "and seeks to identify" with "by identifying"
63-Base 63-Base	general	28	9 1	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "R9s shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, 550 organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there	remove the parenthetical, replace "and seeks to identify" with "by identifying" Change "organizations" to "RPs"
63-Base 63-Base 63-Base	general 3.2.1	28	1 1	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is 27 consistent In all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least it most cases. There are other areas in which agency, organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there	remove the parenthetical, replace "and seeks to identify" with "by identifying" Change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conduct
63-Base 63-Base	general	28	1 1	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "R9s shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, 550 organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there	remove the parenthetical, replace "and seeks to identify" with "by identifying" Change "organizations" to "RPs"
63-Base 63-Base 63-Base	general 3.2.1	28 29 35 38	3 1 3 1 3 1	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, 65 organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there 158 would be an IAL0 so it can be recorded properly when agencies do assessments	remove the parenthetical, replace "and seeks to identify" with "by identifying" Change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conduc
63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	general 3.2.1 3.3.2.1 3.3.3.1	29 35 38 40	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "R9s shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, 56 organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there 158 would be an IAL0 so it can be recorded properly when agencies do assessments 14 holds suggests possession and not existence.	remove the parenthetical, replace "and seeks to identify" with "by identifying" Change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conductionage "holds" to "is"
63-Base 63-Base 63-Base 63-Base	general 3.2.1 3.3.2.1 3.3.3.1	29 35 38 40	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there would be an IAL0 so it can be recorded properly when agencies do assessments would be an IAL0 so it can be recorded properly when agencies do assessments move footnote marker to end of sentence	remove the parenthetical, replace "and seeks to identify" with "by identifying" Change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conduct change "holds" to "is"
63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	general 3.2.1 3.3.2.1 3.3.3.1	29 35 38 40	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, 65 organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there 58 would be an IAL0 so it can be recorded properly when agencies do assessments Another suggests possession and not existence. The proof of the pare underserved now, there should be a focus on them The proof of the pare underserved now, there should be a focus on them The proof of the pare underserved now, there should be a focus on them The proof of the pare of the parent of the sentence of the proof of sentence The proof of the parent proof of sentence The proof of the parent proof of the sentence of the proof of the parent p	remove the parenthetical, replace "and seeks to identify" with "by identifying" Change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conductionage "holds" to "is"
63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	general 3.2.1 3.3.2.1 3.3.3.1	29 35 38 40	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "R9s shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, 56 organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there 58 would be an IAL0 so it can be recorded properly when agencies do assessments 34 holds suggests possession and not existence. 59 if they are underserved now, there should be a focus on them 100 move footnote marker to end of sentence 50me types of impacts are not easily captured by the listed impact categories, such as a loss of Medicare coverage. Such a loss of coverage can lead to financial loss, endanger someone's health, and	remove the parenthetical, replace "and seeks to identify" with "by identifying" Change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conductionage "holds" to "is"
63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	general 3.2.1 3.3.2.1 3.3.3.1	29 35 38 40	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, 65 organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there 58 would be an IAL0 so it can be recorded properly when agencies do assessments Another suggests possession and not existence. The proof of the pare underserved now, there should be a focus on them The proof of the pare underserved now, there should be a focus on them The proof of the pare underserved now, there should be a focus on them The proof of the pare of the parent of the sentence of the proof of sentence The proof of the parent proof of sentence The proof of the parent proof of the sentence of the proof of the parent p	remove the parenthetical, replace "and seeks to identify" with "by identifying" Change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conductionage "holds" to "is"
63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	general 3.2.1 3.3.2.1 3.3.3.1	29 35 38 40	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there would be an IAL0 so it can be recorded properly when agencies do assessments Modis suggests possession and not existence. Modis suggests possession and not existence. Modis of they are underserved now, there should be a focus on them move confusion, and a loss of coverage can lead to financial loss, endanger someone's health, and lead to extreme stress at a time when someone may be suffering from serious health conditions.	remove the parenthetical, replace "and seeks to identify" with "by identifying" Change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conductionage "holds" to "is"
63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	general 3.2.1 3.3.2.1 3.3.3.1 3.4	25 35 38 40 40	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, 56 organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there 58 would be an IAL0 so it can be recorded properly when agencies do assessments Another suggests possession and not existence. They are underserved now, there should be a focus on them move footnote marker to end of sentence Some types of impacts are not easily captured by the listed impact categories, such as a loss of Medicare coverage. Such a loss of coverage can lead to financial loss, endanger someone's health, and lead to extreme stress at a time when someone may be suffering from serious health conditions. Delays in receiving disability benefits can also lead to a cascade of negative consequences that can be	remove the parenthetical, replace "and seeks to identify" with "by identifying" Change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conductionage "holds" to "is" remove historically
63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	general 3.2.1 3.3.2.1 3.3.3.1	25 35 38 40 40	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "R9s shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, so aganization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there also holds suggests possession and not existence. if if they are underserved now, there should be a focus on them move footnote marker to end of sentence Some types of impacts are not easily captured by the listed impact categories, such as a loss of Medicare coverage. Such a loss of coverage can lead to financial loss, endanger someone's health, and lead to extreme stress at a time when someone may be suffering from serious health conditions. Delays in receiving disability benefits can also lead to a cascade of negative consequences that can be incredibly detrimental and hard to recover from.	remove the parenthetical, replace "and seeks to identify" with "by identifying" Change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conductionage "holds" to "is"
63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	general 3.2.1 3.3.2.1 3.3.3.1 3.4	25 35 38 40 40	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, 556 organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there would be an IAL0 so it can be recorded properly when agencies do assessments 334 holds suggests possession and not existence. 356 organization and RP seem interchangeable, which adds confusion. 357 if they are underserved now, there should be a focus on them move footnote marker to end of sentence. 358 Some types of impacts are not easily captured by the listed impact categories, such as a loss of Medicare coverage. Such a loss of coverage can lead to a cascade of negative consequences that can be lead to extreme stress at a time when someone may be suffering from serious health conditions. Delays in receiving disability benef	remove the parenthetical, replace "and seeks to identify" with "by identifying" Change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conduct change "holds" to "is" remove historically
63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	general 3.2.1 3.3.2.1 3.3.3.1 3.4 3.2.2	25 35 38 40 40	1206	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, 65 organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there would be an IAL0 so it can be recorded properly when agencies do assessments and IAL0 so it can be recorded properly when agencies do assessments. In they are underserved now, there should be a focus on them move footnote marker to end of sentence. Some types of impacts are not easily captured by the listed impact categories, such as a loss of Medicare coverage. Such a loss of coverage can lead to financial loss, endanger someone's health, and lead to extreme stress at a time when someone may be suffering from serious health conditions. Delays in receiving disability benefits can also lead to a cascade of negative consequences that	remove the parenthetical, replace "and seeks to identify" with "by identifying" Change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conductionage "holds" to "is" remove historically Consider adding an additional Impact Category such as "Quality of Life Degradation"
63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	general 3.2.1 3.3.2.1 3.3.3.1 3.4	25 35 38 40 40	1206	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, 556 organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there would be an IAL0 so it can be recorded properly when agencies do assessments 334 holds suggests possession and not existence. 356 organization and RP seem interchangeable, which adds confusion. 357 if they are underserved now, there should be a focus on them move footnote marker to end of sentence. 358 Some types of impacts are not easily captured by the listed impact categories, such as a loss of Medicare coverage. Such a loss of coverage can lead to a cascade of negative consequences that can be lead to extreme stress at a time when someone may be suffering from serious health conditions. Delays in receiving disability benef	remove the parenthetical, replace "and seeks to identify" with "by identifying" Change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conductionage "holds" to "is" remove historically
63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	general 3.2.1 3.3.2.1 3.3.3.1 3.4 3.2.2	25 35 38 40 40	1206	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, 65 organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there would be an IAL0 so it can be recorded properly when agencies do assessments and IAL0 so it can be recorded properly when agencies do assessments. In they are underserved now, there should be a focus on them move footnote marker to end of sentence. Some types of impacts are not easily captured by the listed impact categories, such as a loss of Medicare coverage. Such a loss of coverage can lead to financial loss, endanger someone's health, and lead to extreme stress at a time when someone may be suffering from serious health conditions. Delays in receiving disability benefits can also lead to a cascade of negative consequences that	remove the parenthetical, replace "and seeks to identify" with "by identifying" Change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conductionage "holds" to "is" remove historically Consider adding an additional Impact Category such as "Quality of Life Degradation"
63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	general 3.2.1 3.3.2.1 3.3.3.1 3.4 3.2.2	25 35 383 40 40 40	1206 2 1256	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, 65 organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there would be an IAL0 so it can be recorded properly when agencies do assessments and IAL0 so it can be recorded properly when agencies do assessments. In they are underserved now, there should be a focus on them move footnote marker to end of sentence. Some types of impacts are not easily captured by the listed impact categories, such as a loss of Medicare coverage. Such a loss of coverage can lead to financial loss, endanger someone's health, and lead to extreme stress at a time when someone may be suffering from serious health conditions. Delays in receiving disability benefits can also lead to a cascade of negative consequences that	remove the parenthetical, replace "and seeks to identify" with "by identifying" Change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conductionage "holds" to "is" remove historically Consider adding an additional Impact Category such as "Quality of Life Degradation"
63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	general 3.2.1 3.3.2.1 3.3.3.1 3.4 3.2.2	25 35 383 40 40 40	1206 2 1256	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, 556 organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there would be an IAL0 so it can be recorded properly when agencies do assessments 158 would be an IAL0 so it can be recorded properly when agencies do assessments 159 if they are underserved now, there should be a focus on them 150 move footnote marker to end of sentence 151 Some types of impacts are not easily captured by the listed impact categories, such as a loss of Medicare coverage. Such a loss of coverage can lead to also should be a focus on them 150 if they are underserved now, there should be a focus on them 151 move footnote marker to end of sentence 152 incredibly detrimental and hard to recover from. 153 While it is	remove the parenthetical, replace "and seeks to identify" with "by identifying" Change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conductionage "holds" to "is" remove historically Consider adding an additional Impact Category such as "Quality of Life Degradation" Remove "including mental health treatment". Update the guidance to realistically reflect the limited options RPs will have when they are using an external CSP such as Login.gov.
63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	general 3.2.1 3.3.2.1 3.3.3.1 3.4 3.2.2	25 35 383 40 40 40	1206 2 1256	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "Res shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, 550 organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there 38 would be an IAL0 so it can be recorded properly when agencies do assessments 39 if they are underserved now, there should be a focus on them 30 if they are underserved now, there should be a focus on them 30 move footnote marker to end of sentence 30 move footnote marke	remove the parenthetical, replace "and seeks to identify" with "by identifying" Change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conductive to "is" remove historically Consider adding an additional Impact Category such as "Quality of Life Degradation" Remove "including mental health treatment". Update the guidance to realistically reflect the limited options RPs will have when they are using an external CSP such as Login.gov. Recommend replacing: "The robustness of the authentication process itself, and the binding between an authenticator and a specific
63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	general 3.2.1 3.3.2.1 3.3.3.1 3.4 3.2.2	25 25 35 36 40 40 40 30-31	1206	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, 556 organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there 158 would be an IAL0 so it can be recorded properly when agencies do assessments 34 holds suggests possession and not existence. 55me types of impacts are not easily captured by the listed impact categories, such as a loss of Medicare coverage. Such a loss of coverage can lead to financial loss, endanger someone's health, and lead to extreme stress at a time when someone may be suffering from serious health conditions. Delays in receiving disability benefits can also lead to a cascade of negative consequences that can be 10 incredibly detrimental and hard to recover from. While it is possible to anticipate the types of medical t	remove the parenthetical, replace "and seeks to identify" with "by identifying" Change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conductionage "holds" to "is" remove historically Consider adding an additional Impact Category such as "Quality of Life Degradation" Remove "including mental health treatment". Update the guidance to realistically reflect the limited options RPs will have when they are using an external CSP such as Logingov. Recommend replacing: "The robustness of the authentication process itself, and the binding between an authenticator and a specific individual's identifier." with "the level of assurance that the claimant is the same individual to whom the credential or authenticator was
63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	general 3.2.1 3.3.2.1 3.3.3.1 3.4 3.2.2 3.2.2	25 35 38 40 40 40 30-31 32 34	1206 2 1256 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "Res shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there should be an IALO so it can be recorded properly when agencies do assessments 363 holds suggests possession and not existence. 369 If they are underserved now, there should be a focus on them 361 move footnote marker to end of sentence 362 some types of impacts are not easily captured by the listed impact categories, such as a loss of Medicare coverage. Such a loss of coverage can lead to financial loss, endanger someone's health, and lead to extreme stress at a time when someone may be suffering from serious health conditions. 363 Delays in receiving disability benefits can also lead to a cascade of negative consequences that ca	change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conductive change "holds" to "is" remove historically Consider adding an additional Impact Category such as "Quality of Life Degradation" Remove "including mental health treatment". Update the guidance to realistically reflect the limited options RPs will have when they are using an external CSP such as Login.gov. Recommend replacing: "The robustness of the authentication process itself, and the binding between an authenticator and a specific individual's identifier." with "the level of assurance that the claimant is the same individual to whom the credential or authenticator wa issued."
63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	general 3.2.1 3.3.2.1 3.3.3.1 3.4 3.2.2	25 35 38 40 40 40 30-31 32 34	1206 2 1256 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "RPs shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, 556 organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there 158 would be an IAL0 so it can be recorded properly when agencies do assessments 34 holds suggests possession and not existence. 55me types of impacts are not easily captured by the listed impact categories, such as a loss of Medicare coverage. Such a loss of coverage can lead to financial loss, endanger someone's health, and lead to extreme stress at a time when someone may be suffering from serious health conditions. Delays in receiving disability benefits can also lead to a cascade of negative consequences that can be 10 incredibly detrimental and hard to recover from. While it is possible to anticipate the types of medical t	remove the parenthetical, replace "and seeks to identify" with "by identifying" Change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conduct change "holds" to "is" remove historically Consider adding an additional Impact Category such as "Quality of Life Degradation" Remove "including mental health treatment". Update the guidance to realistically reflect the limited options RPs will have when they are using an external CSP such as Login.gov. Recommend replacing: "The robustness of the authentication process itself, and the binding between an authenticator and a specific individual's identifier." with "the level of assurance that the claimant is the same individual to whom the credential or authenticator was
63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	general 3.2.1 3.3.2.1 3.3.3.1 3.4 3.2.2 3.2.2	25 35 38 40 40 40 30-31 32 34	1206 2 1256 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "Res shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there should be an IALO so it can be recorded properly when agencies do assessments 363 holds suggests possession and not existence. 369 If they are underserved now, there should be a focus on them 361 move footnote marker to end of sentence 362 some types of impacts are not easily captured by the listed impact categories, such as a loss of Medicare coverage. Such a loss of coverage can lead to financial loss, endanger someone's health, and lead to extreme stress at a time when someone may be suffering from serious health conditions. 363 Delays in receiving disability benefits can also lead to a cascade of negative consequences that ca	Change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conduct change "holds" to "is" remove historically Consider adding an additional Impact Category such as "Quality of Life Degradation" Remove "including mental health treatment". Update the guidance to realistically reflect the limited options RPs will have when they are using an external CSP such as Login.gov. Recommend replacing: "The robustness of the authentication process itself, and the binding between an authenticator and a specific individual's identifier." with "the level of assurance that the claimant is the same individual to whom the credential or authenticator was issued."
63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base 63-Base	general 3.2.1 3.3.2.1 3.3.3.1 3.4 3.2.2 3.2.2	25 35 36 40 40 40 30-31 32 34 34 34 36	1200 1200 1200 1200 1200 1200	The first dimension is defined earlier as "risks to the online service that might be addressed by an identity system." The parenthetical suggests something else, though the rest of the sentence is consistent in all volumes, there is too much passive voice. Leaving out the subject of a sentence often does not impact the interpretation, but can lead to confusion, particularly when assigning responsibility. This is especially important near normative statements. For instance, some sections and subsections do not clearly state the actor. 63-4 Section 3 is a good example where the document would be well served to state "Res shall" or the like at the start of each subsection to eliminate potential confusion prior sections have mentioned RPs as the actor here. This one says "organizations." I don't think there is a different actor here; the RP is best suited for this activity. Ditto line 1218, 1312, 1320, 1323, and others. If there is a value in saying organizations and not RPs, make it clear at the beginning of section 3 that RPs are responsible for this, at least in most cases. There are other areas in which agency, organization, and RP seem interchangeable, which adds confusion Given the significance of the change, call out that no identity proofing is no longer IAL1. I don't think you have to state that it's a "change" but mentioned it explicitly to remove confusion. Ideally there should be an IALO so it can be recorded properly when agencies do assessments 363 holds suggests possession and not existence. 369 If they are underserved now, there should be a focus on them 361 move footnote marker to end of sentence 362 some types of impacts are not easily captured by the listed impact categories, such as a loss of Medicare coverage. Such a loss of coverage can lead to financial loss, endanger someone's health, and lead to extreme stress at a time when someone may be suffering from serious health conditions. 363 Delays in receiving disability benefits can also lead to a cascade of negative consequences that ca	Change "organizations" to "RPs" Add a bullet: No identity proofing: Knowledge of the user's real-life identity is not needed and no identity proofing activities are conduct change "holds" to "is" remove historically Consider adding an additional impact Category such as "Quality of Life Degradation" Remove "including mental health treatment". Update the guidance to realistically reflect the limited options RPs will have when they are using an external CSP such as Login.gov. Recommend replacing: "The robustness of the authentication process itself, and the binding between an authenticator and a specific individual's identifier." with "the level of assurance that the claimant is the same individual to whom the credential or authenticator was issued." Change "Support multifactor authentication" to "Requires multifactor authentication" or "Enforces"

	1	- 1		т -		Marginalized and historically undersayed nanulations are those which are often most soverely	
						Marginalized and historically underserved populations are those which are often most severely impacted by DI errors that can result in consequences such as stolen benefits or identity theft. Yet the	
						tailoring instructions direct agencies to focus exclusively on frustrations with the DI controls	Add: "These considerations should be weighed against the disproportionate impacts that may be experienced by these same populations
63-Base		3.4	40	150	507-15	themselves.	in the event of a DI error."
63-Base		3.4				Keeping individuals safe is also critical.	Change to "while supporting security, equity, privacy, and usability for individuals."
							Extend the final sentence: "The intent of this assessment is to mitigate
							potential impacts on marginalized and historically underserved groups and limit
							disproportionate impacts from the requirements of the identity management
						Marginalized and historically underserved populations are those which are often most severely	functions while providing adequate protections against impacts of the fraud and impersonation that can occur when those functions
63-Base	3.4.1		42	+	1574	impacted by DI errors that can result in consequences such as stolen benefits or identity theft. There is a real risk that focusing exclusively on equity & accessibility will result in greater harms being	fail."
						done to vulnerable individuals whose money and data are then stolen due to a reduction in effective	Change to: "A primary purpose of continuous improvement is to improve Equity and Accessibility outcomes for different user
63-Base	3.5.3		48		1726		populations in a way that does not result in a substantial increase in fraud or theft of PII or personal or sensitive information."
				T		While a digital wallet could be used as an IdP, it's not advised to be used as one. A digital wallet holds a	
						user's attributes, uses strong authentication (generally phishing resistant) to open the wallet, and	
						requires user consent to submit attributes to a requesting RP. As a wallet is focused on holding	
						attributes and not authenticators, most wallet providers also provide an IdP that allow verified users	
						(who hold a digital wallet/verified credential) to create strong MFA authenticators to use for	
						authentication with a variety of RPs. Additionally, not all subscriber-controlled wallets are on-device.	
						While the private key to unlock the identity attribute is stored with the subscriber, many wallet vendors have taken a privacy-focused, cloud-storage approach for wallets, which reduces the loss of	
63C		1	1	40:	13-407	verified attributes when a device is lost/stolen/broken.	Remove subscriber-controlled device as an IdP.
63C		2				Trust Agreements can be bilateral or through a trust framework.	Recommend introducing the idea of a trust framework in this section.
63C		2.3	6			typographical error	"At FAL2, the assertion SHALL be audience restricted to a single RP."
						While informing the RP of the IAL of the subscriber and FAL of the transaction is good practice, there	
				1		might be scenarios where the RP doesn't want the IAL of the subscriber. This should be a SHOULD	
				1		statement, as the RP should be able to decide what information it needs from the IdP to make a	
				1		holistic decision of whether the subscriber should gain access. Similarly, both the IdP and RP SHOULD	
63C		2.5	_			have a record of what the FAL of the transaction is, so requiring an IdP to submit that information seems excessive.	Channel M. and F.M. as wiscons and the GUOLIE pathologists
63C	+	2.5	7			The lowest IAL in the guidelines is IALO (no proofing), not IAL1.	Change IAL and FAL requirements to SHOULD statements Change IAL1 to IAL0
050		2.5		1	000	This statement is only true for traditional general purpose IdPs, as a privacy-preserving digital	Change INCL to INCO
						wallet/verifiable credential does not have "direct access" to all the details of the subscriber account,	
63C		2.5	7	609	9-612	only the details the subscriber consented to.	Remove these lines
						Because there are two distinct places where identity evidence is stored on behalf of the subscriber of	
						digital identity wallets (device or the cloud), a wallet should not be protected just by an activation	
						factor (PIN/password) if a subscriber-controlled wallet doesn't require a private key (which is the case	
63C	3.1.2		11	600	00 600	for mDLs). Similarly, because wallets are used to store attributes, not authenticators, this section should exclusively be discussing IdPs.	Remove either the presentation of an activation factor and/or of subscriber-controlled wallets in Section 3
63C	3.2.2		12			typographical error	"identity attributes" should be plural, not singular
	J.L.L			T		How does a trust agreement "establish usability and equity requirements" in a federation transaction?	Technique and the partial first angular
						To the user, they are only operating with the RP and, in some cases, will be able to understand that	
						they are also using another vendor's program. Because a federated transaction is basically based on	
						protocols, how can we ensure that those universally standardized protocols hit "usability and equity"	
63C	ļ	3.4	17	896	96-897	requirements?	Remove or change to a SHOULD statement
						and the contract of the contra	
						While the trust agreement SHOULD include details of the proofing process, adding compensating controls and exception processes to the trust agreement could be a security issue, as the trust	
						agreement is required to be public later in this section. To drill down more, while exception processes	
				1		and compensating controls must be in place to ensure equity and fairness for applications, making	
				1		those processes and controls public will create a massive attack vector to the CSP with the most	
63C		3.4				relaxed processes, inviting fraudsters to capitalize on those CSPs.	Suggest changing SHALL to SHOULD
		Ţ		919			
63C	-	3.4	17	920	20	FALs also need to be included	include FAL in the list.
				1		While transparency is very important to give to subscribers, it should not be given when it can	
				1		compromise security. If, for example, compensating controls are required to be in the trust agreement, that is not something that an ordinary subscriber should be able to see without a clear reason, as it will	
63C		3.4	18	930	30-938	compromise security of the CSP, IdP, and RP.	Change to "As such, a high-level summary of the terms of the trust agreement"
1 2 2 2		٥	10	1			, and the second of the second
63C	3.4.2				55- <u>96</u> 6	A subscriber-controlled wallet should not also be an IdP, as it holds attributes, not authenticators.	Remove subscriber-controlled wallet reference
63C		3.6	23		1094	typographical error	add "the" before IdP and RP
63C		3.6	23		1099		add an apostrophe in "subscriber's attributes"
63C	3.7.1		25	1	1147	A subscriber should also be notified when the RP terminates their account.	Include a SHALL/SHOULD line for subscriber notification of termination of accounts
636	3.9.1		28	.1	1274	Complying with the law or legal process is a requirement of an IdP, whether or not it is in the trust agreement	
63C	2.9.1		28	╁	1271	Complying with the law or legal process is a requirement of an IdP, whether or not it is in the trust	
63C	3.9.1		28	1	1283	agreement	
				f		This level of detail was not required under 63A. It is an extremely onerous requirement, and would	
				1		ultimately lie on the CSP to detail. Those information points would then be used by certain RPs to	
					381-	determine whether the identity vetting met the RP's standards or not, and then might require a	
63C		3.11	31	138	383	subscriber to re-proof certain attributes.	Either make this requirement a part of 63A or remove it from 63C
63C	3.11.3.1			L.,		How would the RP know definitively that the attributes are allowed to be provided? The shall	
			34	1149	190-14	statement is onerous on the RP	Change from SHALL to SHOULD

					1	
					The private key is used to sign the assertion, not the public key. The public key is then used to verify	
					the signature. (note - this is an issue throughout C - it allows public keys and signing keys to sign	
63C	3.11.1		32	1406	assertions, which is not a normal course of business; see, e.g ISO 18013-5 appendix on VICAL key)	Change 'the public key used to sign the assertion" to "the public key required to verify the signed assertion"
					As AAL2 allows for both phishing resistant and phishable authenticators, how would an RP know that	
					the assertion has a "phishing resistant" authenticator when technology vendors do not transmit that	
63C		3.14	37	1568-15	level of veracity on authentication assertions?	Create a new AAL - AAL0, which would be for single factor authenticators; AAL1 would be for MFA phishable, AAL2 would be MFA phish
					As AAL2 allows for both phishing resistant and phishable authenticators, how would an RP know that	
					the assertion has a "phishing resistant" authenticator when technology vendors do not transmit that	
					level of veracity on authentication assertions? Additionally, this is at least the second - if not more -	
					time in the guidelines that specifically mandates phishing resistant authenticators. If there is a higher	
					level of assurance that comes with them (as we know there is), then phishing resistant MFA should	
63C		3.15	38	1594	become its own assurance level!	Create a new AAL - AALO, which would be for single factor authenticators; AAL1 would be for MFA phishable, AAL2 would be MFA phis
		0.20			The majority of the digital identity wallets in the US and that will be deployed in the EU will be	
					considered "general-purpose IdPs" based on these draft guidelines. These guidelines do not take into	
					account the concept of verifiable credentials, which are not always a "function of the IdP." W3C	
					verifiable credentials, and similarly most digital wallets deployed to networked systems, bake privacy	
					into their wallets by encrypting a subscriber's attributes and giving only the subscriber the private key.	
					As such, these wallets - even though they are deployed to network systems - are subscriber controlled	
					because only the subscriber can decrypt and share their attributes, which seems to be what subscriber-	
63C		4		1700	controlled wallets are focused on.	Remove lines 1709-1710, and include the concept that having a private key in control of the subscriber satisfies subscriber-controlled
030		- 4		1/03	While transparency is very important to give to subscribers, it should not be given when it can	Nemove lines 1709-1710, and include the concept that having a private key in control of the sauschiber satisfies sauschiber-controlled
					compromise security. If, for example, compensating controls are required to be in the trust agreement,	
					that is not something that an ordinary subscriber should be able to see without a clear reason, as it will	
63C	4.3.1		47	1007 10	compromise security of the CSP, IdP, and RP.	Change from SHALL to MAY statement to ensure that Federal security is not compromised by this SHALL statement
030	4.5.1	-	4/	1007-10	compromise security of the CSP, fur, and KP.	Change from Shall to war statement to ensure that rederal security is not compromised by this Shall statement
					Transparency is very important to give to subscribers, and many of the bullets in this section should be	
					required even if not requested, especially if NIST doesn't change the terminology of subscriber-	
					controlled wallets. However, because this section should be mandatorily given prior to obtaining	
					consent to transmit a subscriber's attributes, the identity API disclosure requirement is unnecessary, as	
					the average subscriber (even me!) wouldn't understand what the ramifications of that is. Additionally,	
					subscribers should not know what other subscriber populations are being asserted, as that can	
					compromise security. Similarly, but not as importantly, only a handful of people understands or	
63C	4.3.2	4	17-48		comprehends what an xAL is and why it should matter.	Remove "upon request"; remove the bullet that begins with "what if any identity APIs are made available"; remove the bullet that begins with "what if any identity APIs are made available"; remove the bullet that begins with "what if any identity APIs are made available"; remove the bullet that begins with "what if any identity APIs are made available"; remove the bullet that begins with "what if any identity APIs are made available"; remove the bullet that begins with "what if any identity APIs are made available"; remove the bullet that begins with "what if any identity APIs are made available"; remove the bullet that begins with "what if any identity APIs are made available"; remove the bullet that begins with "what if any identity APIs are made available"; remove the bullet that begins with "what if any identity APIs are made available"; remove the bullet that begins with "what if any identity APIs are made available"; remove the bullet that begins with "what if any identity APIs are made available."
					Maybe 300 people (and I feel like I'm being generous here) fully understand the ramifications of xALs.	
63C	4.3.2		48	1863	Mandatorily providing this to the whole population will unnecessarily confuse them.	Remove line
					While this is a MAY statement, identity wallets that are deployed to network systems but are	
					subscriber-controlled as only the subscriber can unlock their accounts cannot pre-populate attributes	
					without a runtime decision from the subscriber. This behavior, however, makes sense for a centralized	
63C	4.6.1.1		51		IdP that is passing identity attributes to an RP that it is enrolling for SSO within an enterprise.	Digital identity wallets that are deployed to network systems should not be considered a "general IdP".
					"The IdP has a direct view of the subscriber account's attributes" - again, while this is true for a	
					centralized IdP scenario, it is not true for an identity wallet that is deployed to a network system where	
				L	the private key is kept with the subscriber. Only the subscriber has access to and can consent to the	<u></u>
63C	4.6.4		56	2102-23	1 transmission of their attributes.	Digital identity wallets that are deployed to network systems should not be considered a "general IdP".
					While informing the RP of the IAL of the subscriber and FAL of the transaction is good practice, there	
					might be scenarios where the RP doesn't want the IAL of the subscriber. This should be a SHOULD	
					statement, as the RP should be able to decide what information it needs from the IdP to make a	
					holistic decision of whether the subscriber should gain access. Similarly, both the IdP and RP SHOULD	
					have a record of what the FAL of the transaction is, so requiring an IdP to submit that information	
63C		4.9	63	2348	seems excessive.	Move IAL and FAL requirements to MAY statements starting in line 2359
					There are instances in these guidelines where phishing resistant authenticators are required (this is the	
				1	third time in C), yet they do not have their own assurance level. As such, having their authentication	document and create a new AAL - AALO, which would be for single factor authenticators; AAL1 would be for MFA phishable, AAL2 wo
		4.9	64	2364-23	event be a "may" and not a "shall" doesn't make sense.	be MFA phishing resistant, and AAL3 would stay the same. :)
63C		7.5				
63C		4.5			It is critical that RPs and IdPs be informed when either suspects that an account has been	
63C		7.5			It is critical that RPs and IdPs be informed when either suspects that an account has been compromised, especially when RPs are involved that hold highly sensitive data or allow access to funds.	2297 - Remove this item from the 'SHOULD' list and change to:
63C		4.5		2297 &	compromised, especially when RPs are involved that hold highly sensitive data or allow access to funds.	

						T	
						While the EU's digital wallet requirements have a heavy focus on device-bound wallet, they discuss the	
						wallet being accessible on "smartphones or computers" as well as the wallet being available as mobile	
						applications or cloud services (E.g., "European Digital Identity Wallets should ensure the highest level	
						of data protection and security for the purposes of electronic identification and authentication to	
						facilitate access to public and private services, irrespective of whether such data is stored locally or on	
						cloud-based solutions"). The EU also aims to provide a "user-centric approach" to its wallet, which	
						necessitates accessibility across different devices to meet various user needs. This user-centric	
						approach aligns to the Guideline's discussion of usability and equity - as not everyone has access to	
						their own mobile device, but they do have access to a publicly accessible computer in a public library,	
						vendors that provide wallets must create more flexible solutions, which include both mobile-based and	
						networked solutions. Continuing, a networked wallet reduces the need for subscribers to re-enroll and	
						re-verify their attributes when they have their device lost or stolen.	
						Of course, the EU's wallet must meet the privacy requirements found in GDPR, which can be obtained	
						through either device-bound or cloud-based wallets. Because "general IdPs" are traditionally an	
						organization's centralized IdP from which users SSO into a variety of RPs, subscribers expect general	
						IdPs to share their attributes without just in time consent, as subscribers desire as much birthright	
						access to RPs as possible based on security risks. In the situation of digital identity wallets that are	
l						stored in the cloud (which are most digital identity wallets, and are being developed under eIDAS	
						standards), they should be considered subscriber-controlled if the wallet's private key is kept with the	
	63C		_	_		subscriber.	Align 63C to eIDAS 2.
			_		_		change to "When the subscriber has control over the private key that protects their attributes or runs on a device controlled by the
	63C		5	69	2496	A subscriber-controlled wallet can be in the cloud if the subscriber is in control over the private key.	subscriber, whether as a digital wallet"
						An activation factor should always be required before any operation that is using a wallet. While this	
						does create more friction to the subscriber, wallets contain such sensitive information that it's	
						important that the subscriber understands their actions before they do them (e.g., reissue an attribute	
	63C	ţ	5.1	69	2507	bundle)	change SHOULD to SHALL
						While we agree that wallets *could* be used as an IdP for limited purposes, we don't believe that it is a	
						best practice to set a wallet up to always act as an IdP, especially when ISO-based wallets don't contain	
						private keys on the mobile device. Continuting, the wallet should not be providing attribute bundles to	
						every RP at every transaction. Wallets should only be transmitting attribute bundles at time of	
						enrollment and when an RP requests an additional attribute to the subscriber account. Which means,	
						the wallet is acting more like a CSP than an IdP. At all other times, a subscriber should be using an	
						authenticator (preferably a phishing resistant one in its own AAL2 category) to help minimize PII	
						leaving the wallet and to create a more privacy-preserving authentication experience. It's very	
						important for the Guidelines to make this distinction, as the vast majority of the time wallets should	
	63C	Ę	5.2	69	2519	not be performing authentication into RPs, rather traditional IdPs should be providing this service.	
						Maybe 300 people (and I feel like I'm being generous here) fully understand the ramifications of xALs.	
	63C		5.3	72	2561	Mandatorily providing this to the whole population will unnecessarily confuse them.	Remove line
						This section discusses creation of wallets for mDLs under ISO standards, but doesn't discuss verifiable	
	63C			72	2578		include W3c verifiable credentials, especially since eIDAS2 has aligned to those standards.
	63C	ţ	5.6	74	2631	Key to privacy is the ability to selectively disclose a subset of attributes	change from SHOULD to shall
						It is more accurate and understandable to say that the RP 'obtains' the identifier and key rather than it	
	63C			73	2609		Change 'learns' to 'obtains'
	63C					Public keys can't 'present' attributes, but they can verify them.	to present' should be 'to verify'
	63C		8.8	76	2692	Key to privacy is the ability to selectively disclose a subset of attributes	change from SHOULD to shall
						The assertion can NOT include the same key that was used to sign the assertion.	
						Note: This document has repeatedly confused which key is involved in signing vs validating an	
l						assertion. And, unfortunately, the subscriber-controlled wallet doesn't seem to align with any current	
							Change: "This MAY be the same key that the subscriber-controlled wallet uses to sign the assertion." to "This MAY be the public ds ke
l						unfortunately not the leader (while we do have technology vendors who are cutting edge at wallets);	that corresponds to the private key used by the subscriber-controlled wallet to sign the assertion."
				26	674-	instead, APAC and the EU are becoming fast adopters of the technology, which is why our standards	
	63C			75 26	675	should align to them.	Align C to APAC. ISO. and W3C standards. as well as eIDAS2
1	050			75 20	0.5	Should dright to drients	rings of the ring to be determined up to with an experience
						Perhaps the writer is confusing how asymmetric cryptography works for signatures vs encryption?	
1							
						Digital Signatures: The <i>private key</i> is used to sign a message. The corresponding public key is then used	
						to verify that the message was signed by the expected private key.	
1						to verify that the message was signed by the expected private key.	
						Encryption: The message is encrypted using the recipient's <i>public key</i> . The recipient then uses their	
	63C			73	2626	private key to decrypt it.	Change 'signed by the CSP's public key' to 'signed by the CSP's private key'.
 	63C			73		How does the 'RP introduce its properties'?	Provide an explanation.
 	63C		_	75		Language that again implies that the public key was used for signing	Change "for the key" to "that corresponds to the key"
	63C					PII does not include the entire universe of private and potentially sensitive data.	Change to (addition in bold): "contains PII or other private or potentially sensitive data"
			+	-	2,03	Message level encryption should be required whenever PII or other sensitive data is passed through a	private or potentially sensitive data
]	63C			76	2704	third party.	Change SHOULD to SHALL
	000					I amar kan ali	1

		I	$\overline{}$	ı		Line 2664 in Section 5.8 states that the assertion from a subscriber-controlled wallet SHALL contain a	İ
						cryptographic nonce only if it is provided by the RP. Line 2701 in Section 5.9 also indicates that it is	
					2727-	optional for the RP to provide a nonce. Line 2727 then implies that the RP is required to provide a	Either require that the RP provide a nonce (recommended) and update lines 2664 & 2701, or change lines 2727-2728 to indicate that the
	63C				2728	nonce.	requirement only applies if the RP had provided a nonce in its request.
						It is inevitable that some bad actors will be able to obtain signed attribute bundles from CSPs. It is also	
						inevitable that bad actors will succeed in stealing signed attribute bundles from insufficiently protected	
						wallets. (It is only the eventual scale of this fraud that is currently unknown). It is therefore critical that	
						RPs are able to determine whether a particular attribute bundle has been reported as having been	
	63C			76	273	fraudulently obtained so as to prevent its use.	Change MAY to SHALL.
						Additional common attacks include: interception of the password and 2nd factor with a keylogger or redirecting users to a realistic but fake IDP where the password & 2nd factor are captured and relayed	Add information on additional attacks and mitigations. To mitigate against credential theft by fake IDPs and keyloggers, users can be prominently shown logs of their previous visits, or at least the most recent visit, along with instructions for when they see a login that
	63C			76	275	to the IDP. Also see https://githubcom/pushsecurity/saas-attacks	they don't recognize.
	63C			87		Broken link - Account Chooser redirects to a list of WGs	Fix link. Perhaps: https://openid.net/wordpress-content/uploads/2011/12/ac-integration-spec.html
	63C			87		B Typo - remove 'as' in "commercial as IdPs" & adjective recommendation -'some'	Change to "some users may be less comfortable with commercial IdPs"
	050			-			Recommended addition in bold: "based on their historical interactions with government services, or on their knowledge that
	63C			87	2996	There are much better, and perhaps more common, reasons to use commercial IdPs.	commercial IdPs provide greater protection against fraud.
						In talking with the general public , users don't generally think of identity or how authentication works -	
	63C	8.2.1		88		they just want it to work and want it to be easy.	
	63C	8.2.1		89	3056	Age is determined based on birthdate, which is NOT dynamic. A better example is an address.	change age to address
						Most privacy laws require the ability for users to completely delete their identity account. In all cases	
						where privacy laws are in effect, deactivation would not be appropriate, only deletion. To help prevent	
	63C	8.2.1	_	89	3065	fraud, CSPs should have audit trails and other mechanisms in place.	remove suggestion
						Non-preference attributes need to be verified before they can be updated by a user. It is common for	L
	526				205	bad actors to change attributes in a user account to further their purposes, such as replacing the	"update preference attributes. Attributes that may be relied upon by RPs, such as postal address and phone number, require
 	63C	8.2.1		89	3056 3062-	legitimate user's address with one that they control.	validation and verification, and should be subject to fraud prevention analysis, before they are updated in the system."
	63C	8.2.1		90	3062-	What is the use case for this? It would appear to provide bad actors with a way to cover their tracks.	Reconsider including this. If it is retained, provide a concrete example and update the wording so it is not an avenue for exploitation.
	030	0.2.1	-	03	3004	Tribe is the use case for this: it would appear to provide bad actors with a way to cover their tracks.	neconsider meading aris, it it is retained, provide a consiste example and update the wording so it is not an avenue for exploitation.
	63C			90	3109	Redress methods are exploitable by bad actors seeking to change a legitimate users information.	Addition in bold: "Provide secure and effective redress"
						Not only is this paragraph oddly conspiratorial against IdPs with respect to a disadvantaged population,	
						it also assumes IdPs are evil vendors who are trying to somehow gain from the knowledge that a	
						person is disadvantaged. This paragraph is wholly inappropriate, assumes vendors don't care about the	
						entire population, and wrongly targets IdP vendors. For a second time, the document raises the spector	
						of RPs colluding, which is loaded language. The reality is, if a vendor actually did what is suggested here	
						and documented in a government document, the vendor would be canceled by its customers and	
						perhaps face civil or criminal penalties. This paragraph shows a bias from NIST against commercial	
					3209-	providers and undermines the role of 800-63 in fostering quality solutions that federal agencies can	
	63C		9 93	3-94	3212	leverage.	Remove paragraph
							In all four volumes, shorten the definition to its non-controversial and non-political core meaning "The consistent and systematic fair,
						other communities that do consider themselves 'underserved', and uses terminology that significant	just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied
	63C		_	114	384		such treatment"
						In talking with the general public, users don't generally think about federation or perceived risks to	
	63C	8.2.2	_			them - they just want to be able to gain access and want it to be easy.	remove suggestion
	63C		9	95	3253	typographical error	change to "having the RP have its own"
	63C		10			General comment: How does it work for SAML - these guidelines only discuss OpenID Connect.	include SAML examples
						This avample describ reflect today's reality with the surrent Federal wellet wanders and the seen to be	Include a section to reflect today's current examples, which includes digital identity wallets that are cloud-based, not device bound, and
	63C	1	0.4 99	100		This example doesn't reflect today's reality with the current Federal wallet vendors and the soon-to-be operational HHS XMS.	an attribute exchange that will standardize the attributes in the wallets and allow for them to be utilize for multiple RPs.
	030		0.4 5:	9-100		operational Titis Xivis.	an attribute exchange that will standardize the attributes in the wanets and allow for them to be utilize for multiple krs.
						What is described IS FAL with a PKI Authenticator, as a hardware cryptographic authenticator that	
	63C	1	0.7	101	3423		Suggest changing title, perhaps FAL3 with a non-smart card hardware cryptographic authenticator
	63C	†	1	101		any	that does not verify any of the authenticators
					330	These definitions need improvement. The subscriber account at the CSP can also be "subscriber-	
						controlled." A wallet is not always independent of the CSPs infrastructure. "Onboarded" by the CSP	1) as a verifier for authenticators in which the asserted data originate from the CSPs infrastructure for each assertion
	63C		1	1	404-40	does not have a clear meaning	2) as a data structure persisting on a subscriber-controlled device from which assertions are made independent of the CSPs infrastructure
						The last two sentences in this paragraph are very difficult to parse. I believe this conveys the same	With rare exceptions, federation is preferred any time the RP and the subscriber are part of the same organizational domain. Even when
	63C		1	1	410	information more clearly	under the same domain, federation may still be appropriate for centralized account management and technical integration.
						By explicitly stating federal agencies, we are implying this doesn't need to be done outside of federal	
						agencies. The scope of applicability (legally) is federal agencies, but we are establishing best practices	
						wider than that and thus shouldn't limit scope in that way. Others can decide on their own whether to	
ļ	63C		2.2	6	545	model those best practices	remove "by or on behalf of federal agencies"
	500				_	the inheritance works such at "or higher" is not needed. This section has requirements for FAL2 and	W 113 W
	63C		2.2	6	545	should avoid defining requirements for other FALs	remove "or higher"
						By explicitly stating federal agencies, we are implying this doesn't need to be done outside of federal	
						agencies. The scope of applicability (legally) is federal agencies, but we are establishing best practices	
	63C		2 2	_	566	wider than that and thus shouldn't limit scope in that way. Others can decide on their own whether to model those best practices	remove "by or on behalf of federal agencies"
	63C		2.3	6	500	This is not a new requirement as it is inherited from FAL2	remove by or on behalf of federal agencies remove lines 566-568
	63C		2.4	7		The IdP may not have "direct acces" to the details	Restate as "only the IdP has direct knowledge of the xAL achieved by the subscriber. Consequently"
	63C		3	9		The language is ambiguous as to whether the RP can always do these three things	Change lead in sentence to "Depending on the use case, the authenticated session might then be used by the RP to:"

	T					T	
	500			40		make conditional. Alternatively, make clear the ones that will be in the subset (federation identifier,	
	63C		3	10	651	etc) and what might not (additional attributes)	change "is" to "may be" made available
						Should we be referring to IdP as a role given its status with wallets? It might be better described as a	
						function. There may be a third party controlling it, or it may just be a function built into a wallet app, or	
						a standalone app, or could reside with a CSP or some other formulation. Calling it a role (or, worse, a	
	620	3.1.2		11	693	party) boxes it into needing an entity, which it does not	
	63C	3.2.2		11		is the authorized party not a role?	
-	63C	3.3.1.2		15			entropy meeting the latest version of 800-131A, 112 bits as of this publication
	63C	3.3.1.2	3.6	23		Should the entropy be future proofed RP can get additional consent	without specific additional consent from the subscriber
	03C		3.0	23	1096	A federated identifier could be associated with multiple RP subscriber accounts, for instance a small biz	without specific additional consent from the subscriber
						owner that has an account as an indivdual and for the business. Sure, an RP should manage this with	
	620		3.7	24	1110	Prelationships in their system, but that's not for 63C to decide	remove restriction
	63C	3.7.1	3.7	25		missing word?	maybe deleted?
	050	5.7.1		23	1170	shouldn't the account resolution refer to 63A rather than a generic risk assessment? It's a SHALL, but	import deleted:
	63C	3.7.2		25	1166	doesn't accomplish anything without guidelines attached to it.	
	050	5.7.2		23	1100	Why would there be such requirements on the RP? If I want to create native subscriber access and	
						abandon the federation for that subscriber, that's on me. If the federation wants to block that practice,	
	63C	3.7.3		25	1177	2 fine. But I don't think NIST should be in the business of determining that.	
	050	5.7.5		23	11/2	mic. but I don't trink Nist should be in the business of determining that.	
						There are too many instances in this volume of ignoring the good work of the other volumes and NIST	
						SPs. It's nearly written as a standalone document and misses opportunities to set real requirments by	
						pointing back to 63A, 63B. A good example of authenticated protected channel, which is left	
						undefined. Another is requiring "a risk assessment" without specifying any conditions around it. There	
	63C	general				are also requirements that conflict with or duplicate those already met by other volumes.	
	63C	general	3.13	36	1557	2 typo "own its own"	on
	63C		3.15	38		L assertion in figure 4 should say bound authenticator ID	add ID
	050		3.13	30	1331	As a general comment, the 63 suite has common language that is often abandoned in 63C. This should	800 10
						not be the case and 63C needs a complete review with that in mind. Specifically, is "independent of the	
	63C		3.15	38	1606	transaction binding" different than out of band?	change to out of band
	050		3.13	30	1000	a normative section shouldn't refer to requirements vaguely as "slightly different." Provide the	Change to dat or band
	63C		3.15	38	1603	requirements or reference to them	change sentence to refer to 3.15.1
	030		3.13	36	1003	This section buries requirements in a long paragraph of text, yet doesn't include the needed normative	enange sentence to teler to 5.13.1
						statements. This is a weakness of this document overall: it prioritizes the discussion over the	
						requirements, often leaving requirements incomplete. Here, for example, the ways the RP can deliver	
	63C	3.15.1		39	161/	the authenticator never actually appear in a normative statement.	rewrite section to prioritize normative statements over discussion
	050	5.15.1		33	101-	Change name of general purpose. This is, obviously, too general a descriptor. IdP controlled might be	Tewnic section to phonaze normative statements over diseassion
	63C		4	43	170/	more appropriate.	change general purpose IdP to IdP controlled
	63C		4.2	45		The subscriber is not part of the trust agreement	change all parties to list the specific parties
	050			.5	1,0,		and the same as the same persons
						a priori is two words. This error appears elsewhere in the document as well. Broader point: why use	
	63C	4.3.1		46	1770	latin when english will do? It feels like an effort to make the document even less approachable	remove a priori throughout document and replace with common english words
	050	4.5.1		40	1//,	having a may nested in a shall like that is very confusing. So those terms are required but the might	Terrore a priori arroagrious accument and replace was common engines words
	63C	4.3.1		46	1781	L vary, thus some are not required?	SHALLs can't be MAYed. Rewrite for clarity
	63C	4.3.1		46		7 is the point how the RP will use them? If so, that's a use specification. Purpose is ambiguous.	rewrite for clarity
	050	4.5.1			1/5/	The requirement for notification of RPs is an issue. If I delete my google account, google should not be	iemeto dany
						required to notify www.cutekittymugs.com when I delete my account. Moreover, the RP shouldn't be	
						required to delete shared attributes. Should the IRS have to delete my personal information if my idp	
	63C	4.6.5		57	2169	account is terminated (for non-fraud reasons)?	remove this requirement, particularly for non-fraud reasons
	030	T.U.J		5/	2100	s decount is terminated for non-mada reasons):	service and requirement, per reading for front made reading
						For privacy reasons these signals may not be desirable. For instance, if my IAL2 expires at the IdP/CSP, I	
						don't want every RP notified. I may just need to come back and re-proof and go about my day. If an RP	
						is relying on the IdP's assertion at logon anyway, they don't need this update ahead of time; they just	
						won't get an IAL2 assertion from the IdP. Likewise, not every RP needs to know if I delete my google	
						account. The RP may not even know my email address, so why would the IdP signal the RP if I change	
	63C		4.8	62	2200	it? There's just too much unneeded attribute sharing going on here.	rethink these and remove all but the essentialwhich may just be compromise
	03C		4.6	02	2293	Similarly, the IdP does not need to know if I delete my account at www.cutekittymugs.com. Nor does	Technic triese and remove all but the essential—which may just be compromise
	63C		4.8	62	2202	B the IdP need to know what authenticators I've bound directly with the RP	rethink these and remove all but the essentialwhich may just be compromise
	630		4.8	62		subject to is not normative. Add a SHALL statement about privacy and security review	change subject to to SHALL
	030		4.6	02	2313	normative statement nested in a list about a different process. Move this requirement to a standalone	winings souplest to to district
	63C		4.9	63	2226	statement	move requirement after the list
	030		4.9	US	2330	this is repeated from earlier in the document. Repeating normative statements can cause confusion,	into requirement after the fac
	63C		4.9	64	2270	particularly when different words are used	delete paragraph
			4.3	04	23/5	this is repeated from earlier in the document. Repeating normative statements can cause confusion,	secret puringrupin
	63C		4.9	64	2202	particularly when different words are used	delete paragraph
	USC		4.9	04	2383	this is repeated from earlier in the document. Repeating normative statements can cause confusion,	delete paragraph
	63C		4.9	64	220/	particularly when different words are used	delete last sentence
	030		4.9	04	2394	The document repeats requirements in different sections, stating them slightly differently, and putting	Secretarias definence
	63C	general				them both in normative statements. This can create a significant issue with compliance.	
——	UJC	general				them both in normative statements. This can create a significant issue with compliance.	
	630	4.11.1		66	2/120	Stating a required time limit without setting an actual limit has the effect of no time limit. Establish one	actablish a required time limit
	030	7.11.1		UÜ	4433	Placeting a required time without setting an actual minit has the effect of no time limit. Establish one	lestablish a required time limit

					1	
					Are we assuming the wallet is associated with a multifactor device and thus has an activation factor?	
					We should be clearer about this assumption. If we're not making it, why are we invoking an activation	
63C		5	69		factor?	Clear up language around authenticators associated with subscriber controlled wallets
63C	5.4.1		73		Is there a difference between line 2590 and 2597?	
63C		5.5	73	2604	typo, though I like the idea of an RP singing the public key	signing
					normative statement nested in a list about a different process. Move this requirement to a standalone	
63C		5.8	75	2682	statement	move requirement after the list
					out of band does not have the same meaning here as elsewhere and could cause confusion. It's not	
63C		5.8			necessary	delete out of band
63C		5.9		2712		delete "other requirements in these guidelines are met. For additional requirements for"
63C		6.1	79	2770	including repudiation as threat makes it sound like the IdP and Subscriber are malicious actors.	Either leave repudiation threats out or find a less hostile way of describing them
					NIST seems to have reverted to using PII instead of personal information. This is a mistake. We should	
					be taking a more expansive view risk management associated with personal informmation as a whole,	
63C		7.1	81		rather that just PII. This applies in many place in the document.	revert PII to personal information everywhere except where it truly is limited to PII
63C		7.1	81	2802	this comes awfully close to making a normative statement	change "cannot" to something like IdPs must take care in gaining consent for additional uses
					colluse is a pretty charged term. It may be in some RPs interest to share data to improve their business	
63C		7.1	81	2808	efforts, but we don't need to put those activities into terms that suggest illegality	rewrite sentence to talk about privacy protetions and not nefarious business practices
63C		7.1	81	2810	some bound authenticators are recognizable, not all	add some
63C		7.1	82	2813	this again is close to a normative statement	an identity API, implying these additional attributes may fall under the privacy risk assessment
63C		7.1	82	2815	normative statement	change to "The SAOP can typically answer questions about"
63C		7.1	82	2828	normative statement	perhaps add "typically"
63C		7.3	83	2882	normative statement that conflicts with the normative statement in the normative section (3.10.2)	change required to recommended (or the like)
63C	8.2.1		88	3033	normative statement	replace "ought to" with "may consider"
63C	8.2.1		88	3036	normative statement	replace "ought to" with "may consider"
63C	8.2.1		88	3033	the topic of this paragraph is covered in the privacy section and is not really about usability	delete paragraph
63C	8.2.2		90	3097		delete sentence about security practices
					it seems several items in this list are already covered by normative statements elsewhere in the	
63C	8.2.2		90	3095		remove repeated recommendations
63C	8.2.2		91	3124	what's the consideration here? What action is one to take as a result of this paragraph?	delete paragraph
63C		9	93		normative statement	remove sentence
					is there a word missing from this sentence? It feels like it is supposed to have a SHOULD in there, but	
63C		9	93	3181	that would be normative and should not be in this section.	review for completeness; do not make normative
					normative statement. Also this is the equity section, not the usability section, so this last sentence does	
63C		9	93	3183	not need to be here.	remove
63C		9	93		the first two sentences are covered in 63A and 63B	remove first two sentences of paragraph
63C		9	94		Let's not call people thoughtless	replace "thoughtless clickthrough" with "users clicking through without fully understanding the implications of their consent."
			اتا		entire paragraph is normative. Moreover it has little to do with equity. These are privacy and usability	, and the same and
					requirements (again, in an informative section) and while such things can impact equity, in this case	
63C		9	94	3225	their rightful place is in a normative section on privacy	remove paragraph
050			54	5225		
					what differences in requirements are we talking about here? I assume by "interests" we mean	
63C		0	94	222/	incentives, but what are the requirements? Also, "has to be addressed" is awful close to normative.	rewrite for clarity; do not make normative
030		3	34	3234	motivations makes it sound quite nefarious for both the government and "private" entities. If you	newrite for clarity, do not make normative
63C			94	2240	mean commercial, say commercial, and be neutral with the language	rewrite for neutrality and clarity
63C		9	94		awkward sentence. Avoiding passive voice may help	rewrite for clarity
63C		9	94		normative statement	remove sentence
030		9	94	3240	This paragraph is difficult to parse. What inequity? If an RP only accepts one IdP, that impacts everyone	Terrove Sentence
					equally that wishes it accepted more than one. The solution of an account recovery process is fine, but	
cac		_	05	22.00	what follows ("allows for the secure linking") doesn't make sense given the start of the paragraph	and the state of t
63C		9	95	3249	established it was difficult to find a second IdP the RP would accept.	remove everything about multiple IdPs and keep the part about recovery