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: The Digital Chamber

Name of Submitter/POC: Jonathan Rufrano and Jean-Phillippe Beaudet

Email Address of Submitter/POC:

Section 1 (1992) No. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10								
1 to 100 2 12 12 12 18 98-86 control in the galaction of process of adaptive control of selection of process of adaptive control of the selection of process of adaptive control of the selection		Publication					Comment	
services and the services of t	Comment #	(Base, 63A, 63B, 63C)	Section		Page #	Line #	(Include rationale for comment)	Suggested Change
Service of the control of the contro							We strongly support the inclusion of general purpose and subscriber-controlled wallets as a standard	
Service Servic	1	Base		2.2.1	12	683-684		
See 1 2 29, 99, 1980 what is not be appropriate to all on the proposed to a state of the property of the of the								
Secondary 1	2			2.4				
here 1 1 27 (179-160) please well-extend the third size is being bandled and what rights they have 10 1 1 2 1 (179-160) please well-extend the third size is being bandled and what rights they have 11 2 1 1 1 2 1 (179-160) please well-extend the size is being bandled and what rights they have 12 2 1 1 1 1 2 1 2 (179-160) please well-extend the size is being and rights of addression. 13 3 1 3 1 1 3 (179-160) please well-extend the size is being and residue of extending of extending the size is being and residue of extending the size is the size of addression. 14 5 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	3	Base		3	23	982-984		Make DIAS available to subscriber as well.
Bus 5.4 44 150 Week from the segregoration to all marks the DNS provides the security of the security of the security of the security of secur								
Ratio 1.4 49 Type John Appendix point Appendix	4			_				
Recognising that data collection and analysis a beneficial to system improvements and that collection of automation. The proposition requires granting trading and trading of reviews data is a threat vector for cybersecurity. The proposition requires granting trading and trading of reviews data is a threat vector for cybersecurity. The proposition requires granting trading and trading of reviews data is a threat vector for cybersecurity. The proposition requires granting trading and trading of reviews data is a threat vector to use privacy and system operacecurity, we suggest this data solicities and analysis as the company of the proposition of the reduction of the proposition of the reduction of the reduction of the proposition of the reduction of the reducti	5	Base		3.4.4	44	1652		Make DIAS available to subscriber as well.
The provision requiring fracting and tracking of referes issue data is a threat vector for operacularly supplications and analysis is bearderically as system operacularly as supplications and analysis is bearderically as system, operacularly, we suggest this data should be either anomymised. Bear 3, 15, 12, 13, 12, 13, 13, 13, 13, 13, 13, 13, 13, 13, 13		D		2.0	40	1700	• • •	
Bee 1.6 6. 7/39-1786 and privacy require good reacting of reference to sear data is a threat vector for spherescentry. You suggest this data should be either accompanied, aggregated, and privacy specifications in the parameter of the search	ь	Base		3.6	49	1/69	system, especially in digital identity systems that have higher levels of automation.	Decompling that data collection and analysis is honoficial to system improvements and that collection of such data is a
1							This provision requiring tracing and tracking of redress issue data is a threat vector for subgressurity	
Bee 3.6 59 (80-).181 We appear the NST 's galactice to minimate data in this around. We appear the NST for including to a provider. It is parameter that the use of A/Ms in identity process Base 3.8 31 (80-).186 case, but in the control of the c	7	Paca		26	40	1702 1704		
We applied NST for including this provision. It is paramount that the use of Al/Mit in identity process. It is seen to only independent of the provision of th	,		-					aggregated, and entrypted.
Base 3.8 5; 1870-1874 (suspense that a dustible). This allows not only understanding of proteins and proteins	٥	Dase	-	3.0	30	1009-1011	we appreciate NIST's guidance to minimize data in this arena.	+
Base 3.8 5; 1870-1874 (suspense that a dustible). This allows not only understanding of proteins and proteins							We applaud NIST for including this provision. It is paramount that the use of AI/ML in identity processes	s. We suggest adding specific methods of sharing this data, and would value seeing this data posted on a public, immutable.
Bose 3.8 5 1 385 1585 1585 1585 1585 1585 1585								
We strongly support the inclusion of such strong AVML model transparency requirements, especially as it comes to digital identity, explained NTS and would hope federal agreements, especially as it comes to digital identity, explained that are supported to the strong and the common and the support of the common and the support of the s	9	Base		3.8	51	1830-1834		
as it cares to digital identity. We applied MST and would begin efederal agencies follow this normative As remote unattended identity werfication use cases are growing in number, we believe it would be the control of the control o	,	5430		5.0		1000 1001		and the expectation of the expec
Base 3,5 5, 185-183d goldance for non-indentity systems as well. A remote unattended indentity well-ration use cases are growing in number, we believe it would be wise to create a discrete section for this, instead of sequestering this method to in an example in the Create a discrete section for remote unattended identity verification methods. Create a discrete section for remote unattended identity verification methods. Create a discrete section for remote unattended identity verification methods. Create a discrete section for remote unattended identity verification methods. Create a discrete section for remote unattended identity verification methods. Create a discrete section for remote unattended identity verification methods. Create a discrete section for remote unattended identity verification methods. Create a discrete section for remote unattended identity verification methods. Create a discrete section for remote unattended identity verification methods. Create a discrete section for remote unattended identity verification methods. Create a discrete section for remote unattended identity verification methods. Create a discrete section for remote unattended identity verification methods. Create a discrete section for remote unattended identity verification methods. Create a discrete section for remote unattended identity verification methods. Create a discrete section for remote unattended identity verification methods. Create a discrete section for remote unattended identity verification methods. Create a discrete section for remote unattended identity verification methods. Create a discrete section for remote unattended identity verification methods. Create a discrete section for remote unattended identity verification methods. Create a discrete section for remote unattended identity verification methods. Create a discrete section for remote unattended identity verification methods. Create a discrete section for remote unattended identity verification methods. Create a discrete								
Ar emote unstrended identity verification use cases are growing in number, we believe it would be the create a discrete section for five instead of sequestering this cold in an example in the Create a discrete section for remote unattended identity verification methods. 12 63A 3.1.3 1 21 1008-1010 We applied NRT for creating normative requirements or creation, mitigation, and documentation of a significant of the control	10	Base		3.8	51	1830-1834		
wise to create a discrete section for this, instead of sequestering this method to in an example in the 12 63A 3.1.3.1 21 1008-1010 We applaud NIST for creating normative risk assessments requirements around non-Pil data risks. We applaud NIST for creating normative requirements on creation, mitigation, and documentation of 14 63A 3.1.3.2 1 2012-1017 privacy risks associated with dentity promoting and enrollment. 15 63A 3.1.3.2 2 1001-1017 privacy risks associated with dentity promoting and enrollment. 16 63A 3.1.3.2 2 1003-1003 this sunction why summarises of privacy risk assessments would not be available to subscribers as well. 16 63A 3.1.3.2 2 1003-1003 this sunction why summarises of privacy risk assessments would not be available to subscribers as well. 17 63A 3.1.3 2 2 1046-1052 We believe this section is suited for additional user data protections. We applaud NIST for including equity considerations so prominently in the 10 proming process, as introduced in the control of committee of the control of committee of the control of committee of the control of co								
11 63A 2.5.1 is 775-838 last settence in the Authemication and Federation Protocols bullet. 12 63A 3.1.3.1 21 3008-1010 (We appliad NRT for creating normative risk assessments requirements around non-Pil data risks. 13 63A 3.1.3.2 1 2012-017 provery risk associated with identity proofing and erroriment. 14 63A 3.1.3.2 1 2012-017 provery risk associated with identity proofing and erroriment. 15 63A 3.1.3.2 2 103-3005 is in undear why summarise of privacy risk assessments would not be available to subscribers as well. 16 63A 3.1.3.2 2 103-3005 is in undear why summarise of privacy risk assessments would not be available to subscribers as well. 16 63A 3.1.3.2 2 103-3005 is in undear why summarise of privacy risk assessments would not be available to subscribers as well. 17 63A 3.1.4 23 107-5007 dischard and the experimentation of the proofing process. as intentional or unintentional bias in these processes is a present risk, and the outcomes are potentially and the details of any records retention requirement if one is in place. In o'm of the details of any records retention requirement if one is in place, including applicant's right to request data deletion or engage in other forms of redress." 18 63A 3.1.4 23 1075-1077 dischard as which is reported that not all if deeral agencies have Senior Agency Officials for Privacy, and are therefore unsure to whom the responsible would be deletated or any records retention requirement if one is in place, including applicant's right to request data deletion or engage in other forms of redress." 19 63A 3.1.4 23 1075-1077 disaggle. We are concerned that not all if deeral agencies have Senior Agency Officials for Privacy, and are therefore unsure to whom the responsible would be deletated on any records retention requirement if one is in place, including applicant's right to request data deletion or engage in other forms of redress." 18 63A 3.1.7 24 1115-1118 (or privacy privacy privacy privacy prepared to the privacy privacy prepared to the privacy privacy prepared								
Section Sect	11	63A		2.5.1	14	775-818		Create a discrete section for remote unattended identity verification methods.
Section Sect								
13	12	63A	3.	1.3.1	21	1008-1010	We applaud NIST for creating normative risk assessments requirements around non-PII data risks.	
14 63A 3.1.3. 22 1023-1025 It is unclear why summaries of privacy risk assessments would not be available to subscribers as well. 15 63A 3.1.3. 22 1033-1035 that have access to Pil gathered or retained by the CSPs. 16 63A 3.1.3. 22 1046-1052 We believe this section is suited for additional user data protections. 16 63A 3.1.3. 22 1046-1052 We believe this section is suited for additional user data protections. 17 63A 3.1.4 23 1075-1077 We appeal NST for including equity considerations so prominently in the ID proofing process, as intentional or unintentional bias in these processes is a present risk, and the outcomes are potentially damaging. 18 63A 3.1.7 24 Intentional or unintentional bias in these processes is a present risk, and the outcomes are potentially damaging. 19 63A 3.1.8 25 1126-1129 We applied NST for including equity considerations so prominently in the ID proofing process, as intentional or unintentional bias in these processes is a present risk, and the outcomes are potentially damaging. 19 63A 3.1.1 2-24 Intentional or unintentional bias in these processes is a present risk, and the outcomes are potentially damaging. 20 63A 3.1.1 2-24 Intentional or unintentional or uni							We applaud NIST for creating normative requirements on creation, mitigation, and documentation of	
We support the normative requirements of training in privacy policies for all individuals and entities 15 63A 3.1.3.2 22 1033-103S that have access to Pili gathered or retained by the CSPs. We applied NST for including equity considerations or prominently in the ID proofing process, as intentional or unintentional bias in these processes is a present risk, and the outcomes are potentially and the details of any records retention requirement if one is in place, including applicant's right to request data deletion or engage in other forms of redress." We applied NST for including equity considerations or prominently in the ID proofing process, as intentional or unintentional bias in these processes is a present risk, and the outcomes are potentially and the outcomes are potentially and the outcomes are potentially on the concerned that and addinged may not have been delegated in an SAOP does not exist, and are further concerned that such a delegated may not have required cybersecurity and privacy expertise. In the process and who is responsible if an agency does not have an SAOP or other qualified responsible party to take on these requirements. 19 63A 3.1.8 25 1116-11129 We applied will be intelligent to be deleted by subscribers, and that CSPs must comply, Reterior than 5 in ensuring that diverse populations are equitably and fairly served. 20 63A 3.1.11 27-28 1230-1234 the initial proofing event is a significant cybersecurity and privacy risk. We applied NST in ensuring that Diometric data can be requested to be deleted by subscribers, and that CSPs must comply, Reterior that of the subscribers, and that CSPs must comply, Reterior that of the subscribers and the subscribers, and that CSPs must comply and the subscribers and the s	13	63A	3.	1.3.1	21	1012-1017	privacy risks associated with identity proofing and enrollment.	
We support the normative requirements of training in privacy policies for all individuals and entities 15 63A 3.1.3.2 22 1033-103S that have access to Pili gathered or retained by the CSPs. We applied NST for including equity considerations or prominently in the ID proofing process, as intentional or unintentional bias in these processes is a present risk, and the outcomes are potentially and the details of any records retention requirement if one is in place, including applicant's right to request data deletion or engage in other forms of redress." We applied NST for including equity considerations or prominently in the ID proofing process, as intentional or unintentional bias in these processes is a present risk, and the outcomes are potentially and the outcomes are potentially and the outcomes are potentially on the concerned that and addinged may not have been delegated in an SAOP does not exist, and are further concerned that such a delegated may not have required cybersecurity and privacy expertise. In the process and who is responsible if an agency does not have an SAOP or other qualified responsible party to take on these requirements. 19 63A 3.1.8 25 1116-11129 We applied will be intelligent to be deleted by subscribers, and that CSPs must comply, Reterior than 5 in ensuring that diverse populations are equitably and fairly served. 20 63A 3.1.11 27-28 1230-1234 the initial proofing event is a significant cybersecurity and privacy risk. We applied NST in ensuring that Diometric data can be requested to be deleted by subscribers, and that CSPs must comply, Reterior that of the subscribers, and that CSPs must comply, Reterior that of the subscribers and the subscribers, and that CSPs must comply and the subscribers and the s								
15 63A 3.1.3.2 22 1033-1035 that have access to PII gathered or retained by the CSPs. Amend "and the details of any records retention requirement if one is in place" to "and the details of any records retention requirement if one is in place to "and the details of any records retention requirement if one is in place, including applicant's right to request data deletion or engage in other forms of redress." We appliaud NIST for including equity considerations so prominently in the ID proofing process, as intentional or unintentional bias in these processes is a present risk, and the outcomes are potentially intentional to requirement if one is in place, including applicant's right to request data deletion or engage in other forms of redress." We appliaud NIST of including equity considerations so prominently in the ID proofing process, as intentional or unintentional or unintentional bias in these processes is a present risk, and the outcomes are potentially intentional to requirement if one is in place, including applicant's right to request data deletion or engage in other forms of redress." We appliaud NIST of including equity considerations so prominently in the ID proofing process, as intentional or unintentional bias in these processes is a present risk, and the outcomes are potentially intentionally and research and the opposition of the expression of proofing and processes or present risk, and the outcomes are potentially in unintentional to the expression of the process, as a ment of expression of proofing expects as a present risk, and the outcomes are potentially in unintentional to the expression of the process and who is responsible if an agency does not have an SAOP or other qualified responsible party to take on these requirements. Using the process and who i	14	63A	3.	1.3.1	22	1023-1025	It is unclear why summaries of privacy risk assessments would not be available to subscribers as well.	Require privacy risk assessments to be available to subscribers as well.
Amend "and the details of any records retention requirement if one is in place" to "and the details of any records retention requirement if one is in place" to "and the details of any records retention requirement if one is in place. Including applicant's right to request data deletion or engage in other forms of redress." We appliad NIST for including equity considerations so prominently in the ID proofing process, as intentional or unintentional bias in these processes is a present risk, and the outcomes are potentially damaging. We are concerned that not all federal agencies have Senior Agency Officials for Privacy, and are therefore unsure to whom this responsibility would be delegated if an SADP does not exist, and are further concerned that such a delegate may not when the required cybersecurity and privacy expertise. If a concerned that such a delegate may not a de								
15 63A 3.1.3 2 1045-1052 We believe this section is suited for a diditional user data protections. 17 63A 3.1.4 23 1075-1077 damaging. 18 63A 3.1.7 24 1116-1138 to explain MST for including equity and privacy risk. 19 63A 3.1.8 12 1126-1129 We are concerned that not all federal agencies have Senior Agency Officials for Privacy, and are therefore unsure to whom this responsibility would be delegated if an SAOP does not exist, and are further concerned that such a delegate not have on the reforming on the profit of the profit o	15	63A	3.	1.3.2	22	1033-1035	that have access to PII gathered or retained by the CSPs.	
15 63A 3.1.3 2 1045-1052 We believe this section is suited for a diditional user data protections. 17 63A 3.1.4 23 1075-1077 damaging. 18 63A 3.1.7 24 1116-1138 to explain MST for including equity and privacy risk. 19 63A 3.1.8 12 1126-1129 We are concerned that not all federal agencies have Senior Agency Officials for Privacy, and are therefore unsure to whom this responsibility would be delegated if an SAOP does not exist, and are further concerned that such a delegate not have on the reforming on the profit of the profit o								
We appliad MIST for including equity considerations so prominently in the ID proofing process, as intentional or unintentional bias in these processes is a present risk, and the outcomes are potentially damaging. We are concerned that not all federal agencies have Senior Agency Officials for Privacy, and are therefore unsure to whom this responsibility would be delegated if an SAOP does not exist, and are further concerned that such a delegate may not have the required cybersecurity and privacy expertise therefore unsure to whom this responsibility would be delegated if an SAOP does not exist, and are further concerned that such a delegate may not have the required cybersecurity and privacy expertise therefore unsure to whom this responsibility would be delegated if an SAOP does not exist, and are further concerned that such a delegate may not have the required cybersecurity and privacy expertise. 18 63A 3.1.7 24 1116-1118 (be perform this function as written. 19 63A 3.1.8 25 1126-1129 We appliad NIST in ensuring that diverse populations are equitably and fairly served. We appliad NIST in ensuring that biometric data in circumstances where it is no longer needed after the complex of			_					
intentional or unintentional bias in these processes is a present risk, and the outcomes are potentially damaging. We are concerned that not all federal agencies have Senior Agency Officials for Privacy, and are therefore unsure to whom this responsibility would be delegated if an SAOP does not exist, and are further concerned that such a delegate may not have the required cybersecurity and privacy expertise. 18 63A 3.1.7 24 1116-1118 to perform this function as written. 19 63A 3.1.8 2 1126-1129 We applaud NIST in ensuring that diverse populations are equitably and fairly served. We applaud NIST in ensuring that itoimetric data can be requested to be deleted by subscribers, and that CSPs must comply. Retention of biometric data in circumstances where it is no longer needed after the initial proofing event is a significant references as an option for identity proofing. In various communities and across certain industries, this is a more viable option—and sometimes the only viable 21 63A 3.1.13 33 1412 option—than other methods of proofing. We believe that statements recorded on public blockchains could also suffice if multiple data points are referenced to demonstrate a relationship between the applicant's reference. TDC does not seek to prescribe, however, the standards or requirements needed to create certainty in such a relationship. We merely want to keep the door open to the technology as a method of verification in the support the inclusion of non-biometric proofing methods. Due to personal or cultural beliefs, levels of technical literacy, or cybersecurity and privacy concerns, certain individuals or populations will refleve to go through an identity proofing process if biometrics are involved. We suggest adding "blockchain-based verification" to the list of example verification methods in this section.	16	63A	3.	1.3.2	22	1046-1052		requirement if one is in place, including applicant's right to request data deletion or engage in other forms of redress."
17 63A 3.1.4 23 1075-1077 damaging. We are concerned that not all federal agencies have Senior Agency Officials for Privacy, and are therefore unsure to whom this responsibility would be delegated if an SAOP does not exist, and are further concerned that such a delegate may not have the required cybersecurity and privacy expertise 18 63A 3.1.7 24 1116-1118 to perform this function as written. 19 63A 3.1.8 25 1126-1129 We applaud NIST in ensuring that diverse populations are equitably and fairly served. We applaud NIST in ensuring that biometric data can be requested to be deleted by subscribers, and that CSPs must comply. Retention of biometric data in circumstances where it is no longer needed after the initial proofing event is a significant cybersecurity and privacy risk. We applaud NIST in ensuring that biometric data in circumstances where it is no longer needed after the initial proofing event is a significant cybersecurity and privacy risk. We applaud NIST or including applicant references as an option for identity proofing, in various communities and across certain industries, this is a more viable option—and sometimes the only viable observed the decendance of the proof of								
We are concerned that not all federal agencies have Senior Agency Officials for Privacy, and are therefore unsure to whom this responsibility would be delegated if an SAOP does not exist, and are further concerned that such a delegate may not have the required cybersecurity and privacy expertise. 18 63A 3.1.7 24 1116-1118 to perform this function as written. 19 63A 3.1.8 25 1126-1129 We applaud NIST in ensuring that diverse populations are equitably and fairly served. We applaud NIST in ensuring that biometric data can be requised to be deleted by subscribers, and that CSPs must comply. Retention of biometric data in circumstances where it is no longer needed after the initial proofing event is a proofing event is a communities and across certain industries, this is a more viable option—and sometimes the only viable 21 63A 3.1.13 33 1412 option—than other methods of proofing. We believe that statements recorded on public blockchains could also suffice if multiple data points are referenced to demonstrate a relationship. We merely want to keep the door open to the technology as a method of verification in 22 63A 3.1.13 34 1468-1469 this circumstance. We support the inclusion of non-biometric proofing methods. Due to personal or cultural beliefs, levels of technical literacy, or cybersecurity, and privacy concerns, certain industries reinholded or provided or provided or provided or propried to the technology as a method of verification in 4 we support the inclusion of non-biometric proofing methods. Due to personal or cultural beliefs, levels of technical literacy, or cybersecurity and privacy concerns, certain industries reinholded or possible of the decining an alternative is 1 to the support the inclusion of non-biometric proofing methods. Due to personal or cultural beliefs, levels of technical literacy, or cybersecurity and privacy concerns, certain industries are involved. Creating an alternative is	17	624		2 4 4	22	1075 1077		
therefore unsure to whom this responsibility would be delegated if an SAOP does not exist, and are further concerned that such a delegate may not have the required cybersecurity and privacy expertise. 18 63A 3.1.7 24 1116-1118 to perform this function as written. 19 63A 3.1.8 25 1126-1129 We applaud NIST in ensuring that diverse populations are equitably and fairly served. We applaud NIST in ensuring that biometric data can be requested to be deleted by subscribers, and that CSPs must comply. Retained to fair incrimentances where it is no longer needed after the initial proofing event is a significant cybersecurity and privacy risk. We applaud NIST for including applicant references as an option for identity proofing. In various communities and across certain industries, this is a more viable option—and sometimes the only viable communities and across certain industries, this is a more viable option—and sometimes the only viable of the efferenced to demonstrate a relationship between the applicant and the applicant is reference. TOC does not seek to prescribe, however, the standards or requirements needed to create certainty in such a relationship. We merely want to keep the door open to the technology as a method of verification. We suggest adding "blockchain-based verification" to the list of example verification methods in this section. We suggest adding "blockchain-based verification" to the list of example verification methods in this section.	1/	63A		3.1.4	23	10/5-10//		
further concerned that such a delegate may not have the required cybersecurity and privacy expertise further concerned that such a delegate may not have the required cybersecurity and privacy expertise further concerned that such a delegate may not have the required cybersecurity and privacy expertise further concerned that such a delegate may not have the required cybersecurity and privacy expertise further concerned that such a delegate may not have the required cybersecurity and privacy expertise further concerned that such a delegate may not have the required cybersecurity and privacy expertise further concerned that such a delegate may not have the required cybersecurity and privacy expertise further concerned that such a delegate may not have the required cybersecurity and privacy expertise further concerned that such a delegate may not have the required cybersecurity and privacy expertise further concerned that such a delegate may not have the required cybersecurity and privacy expertise further concerned that such a delegate may not have the required cybersecurity and privacy expertise further concerned that such a delegate may not have the required cybersecurity and privacy expertise further concerned that such a delegate may not have the such as the palpidan title of the sequirements. Clarify the process and who is responsible if an agency does not have an SAOP or other qualified responsible party to take on these requirements. Clarify the process and who is responsible if an agency does not have an SAOP or other qualified responsible party to take on these requirements. Clarify the process and who is responsible if an agency does not have an SAOP or other qualified responsible party to take on these requirements. Clarify the process and who is responsible if an agency does not have an SAOP or other qualified responsible party to take on these requirements. Clarify the process and who is responsible if an agency does not have an SAOP or other qualified responsible party end. We appli								
18 63A 3.1.7 24 1116-1118 to perform this function as written. these requirements. 19 63A 3.1.8 25 1126-1129 We applaud NIST in ensuring that biometric data can be requested to be deleted by subscribers, and that CSPs must comply. Retention of biometric data in circumstances where it is no longer needed after 20 63A 3.1.11 27-28 1230-1234 the initial proofing event is a significant cybersecurity and privacy risk. 20 63A 3.1.13 33 1412 Option—than other methods of proofing. 21 63A 3.1.13 33 1412 Option—than other methods of proofing. We believe that statements recorded on public blockchains could also suffice if multiple data points are referenced to demonstrate a relationship between the applicant's reference. TDC does not seek to prescribe, however, the standards or requirements needed to create certainty in such a ralationship. We merely want to keep the door open to the technology as a method of verification in 468-469 this circumstance. 22 63A 3.1.13.5 34 1468-1469 this circumstance. We support the inclusion of non-biometric proofing methods. Due to personal or cultural beliefs, levels of technical literacy, or cybersecurity and privacy concerns, certain individuals or populations will refuse to go through an identity proofing process if biometrics are involved. Creating an alternative is							· · · · ·	Clarify the process and who is responsible if an agency does not have an SAOP or other qualified responsible party to take on
19 63A 3.1.8 25 1126-1129 We applaud NIST in ensuring that diverse populations are equitably and fairly served. We applaud NIST in ensuring that biometric data can be requested to be deleted by subscribers, and that CSPs must comply. Retention of biometric data in circumstances where it is no longer needed after 20 63A 3.1.11 27-28 1230-1234 the initial proofing event is a significant cybersecurity and privacy risk. We applaud NIST for including applicant references as an option for identity proofing. In various communities and across certain industries, this is a more viable option—and sometimes the only viable 21 63A 3.1.13 33 1412 option—than other methods of proofing. We believe that statements recorded on public blockchains could also suffice if multiple data points are referenced to demonstrate a relationship between the applicant and the applicant's reference. TDC does not seek to prescribe, however, the standards or requirements needed to create certainty in such a relationship. We merely want to keep the door open to the technology as a method of verification in We suggest adding "blockchain-based verification" to the list of example verification methods in this section. We support the inclusion of non-biometric proofing methods. Due to personal or cultural beliefs, levels of technical literacy, or cybersecurity and privacy concerns, certain individuals or populations will refuse to got through an identity proofing process if biometrics are involved. Creating an alternative is	19	630		3 1 7	2/1	1116-1112		
We applaud NIST in ensuring that biometric data can be requested to be deleted by subscribers, and that CSPs must comply. Retention of biometric data in circumstances where it is no longer needed after 20 63A 3.1.11 27-28 1230-1234 the initial proofing event is a significant references as an option for identity proofing. In various communities and across certain industries, this is a more viable option—and sometimes the only viable 21 63A 3.1.13 33 1412 option—than other methods of proofing. We believe that statements recorded on public blockchains could also suffice if multiple data points are referenced to demonstrate a relationship between the applicant and the applicant's reference. TDC does not seek to prescribe, however, the standards or requirements needed to create certainty in such a relationship. We merely want to keep the door open to the technology as a method of verification in We suggest adding "blockchain-based verification" to the list of example verification methods in this section. We support the inclusion of non-biometric proofing methods. Due to personal or cultural beliefs, levels of technical literacy, or cybersecurity and privacy concerns, certain individuals or populations will refuse to got through an identity proofing process if biometrics are involved. Creating an alternative is								unese requirements.
that CSPs must comply. Retention of biometric data in circumstances where it is no longer needed after 20 63A 3.1.11 27-28 1230-1234 the initial proofing event is a significant cybersecurity and privacy risk. 21 63A 3.1.13 33 1412 option—than other methods of proofing. 21 63A 3.1.13 33 1412 option—than other methods of proofing. 3	13	U3A	 	0	-23	1120 1123		
20 63A 3.1.11 27-28 1230-1234 the initial proofing event is a significant cybersecurity and privacy risk. We applaud NIST for including applicant references as an option for identity proofing. In various communities and across certain industries, this is a more viable option—and sometimes the only viable 21 63A 3.1.13 33 1412 option—than other methods of proofing. We believe that statements recorded on public blockchains could also suffice if multiple data points are referenced to demonstrate a relationship between the applicant and the applicant's reference. TDC does not seek to prescribe, however, the standards or requirements needed to create certainty in such a relationship. We merely want to keep the door open to the technology as a method of verification in 22 63A 3.1.13.5 34 1468-1469 this circumstance. We support the inclusion of non-biometric proofing methods. Due to personal or cultural beliefs, levels of technical literacy, or cybersecurity and privacy concerns, certain individuals or populations will refuse to got through an identity proofing process if biometrics are involved. Creating an alternative is			1					
We applaud NIST for including applicant references as an option for identity proofing. In various communities and across certain industries, this is a more viable option—and sometimes the only viable as a state of the proofing. We believe that statements recorded on public blockchains could also suffice if multiple data points are referenced to demonstrate a relationship between the applicant and the applicant's reference. TDC does not seek to prescribe, however, the standards or requirements needed to create certainty in such a relationship. We merely want to keep the door open to the technology as a method of verification in we suggest adding "blockchain-based verification" to the list of example verification methods in this section. We support the inclusion of non-biometric proofing methods. Due to personal or cultural beliefs, levels of technical literacy, or cybersecurity and privacy concerns, certain individuals or populations will refuse to got through an identity proofing process if biometrics are involved. Creating an alternative is	20	63A	3	.1.11	27-28	1230-1234		
communities and across certain industries, this is a more viable option—and sometimes the only viable 3.1.13 33 1412 option—than other methods of proofing. We believe that statements recorded on public blockchains could also suffice if multiple data points are referenced to demonstrate a relationship between the applicant and the applicant's reference. TDC does not seek to prescribe, however, the standards or requirements needed to create certainty in such a relationship. We merely want to keep the door open to the technology as a method of verification in We suggest adding "blockchain-based verification" to the list of example verification methods in this section. We support the inclusion of non-biometric proofing methods. Due to personal or cultural beliefs, levels of technical literacy, or cybersecurity and privacy concerns, certain individuals or populations will refuse to got through an identity proofing process if biometrics are involved. Creating an alternative is	20	03/1	,		27 20	ILUU ILU		
21 63A 3.1.13 33 1412 option—than other methods of proofing. We believe that statements recorded on public blockchains could also suffice if multiple data points are reference. TDC does not seek to prescribe, however, the standards or requirements needed to create certainty in such a relationship. We merely want to keep the door open to the technology as a method of verification in 22 63A 3.1.3.5 34 1468-1469 this circumstance. We support the inclusion of non-biometric proofing methods. Due to personal or cultural beliefs, levels of technical literacy, or cybersecurity and privacy concerns, certain individuals or populations will refuse to got through an identity proofing process if biometrics are involved. Creating an alternative is								
We believe that statements recorded on public blockchains could also suffice if multiple data points are referenced to demonstrate a relationship between the applicant and the applicant's reference. TDC does not seek to prescribe, however, the standards or requirements needed to create certainty in such a relationship. We merely want to keep the door open to the technology as a method of verification in a relationship. We merely want to keep the door open to the technology as a method of verification in we suggest adding "blockchain-based verification" to the list of example verification methods in this section. We support the inclusion of non-biometric proofing methods. Due to personal or cultural beliefs, levels of technical literacy, or cybersecurity and privacy concerns, certain individuals or populations will refuse to go through an identity proofing process if biometrics are involved. Creating an alternative is	21	63A	3	.1.13	33	1412		
referenced to demonstrate a relationship between the applicant and the applicant's reference. TDC does not seek to prescribe, however, the standards or requirements needed to create certainty in such a relationship. We merely want to keep the door open to the technology as a method of verification in We suggest adding "blockchain-based verification" to the list of example verification methods in this section. We support the inclusion of non-biometric proofing methods. Due to personal or cultural beliefs, levels of technical literacy, or cybersecurity and privacy concerns, certain individuals or populations will refuse to got through an identity proofing process if biometrics are involved. Creating an alternative is								
does not seek to prescribe, however, the standards or requirements needed to create certainty in such a relationship. We merely want to keep the door open to the technology as a method of verification in We suggest adding "blockchain-based verification" to the list of example verification methods in this section. We suggest adding "blockchain-based verification" to the list of example verification methods in this section. We suggest adding "blockchain-based verification" to the list of example verification methods in this section. We suggest adding "blockchain-based verification" to the list of example verification methods in this section. The property of the including and privacy concerns, certain individuals or populations will refuse to go through an identity proofing process if biometrics are involved. Creating an alternative is			1					
a relationship. We merely want to keep the door open to the technology as a method of verification in 22 63A 3.1.13.5 34 1468-1469 this circumstance. We suggest adding "blockchain-based verification" to the list of example verification methods in this section. We suggest adding "blockchain-based verification" to the list of example verification methods in this section. We compare the inclusion of non-biometric proofing methods. Due to personal or cultural beliefs, levels of technical literacy, or cybersecurity and privacy concerns, certain individuals or populations will refuse to go through an identity proofing process if biometrics are involved. Creating an alternative is	1		l					
We support the inclusion of non-biometric proofing methods. Due to personal or cultural beliefs, levels of technical literacy, or cybersecurity and privacy concerns, certain individuals or populations will refuse to go through an identity proofing process if biometrics are involved. Creating an alternative is			1					
of technical literacy, or cybersecurity and privacy concerns, certain individuals or populations will refuse to go through an identity proofing process if biometrics are involved. Creating an alternative is	22	63A	3.1	.13.5	34	1468-1469	this circumstance.	We suggest adding "blockchain-based verification" to the list of example verification methods in this section.
refuse to go through an identity proofing process if biometrics are involved. Creating an alternative is							We support the inclusion of non-biometric proofing methods. Due to personal or cultural beliefs, levels	
			1				of technical literacy, or cybersecurity and privacy concerns, certain individuals or populations will	
23 63A 4.2.6.1 42 1706 therefore necessary.			l					
	23	63A	4.	2.6.1	42	1706	therefore necessary.	

				TDC supports fully digital identity proofing methods, as they can provide significant improvements in	
				speed, security, and privacy. We also would like to see digital wallets and blockchain-based	We suggest adding "or digital wallet/blockchain based addressor account" in section 2a. We suggest adding "or digital
24	63A	4.2.6.2	43	1743-1751 communications added to this list of approved verification methods.	wallet/blockchain based address or account" in section 2b. We suggest adding "or digital wallet" in section 2c.
				We do not believe CSPs must retain biometric data in order to support account recovery, non-	Change "Shall" to "May." Or, approve other non-biometric pathways to to achieve these requirements, and combine them
25	63A	4.3.3	45		with the biometric options in this section giving CSPs optionality, and keep "Shall."
				The applicant should also have the ability to request deletion of this video after the identity proofing	
				process has been successfully completed, as it is a privacy and cybersecurity risk if the CSPs retain the	Add the following provision after line 1876: "The CSP shall delete any video session(s) recorded during the identity proofing
26	63A	4.3.7	47	1874-1874 data.	process upon the applicant's request."
				We applaud NIST for including this provision. It is critical that subscribers are able to ensure their	
27	63A	5.4	52	1988-1990 sensitive data is not being 'held captive' by a CSP after the relationship is ended.	
				We greatly appreciate NIST including a comprehensive section on privacy. Not only are these	
		_		informative guidelines practical, but they signal NIST's commitment to privacy when setting normative	
28	63A	7	57	2034 requirements for digital identity practices.	
				As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be	We are a second addition to district the second control of the second and a second and a second and a second as
29	63A	8.3	66	forward looking toward the next communications platforms where subscribers will spend their time in 2357 the digital age.	We recommend adding in digital/blockchain based wallets and decentralized protocols or dApps as an example method of valid code transfer.
29	DOM	0.3	00	We greatly appreciate NIST including a comprehensive section on equity. Not only are these	valid code transfer.
				informative guidelines practical, but they signal NIST's commitment to equity when setting normative	
30	63A	q	69	2435 requirements for digital identity practices.	
30	05A		03	We appreciate NIST's normative guidance on minimizing and protecting retained data, and publishing	
31	63B	2.4.3	9	640-650 overall privacy requirements in the authentication process.	
	035	271.0	Ť	Does NIST consider any blockchain-based digital wallets or cryptography sufficient in meeting these	Clarification is needed on whether blockchain-based digital wallets meet these requirements. We would posit that they do
32	63B	3.1.6.1	25	1100 requirements?	meet the requirements.
				Does NIST consider any blockchain-based digital wallets or cryptography sufficient in meeting these	Clarification is needed on whether blockchain-based digital wallets meet these requirements. We would posit that they do
33	63B	3.1.7.1	26	1142 requirements?	meet the requirements.
				We applaud NIST for supporting the usage of subscriber-controlled wallets. We believe this is a wise	
				choice that will allow greater subscriber control over their identity attributes, and may foster a market	
				for wallet creators. We are unclear however if this definition of subscriber-controlled wallets includes,	Clarify whether subscriber-controlled wallet definition includes blockchain-based wallets. We argue that they should and do
34	63B	3.1.7.3	27	1171 or could include, blockchain-based wallets.	meet the definition and requirements.
				We support NIST's decision to make a normative requirement that biometric data shall be erased	
				immediately after authentication. Not only does this protect user privacy broadly, but it also	
25	can	2472	27	significantly lowers the risk of collusion between authenticators that could use such biometric data for	
35	63B	3.1.7.3	27	1184 ill purposes. We strongly support the normative requirement for alternatives to biometric data during	
36	63B	3.2.3	30	1265-1266 authentication.	
37	63B	3.2.3		1273-1274 We applaud NIST for requiring normative equity standards in the authentication process.	
3,	035	5.2.5	50	2275 127 The application of requiring normative equity standards in the detricitied on process.	
				We believe that local biometric comparison should be the standard, but recognize that instances will	We encourage NIST to make local biometric comparisons the required normative method, and allow centralized verifier
38	63B	3.2.3	31	1298-1299 occur where local comparison is not viable or does not meet certain authentication requirements.	comparison as an alternative method if the local method is not viable.
					We would like to see this provision removed completely. As a second alternative, this section should be rewritten to ensure
				We strongly disagree with this practice of biometric data being used for training models, especially as	that user consent is required for both training of comparison algorithms and for research purposes. As currently written, it
39	63B	3.2.3	31	1318-1320 written.	would only be required for research purposes.
				While we do not agree with the broader provision on model training that this point on data erasure	
40	63B	3.2.3	31	1321-1322 refers to, we do appreciate NIST's efforts to include data erasure requirements.	
				Does this provision preclude the use of blockchain wallets and networks as viable methods to achieve	
				these normative requirements in this section? If so, we believe that their exclusion as a viable method	
				from this section would extend to most if not all other sections throughout the entirety of 800-63-4	
41	can	2 2 44	20	draft 2. Is this the case? And is there any distinction made between "hot" and "cold" blockchain wallets, 1499-1500 or permissioned and permissionless blockchain networks?	
41	63B	3.2.11	36	As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be	the normative requirements of the entire publication. We argue that blockchain wallets can/do meet these requirements.
				forward looking toward the next communications platforms where subscribers will spend their time in	We recommend adding in digital/blockchain based wallets and decentralized protocols or dApps as an example method of
42	63B	4.6	47	1848-1849 the digital age.	receiving account notifications.
72	038	4.0	- "	We greatly appreciate NIST including a comprehensive section on privacy. Not only are these	
			1	informative guidelines practical, but they signal NIST's commitment to privacy when setting normative	
43	63B	7	61	2078 requirements for digital identity practices.	
	035	·	1	We greatly appreciate NIST including a comprehensive section on equity. Not only are these	
			1	informative guidelines practical, but they signal NIST's commitment to equity when setting normative	
44	63B	9	75	2514 requirements for digital identity practices.	
				As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be	
				forward looking toward the next communications platforms where subscribers will spend their time in	
45	63C	3	9	635-636 the digital age.	We recommend adding in digital/blockchain based wallets as an example in this section in addition to web browsers.
			1	We greatly appreciate the inclusion of pseudonymous pairwise identifiers, as we believe this practice	
46	63C	3.3.1	15	826 will minimize data retention and increase subscriber privacy and overall cybersecurity.	
.			١.	We applaud NIST for recognizing the importance of creating privacy policies to mitigate and prevent	
47	63C	3.3.1.1	15	843-845 subscriber data correlation.	
48	63C	3.3.1.1	15	We applaud NIST for recognizing the importance of preventing PPI and data mapping to mitigate and	
48	630	3.3.1.1	15	854-856 prevent subscriber identity recreation.	
49	63C	3.3.1.3	16	871 This section should also include subscriber right to delete PPI attribution to their account.	At the end of line 871, add "and is given clear steps on their option and right to request deletion of any shared PPIs."
49	030	3.3.1.3	10	We applaud NIST for recognizing the importance of creating privacy policies to mitigate and prevent	Processes on an experience of an analysis given occur sceps on their option and right to request deletion or any stidied PPIs.
	63C	3.3.1.3	16	877-880 subscriber data correlation.	
50					

1 St. 14 Jan 12 St. 20 common configuration from ording applications and street and programmed and the common configuration of the conf				1		We believe the wording in this provision, specifically in line 932, is inconsistent with how NIST has set	
Sign of the comment o	51	620	2.4	17	022		Change "the terms of the trust agreement need to" to "the terms of the trust agreement Shall "
1 3 1 3 1 3 1 2 1 0 1 3 1 2 1 0 1 3 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	31	030	5.4	1/	952	normative requirements throughout the rest of this publication.	Charge the terms of the trust agreement need to to the terms of the trust agreement shall.
1 3 1 3 1 3 1 2 1 0 1 3 1 2 1 0 1 3 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	52	630	3 / 1	18	9/18	The term "no additional requirements" is yaque: what do "additional requirements" include in scope?	Clarify what "additional requirements" mean
1							
20 45 3.5 21 Sign you where what the trace of interest relative and experimental flower what person provides in the sale of the person of the		050	5.112		, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	The recommend duding in a normalize requirement for data detection.	Time to the 555 to State Tetalition, aggregation, detection, and discussive to time parties.
20 45 3.5 21 Sign you where what the trace of interest relative and experimental flower what person provides in the sale of the person of the	54	63C	3.4.2	20	980-983	We commend NIST for adding privacy risk assessments as a normative requirement to this section	
Solve to the conference representation of reference representation of the conference representation							Define "redress" and provide examples.
special control of the control of th							
special control of the control of th							Clarification on "third party service" responsibilities to remain compliant, consequences if they do not meet these
90 (15.1.) 27 (20) Comment and the processor of the systems or a comment requirement in Noticease (15.1.) 28 (20) Comment and the processor of the systems of the processor of t	56	63C	3.5	22	1030		
As digital interforcings customer to read the mid commence constraint in adopt of them. It is control to be forcing and provided that is a control to an experiment of the provided that is a control to an experi						We appreciate NIST adding the practice of key rotation as a normative requirement in federated	
See N. K. 1.5.1 2, 12 100-150, the digital rags. We regulated NOT or including submariant effective and anomalian equipment. The paratice serves to the control of the digital rags. We applied NOT or including submariant effective and anomalian equipment. The paratice serves to the control of the digital rags. We applied NOT or including submariant effective and the control of the digital rags. We applied NOT or including submariant effective and the control of the digital rags. We applied NOT or including submariant effective and the control of the digital rags. We applied NOT or including submariant effective and the control of the digital rags. We applied NOT or including submariant effective and the control of the digital rags. We applied NOT or including submariant effective and the control of the digital rags. We applied NOT or including submariant effective and the control of the digital rags. We applied NOT or including submariant effective and the control of the digital rags. We applied NOT or including submariant effective and the control of the digital rags. We applied NOT or including submariant effective and the control of the digital rags. We applied NOT or including submariant effective and the control of the digital rags. We applied NOT or including submariant effective and the control of the digital rags. We applied NOT or including submariant effective and the control of the digital rags. We applied NOT or including submariant effective and the control of the digital rags. We applied NOT or including submariant effective and the control of the digital rags. We applied NOT or including submariant effective and the control of the digital rags. We applied NOT or including submariant effective and the control of th	57	63C	3.5.1	23	1051	instances. We believe this should be a standard practice in identity systems.	
9						As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be	
The exposed MS for including otherwise establishors as a normative regardeness. This practice serves to the control of the con						forward looking toward the next communications platforms where subscribers will spend their time in	We recommend adding in digital/blockchain based wallets or public addresses as an example method of valid IdP key
services of the second	58	63C	3.5.1	23	1056-1057	the digital age.	identification and verification.
services of the second							
We separed biff for ricksleding the growthstorn as a normalise requirement. Exclusing expectations of production and the frequirement of sections where the sequence of control where the						We applaud NIST for including software attestations as a normative requirement. This practice serves	
portico must return this requirement contentity means to those protocols will be built with this is a technical speaking of partners. 15	59	63C	3.5.3	23	1073	to protect subscribers from engaging with fraudulent RPs that would improperly use subscriber data.	
60 GIC S 5 23 100% fines a testinate for measurement great the protocol does not have the testhesial capability of transferring (C 5) and C 5 3 100% fines a testinate from supproved protocol and will become beneficial to our education on the control of the cont							
60 GC 35 72 1305-100 has been been been been been been been bee							
61 OSC 3.6 2) 101-1105 late pluming provides in a secessary protocy requirements throughout the rest of this document, and the provides of the				1			
61 65C 5. 10 27 121 jbt -1006 data sharing over time. 62 65C 9. 27 121 jbt -1006 data sharing over time. 63 65C 9. 27 122 jbt -1006 data sharing over time. 64 65C 9. 28 122 jbt -1006 data sharing over time. 65 65C 9. 3.1 22 jbt -1006 data sharing over time. 66 65C 9. 3.1 22 jbt -1006 data sharing over time. 67 65C 9. 3.1 22 jbt -1006 data sharing over time. 68 65C 9. 3.1 22 jbt -1006 data sharing over time. 69 65C 9. 3.1 22 jbt -1006 data sharing over time. 69 65C 9. 3.1 22 jbt -1006 data sharing over time. 60 65C 9. 3.1 2	60	63C	3.6	23	1096-1097		
Column 1							
62 63 3.9 27 123 The "Should" in the 1233 should be changed on "Shall." A very accommend that out all facel agencies have been agency Officials for Phasey, and are therefore usual to the state of the	61	63C	3.6	23	1104-1106		
we are concerned that not all federal agreecies have Senior Agency Children's device and and entered therefore success to show this responsible you've the delegated if an SAGP or charter the specified of the SAGP or charter the therefore success to show that specified in SAGP or charter the specified of the SAGP or charter the SAGP or charter the specified of the SAGP or charter the SAGP or charte				_			
herefore usuare to whom this responsibility would be delegated in a ASOP does not exist, and are further concerned that such a delegated may not have the required spherescurity and privacy operation. These requirements of the requirements of the requirements. Given 39 28 1215 to perform this function is written. Given 39 29 1156 whom the improvision of the function is written. Given 39 20 1215 to perform this function is written. Given 39 20 1215 to perform this function is written. Given 39 20 1215 to perform this function is written. Given 39 20 122 122 to the term "security incident" is too broad. What does is encompass? Given 39 20 122 122 to the term "security incident" is too broad. What does is encompass? Given 39 20 122 122 to the term "security incident" is too broad. What does is encompass? Given 39 20 122 122 to the term "security incident" is encompass? Given 39 20 122 122 to the term "security incident" is encompass? Given 39 20 122 122 to the term security incident is encompass? Given 39 20 122 122 to the term security incident is encompass? Given 39 20 122 122 to the term security incident is encompass? Given 30 20 122 122 to the term security incident is encompass? Given 30 20 122 122 to the term security incident is encompass? Given 30 20 122 122 to the term security incident is encompass? Given 30 20 122 122 to the term security incident is encompass? Given 30 20 122 122 to the term security incident is encompass? Given 30 20 122 122 to the term security incident is encompass? Given 30 20 122 122 to the term security incident is encompass? Given 30 20 20 122 122 to the term security incident is encompass? Given 30 20 20 20 20 20 20 20 20 20 20 20 20 20	62	63C	3.9	27	1231		Change "Should" to "Shall."
further concerned that such a delegate may not have the required cybersecurity and privacy opens. Clarify the process and who is responsible if an agency does not have an SAOP or other qualified responsible party to take on the company of the subscriber opin in, trust agreements. May request that identify attributes the harmonic of the subscriber opin in, trust agreements. May requise that identify attributes the harmonic opin of the subscriber opin in, trust agreements. May requise that defently attributes the harmonic opin of the subscriber opin in, trust agreements. May requise that defently attributes the harmonic opin of the subscriber opin in, trust agreements. May requise that the subscriber opin in trust agreements May requise that the subscriber opin on the subscriber opin in trust agreements. May requise the subscriber opin in trust agreements May requise that the subscriber opin on the subscriber opin in trust agreements May requise that the subscriber opin on the subscriber opin in trust agreements. May requise the subscriber opin in trust agreements May requise that the subscriber opin on the subscriber opin in this section. The subscriber opin in trust agreements May requise that the subscriber opin opin opin opin opin opin opin opin							
63 63C 3,3 28 127 for perform this function as written. 64 63C 3,3 28 127 for perform this function as written. 65 63C 3,3 28 127 for perform this function as written. 66 63C 3,3 28 127 for perform this function and written. 67 63C 3,3 28 127 for perform this function and written. 68 63C 3,3 28 127 for perform this function and written. 69 63C 3,3 28 127 for perform this function and written. 60 63C 3,3 28 127 for perform this function and written. 60 63C 3,3 28 127 for perform this function and written. 60 63C 3,3 28 128 for performance that it would allow inappropriate control was a performance or written the sopposition of this section. 60 63C 3,3 28 128 for performance that it would allow inappropriate attributes to be collected and shared. 61 63C 3,3 2 30 1354 136 for ownered that it would allow inappropriate attributes to be collected and shared. 62 63C 3,3 2 30 1355 1353 (Should or Shall be passed on. 63 63C 3,3 2 30 1355 1353 (Should or Shall be passed on. 64 63C 3,3 2 30 1355 1353 (Should or Shall be passed on. 65 65C 3,3 2 30 1355 1353 (Should or Shall be passed on. 66 65C 3,3 2 30 1355 1353 (Should or Shall be passed on. 67 65C 3,3 2 30 1355 1353 (Should or Shall be passed on. 68 65C 3,3 2 30 1355 1353 (Should or Shall be passed on. 69 65C 3,3 2 30 1355 1353 (Should or Shall be passed on. 69 65C 3,3 2 30 1355 1353 (Should or Shall be passed on. 69 65C 3,3 2 30 1355 1353 (Should or Shall be passed on. 69 65C 3,3 2 30 1355 1353 (Should or Shall be passed on. 69 65C 3,3 2 30 1355 1353 (Should or Shall be passed on. 69 65C 3,3 3 1 30 1355 (Should or Shall be passed on. 69 65C 3,3 3 1 30 1355 (Should or Shall be passed on. 69 65C 3,3 3 1 30 1355 (Should or Shall be passed on. 69 65C 3,3 3 1 30 1355 (Should or Shall be passed on. 69 65C 3,3 3 1 30 1355 (Should or Shall be passed on. 69 65C 3,3 3 1 30 1355 (Should or Shall be passed on. 69 65C 3,3 3 1 30 1355 (Should or Shall be passed or Shall be passe							
64 GC 3.9 28 1259 We believe this provision would be more clear if rewritten. 65 GC 3.9.1 28 1270 The term "security incident" is too broad. What does it encompass? Define examples of "security incident" that would trigger the data transfer provision in this section. 66 GC 3.9.1 28 1287 The term "security incident" is too broad. What does it encompass? Define examples of "security incident" that would trigger the data transfer provision in this section. 67 GC 3.10 30 1344-1346 (on whether the data tanks, place of the intermediate of the security incident that would trigger the data transfer provision in this section. 68 GC 3.10 30 1344-1346 (on whether the data tanks, place of the intermediate of the security incident that would trigger the data transfer provision in this section. 69 GC 3.10 3 134 1346 (onsemble the data tanks, place of the security incident that would trigger the data transfer provision in this section. 69 GC 3.10 3 135 1355 (Should in the security of the security incident that would stop the transfer provision in this section. 69 GC 3.10 3 135 1355 (Should in the security of the sec	63	626	2.0	20	1227		
66 63C 3.9.1 28 1270 The term "security incident" is bor broad. What does it encompass? 67 63C 3.9.1 29 128 1270 The term "security incident" is bor broad. What does it encompass? 68 63C 3.9.1 29 102 The term "security incident" is bor broad. What does it encompass? 69 63C 3.9.2 10 1344-1346-date with the control of the publishes of the control	63	63C	3.9	28	1237	to perform this function as written.	
65 G.Z 3.9.1 28 17.00 The term "security incident" is too broad. What does it encompass? Ordine examples of "security incident" that would trager the data trainfer provision in this section. Before examples of "security incident" that would trager the data trainfer provision in this section. Before examples of "security incident" that would trager the data trainfer provision in this section. Before examples of "security incident" that would trager the data trainfer provision in this section. Before examples of "security incident" that would trager the data trainfer provision in this section. Before examples of "security incident" that would trager the data trainfer provision in this section. Before examples of "security incident" that would trager the data trainfer provision in this section. Before examples of "security incident" that would trager the data trainfer provision in this section. Before examples of "security incident" that would trainger the data trainfer provision in this section. Before examples of "security incident" that would trainger the data trainfer provision in this section. Before examples of "security incident" that would trainger the data trainfer provision in this section. Before examples of "security incident" that would trainger the data trainfer provision in this section. Before examples of "security incident" that would trainger the data trainfer provision in this section. Before examples of "security incident" that would trainfer that would trainfer that the security that the security incident that that the security is not on all seasons. Before examples of "security incident" that would trainfer that sould that the security incident that the security would all that the security incident that the security would all that the security incident that the security would all that	64	630	2.0	20	1250	We heliove this provision would be more clear if rewritten	
66 6 62 3.1.0 2 30 124-1346 on whether the data May, Stould, of Shall be passed on. 67 63C 3.1.0 2 30 1344-1346 on whether the data May, Stould, of Shall be passed on. 68 63C 3.1.0 2 30 1344-1346 on whether the data May, Stould, of Shall be passed on. 69 63C 3.1.0 2 30 1344-1346 on whether the data May, Stould, of Shall be passed on. 69 63C 3.1.0 2 30 1346 concerned that it would be passed on. 60 63C 3.1.0 2 30 1346 concerned that it would be passed on. 60 63C 3.1.0 2 30 1345 concerned that it would be passed on. 60 63C 3.1.0 3 1346 concerned that it would be passed on. 60 63C 3.1.0 3 135 concerned that it would be included and shared. 61 70 63C 3.1.1 3 130 sound the state of							
We believe it's unnecessary and improper for device location and identity to be included in this list, and are unclear why. No. Would its passing this data on as a "good list passing the data on as "good list passing the data on as a "good list passing the data on as "good list passing the data on as "good list passing the data on as a "good list passing the data on as "good list passing the data on as "good list passing the data of the passing the passing the data of the passing the passing the good list passing the							
are unclear wity NST would list passing this data on as a "groot idea," but not make any determinations moved evice location from this list, and clarify any normative requirements in this provision Additional attributes" is too broad. We are unclear on what the scope of this term could entail, but are well attributed to be confirmed attributed to the commending they be used as a primary source where possible. However, we would be to see this changed from "Shall" to go as a primary source where possible. However, we would be to see this changed from "Shall" to go as a primary source where possible. However, we would be to see this changed from "Shall" to go as a primary source where possible. However, we would be seenficial to include a list of source where possible. However, we would be seenficial to include a list of source where possible. However, we would be seenficial to include a list of source where possible. However, we would be seenficial to include a list of source where possible. However, we would be seenficial to include a list of source where possible. However, we would be seenficial to include a list of source where possible were considered attribute. We strongly suggest adding normative requirements to make the earn or overled attribute. The strongly suggest adding normative requirements to make the earn or overled attribute. We strongly suggest adding normative requirements to make the earn or overled attribute. We strongly suggest adding normative requirements to make the earn or overled attribute. We strongly suggest adding normative requirements to make the earn or overled attribute. We strongly suggest adding normative requirements to include a list of the strongly suggest adding normative requirements to include a list of the strongly suggest adding normative requirements to make the earn of the strongly suggest adding normative requirements to make the earn of the strongly suggest adding normative requirements to make the east of mitotach and attribute. And the proper of the strongly sugg	- 00	030	3.5.1	20	1202		
67 6.3 3.0.2 30 1346.1346 on whether the data May, Should, or Shall be passed on the special or the special sp							
68 63 3.0.2 30 1346 Concerned that it would allow inapporpriate attribute to used a roth support attributes to used a roth would allow inapporpriate attribute to used and recommending they be used as a primary source where possible. However, we would like to see this changed from "Shalf" to use as a primary source where possible. However, we would like to see this changed from "Shalf" to use as a primary source where possible. However, we would like to see this changed from "Shalf" to change "Should" to "Shall." 70 63C 3.10.3 31 1360 examples or to link to a section of the guidelines that fully covers what these are. 81 We recommend using derived attribute bundles as a standard where and when derived attribute as a standard when and when derived attribute as a promote as a standard when and when derived attribute as a standard when and standard as a standa	67	630	3 10 2	30	1344-1346		
68 63C 3.102 30 1346 concerned that it would allow inappropriate attributes to be collected and shared. We appliad NF5 for including requirements on derived provision are not added, we appliad the society of "appropriate controls?" It would be beneficial to include a list of Change "Should" in a new additional to include a list of Change "Should" in a first to better ensure user privary and between the service of "appropriate controls?" It would be beneficial to include a list of Change "Should" in a first to better ensure user privary and the beneficial to include a list of Change "Should" in a first to better ensure user privary and the pudelines that fully covers what these are 17 63C 3.111 32 1389 Values meet the quietlenists that fully covers what these are 18 63C 3.112 32 1389 Values meet the underficiation requires of an P. We strongly suggest adding normalive requirements to ensure large and when derived attribute 18 7 63C 3.113 32 1422 values throughout all parts of SP 800-63 may be moot. 19 8 6 3 1.12 32 1423 values throughout all parts of SP 800-63 may be moot. 20 8 1.13 3 1439 Values between the capabilities to read derived attribute values, and that private data in the digital age. 21 8 6 3 1.12 35 1531 We believe subscribers should be required to be notified and must give consent to share attributes. 22 8 6 3 1.12 35 1531 We believe subscribers should be required to be roward looking toward the next communications and data platforms where subscribers will spend to roward looking toward the next communications and data platforms where subscribers will spend forward looking toward the next communications and data platforms where subscribers will spend forward looking toward the next communications and data platforms where subscribers will spend forward looking toward the next communications and data platforms where subscribers will spend forward looking toward the next convolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data	- 07	050	5.10.2	50	15111510		
We applied NST for including requirements on edirected attribute values and recommending they be used as a primary source where possible. However, we may source where possible. However, we was a formation of a special formation of the possible formation of a proportion of the possible formation. However, and the proportion of	68	63C	3.10.2	30	1346		
69 63 3.0.2 30 (351-353) Should' in an effort to better ensure user privary and cybersecurity. 70 63 3.0.3 31 1360 examples or to link to a section of the guidelines that fully covers what these are. 71 63 3.1.1 32 1389 was exampled attribute burdles and activation and verification requirements to ensure displayed role attribute burdles and the provision are not added, we are concerned that the other requirements on ensure that the other requirements on ensure that the other requirements on ensure that the other requirements on a sure to the provision are not added, we are concerned that the other requirements on ensure that the other requirements on ensure to share attribute and the standard where and that plants are subscribers will spend forward looking toward the next communications and atap plants may be subscribers will spend forward looking toward the next communications and adap plants may be subscribers will spend forward looking toward the next communications and adap plants may be subscribers will spend forward looking toward the next communications and adap plants may be subscribers will spend forward looking toward the next communications and adap plants may be subscribers will spend forward looking toward the next communications and adap plants may be subscribers will spend forward looking toward the next communications and adap plants may be subscribers will spend forward looking toward the next communications and adap plants may be subscribers will spend forward looking toward the next communications and adap plants may be subscribers will spend forward looking toward the next communications and adap plants may be subscribers will spend forward looking toward the next communications and adap plants may be subscribers will spend forward looking toward the next communications and adap plants may be subscribers will spend forward looking toward the next communications and adap plants may be subscribers will spend forward looking toward the next communications and that plants may be subscribers wi						We applaud NIST for including requirements on derived attribute values and recommending they be	
What are is included in the scope of "appropriate controls"? "It would be beneficial to include a list of became to find to a section of the guideline the scope of "appropriate controls". We recommend using derived attribute bundles as a standard where and when derived attribute and the scope of "appropriate controls". We recommend using derived attribute bundles as a standard where and when derived attribute and the scope of "appropriate controls". We recommend using derived attribute bundles as a standard where and when derived attribute and using derived attribute values, and that RPs have the capabilities to accept them. If these provisions are not added, we are concernities on servize (RPs.) and CSPs create the technical capabilities to create derived attribute values, and that RPs have the capabilities to accept them. If these provisions are not added, we are concernities on servize (RPs.) and CSPs shall ensure methods of creating, authenticating, and verifying, and accepting derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, and verifying, and accepting derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, and verifying, and accepting derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, and verifying, and accepting derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, and verifying, and accepting derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, and verifying, and accepting derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, and verifying, and accepting derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, and verifying, and accepting derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authentication, and accepting and accepting and accepting and accepting and accepti						used as a primary source where possible. However, we would like to see this changed from "Shall" to	
90 63C 3.1.0 3 31 1360 examples or to link to a section of the quiedlenes that fully covers what these are. 91 80 80 80 3.1.1 32 We recommend using derived attribute bundles as a standard where and when derived attribute 92 81 1388 values meet the authentication and verification requirements of an IP. 93 81 1380 values meet the authentication and verification requirements of an IP. 94 81 1389 values meet the authentication and verification requirements of an IP. 95 81 131 32 1422 values meet the authentication and verification requirements of the RP." 96 82 3.1.2 32 1422 values meet the authentication and verification requirements on derived attribute values, and that RPs have the capabilities to accept them. If these provisions are not added, we are concerned that the other requirements on derived attribute values. The standard practice of a substitute of the special values and the provision standard practice of the RP." 97 83 83 112 32 1433 We believe subscribers should be required to be notified and must give consent to share attributes. As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend forward looking toward the next communications and data platforms where subscribers will spend forward looking toward the next communications and data platforms where subscribers will spend forward looking toward the next communications and data platforms where subscribers will spend forward looking toward the next communications and data platforms where subscribers will spend forward looking toward the next communications and data platforms where subscribers will spend forward looking toward the next communications and data platforms where subscribers will spend forward looking toward the next communications and data platforms where subscribers will spend forward looking toward the next communication and data platforms where subscribers will spend forward looking toward the	69	63C	3.10.2	30	1351-1353		Change "Should" to "Shall."
We recommend using derived attribute bundles as a standard when derived attribute 32						What are is included in the scope of "appropriate controls?" It would be beneficial to include a list of	
71 63C 3.1.1 32 1398 Values meet the authentication and verification requirements of an P. We strongly suggest adding normative requirements or consumers continue to adopt them, if some of such testing these provisions are not added, we are concerned that the other requirements on derived attribute and the parts of 5°8 bods. 3.1.2 32 1422 Values throughout all parts of 5°8 bods. 3.1.3 32 1423 We believe subscribers should be required to be notified and must give consent to share attributes. 3.1.3 32 1493 We believe subscribers should be required to be notified and must give consent to share attributes. 3.1.2 35 1513 their time and find trusted data in the digital age. 3.1.2 35 1513 their time and find trusted data in the digital age. 3.1.2 35 1534 their time and find trusted data in the digital age. 3.1.2 35 1534 their time and find trusted data in the digital age. 3.1.3 38 1607-1608 their time and find trusted data in the digital age. 3.1.4 1828-1829 included in this section and in trust greements. 3.1.5 1828 values meet the authentication and verification and envirous discovered attribute values, and that RPs have the capabilities to accept them. If these provisions are not added, we are concerned that the other requirements on derived attribute attribute with the digital age. 3.1.5 3 1493 We believe subscribers should be required to be forward looking toward the next communications and data platforms where subscribers will spend forward looking toward the next communications and data platforms where subscribers will spend forward looking toward the next communications and data platforms where subscribers will spend forward looking toward the next communications and data platforms where subscribers will spend forward looking toward the next communications and data platforms where subscribers will spend forward looking toward the next communications and data platforms where subscribers will spend forward looking toward the next communications and data platforms where subscribers will spend forward	70	63C	3.10.3	31	1360		Define "appropriate controls"
We strongly suggest adding normative requirements to ensure ldPs and CSPs create the technical capabilities to create derived attribute values, and that RPs have the capabilities to accept them. If these provisions are not added, we are concerned that the other requirements on derived attribute methods of authenticating, verifying, and accepting derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, and verifying derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, and verifying derived attribute values." Add "IDPs and CSPs Shall ensure methods of authenticating, verifying, and accepting derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, and verifying derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, and verifying derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, and verifying derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, and verifying derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, and verifying derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, and verifying derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, and verifying derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, verifying, derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating authenticating, verifying, derived attribute values." Add "IDPs and CSPs Shall ensure methods of authenticating, verifying, derived attribute values." Add "IDPs and CSPs Shall ensure methods of authenticating, verifying, derived attribute values." Add "IDPs and CSPs Shall ensure methods of authenticating, verifying, derived attribute values." Add "IDPs and CSPs Shall ensure methods of authent							
capabilities to create derived attribute values, and that RPs have the capabilities to accept them. If these provisions are not added, we are concerned that the other requirements on derived attribute and "IDPs and CSPs Shall ensure methods of creating, authenticating, and verifying derived attribute values. RPs Shall ensure methods of authenticating, and accepting derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, and verifying derived attribute values. RPs Shall ensure methods of authenticating, verifying, and accepting derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, and verifying derived attribute values. RPs Shall ensure methods of authenticating, verifying, and accepting derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, and verifying derived attribute values. RPs Shall ensure methods of authenticating, and verifying derived attribute values. RPs Shall ensure methods of authenticating, and verifying derived attribute values. RPs Shall ensure methods of authenticating, and verifying derived attribute values. RPs Shall ensure methods of authenticating, and accepting derived attribute values. RPs Shall ensure methods of authenticating, and verifying derived attribute values. RPs Shall ensure methods of authenticating, and verifying derived attribute values. RPs Shall ensure methods of authenticating, and verifying derived attribute values. RPs Shall ensure methods of authenticating, and verifying derived attribute values. RPs Shall ensure methods of authenticating, and verifying derived attribute values. RPs Shall ensure methods of authenticating, and verifying derived attribute values. RPs Shall ensure methods of authenticating, and verifying derived attribute values. RPs Shall ensure methods of authenticating, and verifying derived attribute values. RPs Shall ensure methods of authenticating, and verified entribute values. RPs Shall ensure methods of authenticating. Ad	71	63C	3.11.1	32	1398	'	Amend line 1398 to read "instead Shall be disclosed to the RP when selective disclosure meets the requirements of the RP."
these provisions are not added, we are concerned that the other requirements on derived attribute these provisions are not added, we are concerned that the other requirements on derived attribute and "IDPs and CSPs Shall ensure methods of creating, authenticating, verifying, and accepting derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, verifying, and accepting derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, verifying, and accepting derived attribute values." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, verifying, and accepting derived attribute values." Add provision stating "Subscriber Shall be notified and required to give consent to share the attributes, and be allowed to select each discrete attribute they consent to sharing." Add "IDPs and CSPs Shall ensure methods of creating, authenticating, verifying, and accepting derived attribute values." Add provision stating "Subscriber Shall be notified and required to give consent to share the attributes, and be allowed to select each discrete attribute they consent to sharing." Add provision stating "Subscriber Shall be notified and required to give consent to share the attribute select each discrete attribute they consent to sharing." We recommend adding in blockchain based addressses or registries or verified entries as a normative example. We recommend adding in blockchain based addressses or registries or verified entries as a normative example. We recommend adding in blockchain based addressses or registries or verified entries as a normative example. We recommend adding blockchain based addressses or registries or verified entries as a normative example. We recommend adding blockchain based addressses or registries or verified entries as a normative example. We recommend adding in blockchain based addressses or registries or verified entries as a normative example. We recommend adding blockchain wallet added as notificatio				1			
72 63C 3.11.2 32 1422 values throughout all parts of SP 800-63 may be moot. 73 63C 3.12.3 32 1433 We believe subscribers should be required to be notified and must give consent to share attributes. 74 63C 3.12.2 35 1513 their time and find trusted data in the digital age. 75 63C 3.12.3 35 1534 their time and find trusted data in the digital age. 76 63C 3.15 38 1607-1608 their time and find trusted data in the digital age. 77 63C 4.3.1 46 1780-1805 (included in this section and in trust agreements. 78 63C 4.3.1 47 1828-1829 (included in this section and in trust agreements. 79 63C 4.3.1 47 1828-1829 (included in this section and in trust agreements. 79 63C 4.3.1 47 1828-1829 (included in this section and in trust agreements. 79 63C 4.3.1 47 1828-1829 (included in this section and in trust agreements. 79 63C 4.3.1 47 1828-1829 (included in this section and in trust agreements. 79 63C 4.3.1 47 1828-1829 (included in this section and in trust agreements. 79 63C 4.3.1 47 1828-1829 (included in this section and in trust agreements. 79 63C 4.3.1 47 1828-1829 (included in this section and in trust agreements. 79 63C 4.3.1 47 1828-1829 (included in this section and in trust agreements. 79 63C 4.3.1 47 1828-1829 (included in this section and in trust agreements. 79 63C 4.3.1 47 1828-1829 (included in this section and in trust agreements. 79 63C 4.3.1 47 1828-1829 (included in this section and in trust agreements. 79 63C 4.3.1 47 1828-1829 (included in this section and in trust agreements. 79 63C 4.3.1 47 1828-1829 (included in this section and in trust agreements. 79 63C 4.3.1 47 1828-1829 (included in this section and in trust agreements. 79 63C 4.3.1 47 1828-1829 (included in this section and in trust agreements. 79 63C 4.3.1 47 1828-1829 (included in this section and in trust agreements. 79 63C 4.3.1 47 1828-1829 (included in this section and in trust agreements. 79 63C 4.3.1 47 1828-1829 (included in this section and in trust agreements. 79 63C 4.3.1 47 1828-1829 (included in this section and							
Add provision stating "Subscriber Shall be notified and required to give consent to share the attributes, and be allowed to select each discrete attribute they consent to share the attributes, and be allowed to select each discrete attribute they consent to share the attributes, and be allowed to select each discrete attribute they consent to sharing." Add provision stating "Subscriber Shall be notified and required to give consent to share the attributes, and be allowed to select each discrete attribute they consent to sharing." Add provision stating "Subscriber Shall be notified and required to give consent to share the attributes, and be allowed to select each discrete attribute they consent to share the attributes, and be allowed to select each discrete attribute they consent to sharing." We recommend adding in blockchain based addressses or registries or verified entries as a normative example. We recommend adding in blockchain based addressses or registries or verified entries as a normative example. We recommend adding in blockchain based addressses or registries or verified entries as a normative example. We recommend adding in blockchain based addressses or registries or verified entries as a normative example. We recommend adding in blockchain based addressses or registries or verified entries as a normative example. We recommend adding blockchain wallet added as notification/verification mechanism for subscribers. We recommend adding blockchain wallet added as notification/verification mechanism for subscribers. We would encourage this section to clarify and state that blockchain-based wallets are included. It is critical for user privacy and data minimization that requirements on derived attribute data are and are quired. It is critical for user privacy and data minimization that using derived attribute data are and required. It is critical for user privacy and data minimization that using derived attribute data as on the required. Add to this list "Agreements on using derived attribut							
73 63C 3.11.3 32 1493 We believe subscribers should be required to be notified and must give consent to share attributes. As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend their time and find trusted data in the digital age. As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward he next communications and data platforms where subscribers will spend their time and find trusted data in the digital age. As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward he next communications and data platforms where subscribers will spend their time and find trusted data in the digital age. As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward he next communications and data platforms where subscribers will spend their time and find trusted data in the digital age. As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward he next communications and data platforms where subscribers will spend their time and find trusted data in the digital age. We recommend adding in blockchain based addressses or registries or verified entries as a normative example. We recommend adding blockchain based addressses or registries or verified entries as a normative example. We recommend adding blockchain wallet added as notification/verification mechanism for subscribers. We recommend adding blockchain wallet added as notification/verification mechanism for subscribers. We would encourage this section to clarify and state that blockchain-based wallets are included. It is critical for user privacy and data minimization that requirements on derived attribute data as the standard when non-derived attribute data is not re	72	63C	3.11.2	32	1422	values throughout all parts of SP 800-63 may be moot.	
As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend We recommend adding in blockchain based addresses or registries or						L	
forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend We recommend adding in blockchain based addressses or registries or verified entries as a normative example. We recommend adding in blockchain based addressses or registries or verified entries as a normative example. We recommend adding in blockchain based addressses or registries or verified entries as a normative example. We recommend adding in blockchain based addressses or registries or v	73	63C	3.11.3	32	1493		select each discrete attribute they consent to sharing."
Me recommend adding in blockchain based addressses or registries or verified entries as a normative example.				1			
As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend their time and find trusted data in the digital age. As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communication be described with sections and intrust agreements. We recommend adding in blockchain based addressses or registries or verified entries as a normative example. We recommend adding in blockchain based addressses or registries or verified entries as a normative example. We recommend adding in blockchain based addressses or registries or verified entries as a normative example. We recommend adding in blockchain based addressses or registries or verified entries as a normative example. We recommend adding in blockchain based addressses or registries or verified entries as a normative example. We recommend adding in blockchain based addressses or r			2				
forward looking toward the next communications and data platforms where subscribers will spend Social So	/4	63C	3.12.2	35	1513		we recommend adding in blockchain based addressses or registries or verified entries as a normative example.
75 63C 3.12.3 35 1534 their time and find trusted data in the digital age. We recommend adding in blockchain based addressses or registries or verified entries as a normative example. As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend their time and find trusted data in the digital age. Ye recommend adding in blockchain based addressses or registries or verified entries as a normative example. We recommend adding blockchain wallet added as notification/verification mechanism for subscribers. We would encourage this section to clarify and state that blockchain-based wallets are to the included. Add to this list "Agreements on using derived attribute data as the standard when non-derived attribute data is not required." It is critical for user privacy and data minimization that requirements on derived attribute data are the control of line 1829 to read "function of the system, and use derived attribute values can be used in place of actual in the critical for user privacy and data minimization that using derived attribute data is standard practice. As digital technologies continue to evolve and data in the digital age. We recommend adding in blockchain based addressses or registries or verified entries as a normative example. We recommend adding in blockchain based addressses or registries or verified entries as a normative example. We recommend adding in blockchain based addressses or registries or verified entries as a normative example.							
As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend their time and find trust agreements. As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend their time and find trust agreements. We recommmend adding blockchain wallet added as notification/verification mechanism for subscribers. We would encourage this section to clarify and state that blockchain-based wallets are included. It is critical for user privacy and data minimization that requirements on derived attribute data are required." It is critical for user privacy and data minimization that requirements on derived attribute data is not required." And do to this list "Agreements on using derived attribute data as the standard when non-derived attribute data as the standard when non-derived attribute data as the standard when non-derived attribute data is not required." And when the end of line 1829 to read "function of the system, and use derived attribute data as the standard when non-derived attribute data is not required." It is critical for user privacy and data minimization that using derived attribute data is standard practice. And the end of line 1829 to read "function of the system, and use derived attribute data as the standard when non-derived attribute data is not required." And when the end of line 1829 to read "function of the system, and use derived attribute data as the standard when non-derived attribute data is not required." And the end of line 1829 to read "function of the system, and use derived attribute data as the standard when non-derived attribute data is not required."	70	630	2177	25	1524		We recommend adding in blockshain based addressess or registries or verified entries as a normative evenuels
forward looking toward the next communications and data platforms where subscribers will spend for ward looking toward the next communications and data platforms where subscribers will spend We recommmend adding blockchain wallet added as notification/verification mechanism for subscribers. We would encourage this section to clarify and state that blockchain-based wallets are included. We would encourage this section to clarify and state that blockchain-based wallets are included. We would encourage this section to clarify and state that blockchain-based wallets are included. Add to this list "Agreements on using derived attribute data as the standard when non-derived attribute data is not required." It is critical for user privacy and data minimization that requirements on derived attribute data are Amend the end of line 1829 to read "function of the system, and use derived attribute data as the standard when non-derived attribute data is not required." It is critical for user privacy and data minimization that using derived attribute data is standard practice Amend the end of line 1829 to read "function of the system, and use derived attribute data as the standard when non-derived attribute data is not required." It is critical for user privacy and data minimization that using derived attribute data is standard practice. Amend the end of line 1829 to read "function of the system, and use derived attribute data as the standard when non-derived attribute data is not required."	/5	030	3.12.3	35	1534		we recommend adding in procedural pased addresses of registries of verified entries as a normative example.
76 63C 3.15 38 1607-1608 their time and find trusted data in the digital age. 78 63C 4 31 709-1710 it is unclear whether this provision includes blockchain-based digital wallets. 78 63C 4.3.1 46 1780-1805 included in this section and in trust agreements. 78 63C 4.3.1 47 1828-1829 included in this section and in trust agreements on derived attribute data are 179 63C 4.3.1 47 1828-1829 included in this section and in trust agreements. 79 63C 4.3.1 47 1828-1829 included in this section and in trust agreements. 80 63C 4.3.1 47 1828-1829 included in this section and in trust agreements on derived attribute data are 180 fine the end of line 1829 to read "function of the system, and use derived attribute data as the standard when non-derived attribute data is not required." 80 63C 4.3.1 47 1828-1829 included in this section and in trust agreements. 81 63C 4.3.1 47 1828-1829 included in this section and in trust agreements. 82 63C 4.3.1 47 1828-1829 included in this section and in trust agreements. 83 63C 4.3.1 47 1828-1829 included in this section and in trust agreements. 84 63C 4.3.1 47 1828-1829 included in this section and in trust agreements. 85 63C 4.3.1 47 1828-1829 included in this section and in trust agreements. 86 63C 4.3.1 47 1828-1829 included in this section and in trust agreements. 87 63C 4.3.1 47 1828-1829 included in this section and in trust agreements. 88 63C 4.3.1 47 1828-1829 included in this section and in trust agreements. 89 63C 4.3.1 47 1828-1829 included in this section and in trust agreements. 99 63C 4.3.1 47 1828-1829 included in this section and in trust agreements. 90 63C 4.3.1 47 1828-1829 included in this section and in trust agreements. 90 63C 4.3.1 47 1828-1829 included in this section and in trust agreements. 90 63C 4.3.1 47 1828-1829 included in this section and in trust agreements. 90 63C 4.3.1 47 1828-1829 included in this section and in trust agreements. 90 63C 4.3.1 47 1828-1829 included in this section and intrust agreements. 90 63C 4.3.1 47 1828-1829 inclu				1			
77 63C 4 43 1709-1710 It is unclear whether this provision includes blockchain-based digital wallets. We would encourage this section to clarify and state that blockchain-based wallets are included. 18 1709-1710 It is unclear whether this provision includes blockchain-based digital wallets. We would encourage this section to clarify and state that blockchain-based wallets are included. 18 1780-1805 Included in this section and in trust agreements. Add to this list "Agreements on using derived attribute data as the standard when non-derived attribute data is not required." 18 1828-1829 included in this section and in trust agreements. Amend the end of line 1829 to read "function of the system, and use derived attribute data as the standard when non-derived attribute data is not required." 18 1828-1829 included in this section and in trust agreements. Amend the end of line 1829 to read "function of the system, and use derived attribute data as the standard when non-derived attribute data is not required." 18 1828-1829 included in this section and in trust agreements. Amend the end of line 1829 to read "available for the means of deletion, whether derived attribute values can be used in place of actual and the place of actual and th	76	630	2 15	28	1607-1608		We recommend adding blockchain wallet added as notification/verification mechanism for subscribers
It is critical for user privacy and data minimization that requirements on derived attribute data are Add to this list "Agreements on using derived attribute data as the standard when non-derived attribute data is not required."		***					
78 63C 4.3.1 46 1780-1805 included in this section and in trust agreements. required." 1 to critical for user privacy and data minimization that using derived attribute data are 79 63C 4.3.1 47 1828-1829 included in this section and in trust agreements. derived attribute data is not required." 8 to critical for user privacy and data minimization that using derived attribute data is standard practice. Amend the end of line 1829 to read "function of the system, and use derived attribute data as the standard when non-directed attribute data is not required." 8 tit is critical for user privacy and data minimization that using derived attribute data is standard practice. Amend line 1862 to read "available for the means of deletion, whether derived attribute values can be used in place of actual			-	3	2,00 1,10		
tt is critical for user privacy and data minimization that requirements on derived attribute data are 4.3.1 47 1828-1829 included in this section and in trust agreements. 4.3.1 47 1828-1829 included in this section and in trust agreements. 4.3.1 47 1828-1829 included in this section and in trust agreements. 4.3.1 47 1828-1829 included in this section and in trust agreements. 4.3.1 47 1828-1829 included in this section and in trust agreements. 4.3.1 47 1828-1829 included in this section and in trust agreements. 4.3.1 47 1828-1829 included in this section and in trust agreements. 4.3.1 47 1828-1829 included in this section and in trust agreements. 4.3.1 47 1828-1829 included in this section and in trust agreements. 4.3.1 47 1828-1829 included in this section and in trust agreements. 4.3.1 47 1828-1829 included in this section and in trust agreements. 4.3.1 47 1828-1829 included in this section and in trust agreements. 4.3.1 47 1828-1829 included in this section and in trust agreements. 4.3.1 4.7 1828-1829 included in this section and in trust agreements. 4.3.1 4.7 1828-1829 included in this section and in trust agreements. 4.3.1 4.7 1828-1829 included in this section and in trust agreements. 4.3.1 4.7 1828-1829 included in this section and in trust agreements. 4.3.1 4.7 1828-1829 included in this section and in trust agreements. 4.3.1 4.7 1828-1829 included in this section and in trust agreements. 4.3.1 4.7 1828-1829 included in this section and in trust agreements. 4.3.1 4.7 1828-1829 included in this section and in trust agreements. 4.3.1 4.7 1828-1829 included in this section and in trust agreements. 4.3.1 4.7 1828-1829 included in this section and in trust agreements. 4.3.1 4.7 1828-1829 included in this section and in trust agreements. 4.3.1 4.7 1828-1829 included in this section and in trust agreements. 4.3.1 4.7 1828-1829 included in this section and in trust agreements. 4.3.1 4.7 1828-1829 included in this section and in trust agreements. 4.3.1 4.7 1828-1829 included in this se	- ''	630				Tit is critical for user privacy and data minimization that reduirements on derived attribute data are	
79 63C 4.3.1 47 1828-1829 included in this section and in trust agreements. derived attribute data is not required." It is critical for user privacy and data minimization that using derived attribute data is standard practice. Amend line 1862 to read "available for the means of deletion, whether derived attribute values can be used in place of actual and the pl			4.3.1	46	1780-1805		
It is critical for user privacy and data minimization that using derived attribute data is standard practice Amend line 1862 to read "available for the means of deletion, whether derived attribute values can be used in place of actual			4.3.1	46	1780-1805	included in this section and in trust agreements.	required."
	78	63C				included in this section and in trust agreements. It is critical for user privacy and data minimization that requirements on derived attribute data are	required." Amend the end of line 1829 to read "function of the system, and use derived attribute data as the standard when non-
	78	63C				included in this section and in trust agreements. It is critical for user privacy and data minimization that requirements on derived attribute data are included in this section and in trust agreements.	required." Amend the end of line 1829 to read "function of the system, and use derived attribute data as the standard when non-derived attribute data is not required."

			T T	1		We applaud NIST for including manual registration, and including normative requirements on trust	
						agreements pertaining to automated registration, including cybersecurity enhancing techniques such	
81	63C	4.4.1	49	1895	5-1899	as key distribution and cache lifetimes.	
						Does this mean that the IdP shall not flag the RP as a blocklisted entity? If so, how does this impact	
						future cases of fraud or improper subscriber attribute sharing with this blocklisted RP? What are the	
82	63C	4.6.1.2	51			risks to subscribers?	Clarity is needed on this provision.
83	63C	4.6.1.3	52	1984	4-1991	Who can take on the role of an administrator?	Clarity needed on who can take the role of "administrator."
						It may be an easier solution to just show the attribute fields requested, instead of the attribute values	
84	63C	4.6.1.3	52	2003		being requested, in order to solve the issue of "shoulder surfing."	Change the provision to show the requested attribute fields instead of showing the actual data being requested.
						We believe the subscriber should be notified of this practice, and be presented with the option to	
				1			Amend lines 2010 and 2011 to read "If such a mechanism is provided, the IdP shall gain consent from the subscriber. The IdP
85	63C	4.6.1.3	52	2008		to store their credit card data for future purchases.	Shall allow the authorized party to revoke such remembered access at a future time."
						As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be	
0.5	525	4622	53			forward looking toward the next communications and data platforms where subscribers will spend	Add blockchain wallet address as an example in addition to email address.
86	63C	4.6.2.3	53	-	2040	their time and find trusted data in the digital age. We believe the subscriber should be notified of this practice, and be presented with the option to	Add blockchain wallet address as an example in addition to email address.
						consent. This is a standard practice in other areas, such as prompting users to give consent for websites	Amend lines 2048 and 2049 to read "If such a mechanism is provided, the RP shall gain consent from the subscriber. The RP
87	63C	4.6.2.3	53	2044	4-2049	to store their credit card data for future purchases.	shall also allow the authorized party to revoke such remembered options at a future time."
0,	030	4.0.2.3	- 55	2044		We are unclear on when or in which scenarios the pre-provisioning process would occur. This process	Shah diso dhow the duthorized party to revoke satemental end of the duthorized party t
						seems to be a potentially large threat vector to both user privacy and cybersecurity, and therefore TDC	
88	63C	4.6.3	54	2077		would appreciate examples on when this process would be relevant.	Add examples of situations where pre-provisioning would occur.
				1		We applaud NIST for categorizing and creating normative guidance around authentication processes	
						where subscriber data is deleted after authentication, and therefore not retained. This is a significant	
			1	1		privacy and cybersecurity enhancement that will allow subscribers to gain greater confidence in IdPs,	
89	63C	4.6.3	54	2083	3-2092	CSPs, RPs, and in digital identity overall.	
						We strongly suggest the specification of what "other attributes" RPs may collect, as we fear the	
						provision as written is extremely broadly. Further, we are concerned by RPs having the ability to	
						overwrite data asserted and verified by the IdP. This gives RPs tremendous ability to damage subscriber	
						data attributes and prevent them from being used at other RPs. We believe this is dangerous and	
90	63C	4.6.4	56			creates empowers RPs to act unethically. We are concerned that NIST would approve of this.	Clarify what "other attributes" entail. Remove ability for RPs to override IdP assertions.
91	63C	4.6.5	57	1	2139	Does the RP direct query ability in line 2139 refer to the ability for RPs to "phone home?"	Clarify whether this provision allows for "phoning home."
0.2	626	4.6.5		21.05	F 2467	Do the "external attribute providers" in this provision have the ability to provide primary identity	Clarify whether external attribute providers have the ability to provide only primary identity data, or subblemental data as
92	63C	4.6.5	57	2165		attribute data, or only supplemental data? We believe the subscriber should be notified of this practice, and be presented with the option to	well, what is within the scope of supplemental data.
						consent. This is a standard practice in other areas, such as prompting users to give consent for websites	
93	63C	4.6.6	58	2175		to store their credit card data for future purchases.	Amend line 2176 to read "those provided by the IdP. The RP shall request and gain subscriber consent to do so."
- 55	030	4.0.0	30	, 21/3		We assert that these attributes should be governed by a separate trust agreement between the RP and	
94	63C	4.6.6	58	2184		the Subscriber, and follow the requirements of other trust agreements in 800-63.	Subscriber, and Shall follow the requirements of other trust agreements in 800-63.
						We believe approval of RP and IdP communication in this section may result in collusion for nefarious	If this provision remains, create privacy-oriented rules that protect the subscriber's attribute bundle usage data and prevent
95	63C	4.7	59	2233	3-2235	purposes, unbeknownst to the subscriber.	tracking. Otherwise, we request the removal of this provision.
96	63C	4.7	61	2262	2-2265	We appreciate this clarification on RP authentication of identity APIs and assertions.	
						We suggest that this SP should in fact cover RP access to non-identity APIs, as in many cases, these APIs	i
						contain or provide user data that, while perhaps not containing information about address, phone	
						number, health records, or other primary attribute data covered by this SP, such data and metadata	
			1	1		could still be considered PII broadly. Moreover, it is unclear why an RP would need to, or be provided	L.,
l				l		the ability to, access these APIs on a subscriber's behalf if the subscriber is no longer associated with	Include normative requirements and restrictions on RP access to non-identity APIs, placing privacy and cybersecurity
97	63C	4.7	61	2271		the RP. This seems like a large threat vector against subscriber privacy and data security.	considerations as top priorities.
00		• •	61.00	2202		We are concerned that the section on shared signaling is an approval by NIST of issuer-verifier	We highly recommend holding another public comment feedback session in order for commenters to speak with the authors
98 99	63C	4.8	61-62 62			collusion. We are unclear why this section is not required.	on this section and address concerns. Change "Should" to "Shall."
99	630	4.8	02	+	2303	As shared signaling seems to be a method of issuer-verifier collusion, it is critical that if this practice is	change should to shall.
100	63C	4.8	62	.1	2313	allowed to stand, that subscriber privacy is made paramount.	Remove this provision. If this is infeasible, change "May" to "Shall."
100	030	4.0	02	1	2313	We applaud NIST for including this comment stating that the guidelines do not restrict the type of	
			1	1		protocol or data payload. We believe this will allow these guidelines to remain applicable while	
101	63C	4.9	62			technologies and use cases evolve.	
	393			1		We believe this is invasive to subscriber privacy and goes against the data minimization suggestions and	Remove this provision. If not removed, add a requirement stating that "RPs must inform and gain consent from the
102	63C	4.9	64	2386	6-2388	requirements written into this publication.	subscriber before gathering and associating additional data through identity APIs."
103	63C	4.10	65			Why is this section not mandatory?	Change "Should" to "Shall."
						We are unclear on this new categorization of presentation methods. Is this "back channel" method a	
104	63C	4.11	65	2406	6-2416	new way to describe what has traditionally been know as "phoning home?"	Clarify if this "back channel" method is the functional equivalent of the practice of "phoning home."
				1	T	As written this section is unclear as to whether the subscriber can supply their own wallet(s) that the	We suggest clarifying that subscribers May use their own digital wallets and are not required to use those provided by the
105	63C	5.2	69	2526	6-2527	data attribute bundle will be issued to.	IdP.
						L	
						Does this established relationship require the wallet to be provisioned by the CSP? If a subscriber elects	
						to use a third party (not CSP provisioned) wallet to contain the CSP-provisioned credential (data	
10-				3		attribute bundle), doesn't the fact that the CSP found the wallet to be an acceptable receptacle for the	Clarification
106	63C	5.3	71	2543		credential (data attribute bundle) mean that the RP can/should trust the third party wallet transitively? We believe that listing derived attribute values that would satisfy RP requirements in many cases. As	Clarification needed.
107			7.	2555		such, we believe that a provision should be added to address this.	Retween lines 2550 and 2560, insert "The set of derived attribute values that see he used to esticit, the PDI
10/1	63C	5.3	71	. 255/	7-2560	, such, we believe that a provision should be added to address this.	Between lines 2559 and 2560, insert "The set of derived attribute values that can be used to satisfy the RP's requirements."

					This section describes the methods acceptable to deprovision attribute bundles, not subscriber-	
108	63C	5.4.1	73	2591-26	1 controlled wallets.	This section needs to be renamed to accurately reflect its content.
					As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be	
					forward looking toward the next communications platforms where subscribers will spend their time in	
109	63C	5.5			6 the digital age.	We suggest adding "public blockchain address" in addition to URL.
110	63C	5.5	73	2614-26	7 We applaud this methodology of ensuring multi-party trust.	
						Change "Should" to "Shall" and add a provision that would require the RP to accept selectively disclosed attributes, and to
					We assert that this should be a base requirement of wallets, and by extension, a base requirement of	prioritize the usage of them over the usage of a full attribute bundle of non-derived attributes, if they meet the RP's
111	63C	5.6	74	26	1 RPs.	requirements.
					We assert that this section should also contain a requirement for wallets, and by extension, RPs, to be	
					able to present, verify, authenticate, and accept derived attribute values, and posit that derived	
					attributes should be used in place of user attributes in order to maximize privacy and lower the	Require for usage of derived attributes as the standard when possible and create requirements for RPs to be able to utilize
112	63C	5.6	74	26	1 probability of data interception, leakage, and RP collusion.	them.
						We suggest that notification of acceptance of derived credentials should be conveyed to the subscriber and the subscriber
113	63C	5.7	74	2642-264	3 In line with the comment on the row above.	should be allowed to choose to assert derived values/credentials in place of full identity attributes/values.
					We believe that requiring attribute bundles to have the capacity to contain derived values in addition to	
114	63C	5.8	76	2691-269	4 user attribute values is key to privacy and protection of personal data.	may then be included in the attribute bundle."
115	63C	5.9			4 It does not seem clear to us why this would be a "should" and not a "shall."	Change "Should" to "Shall."
					We suggest that if the issuer makes this list available, that it should only contain the public keys	
116	63C	5.11	77	2731-27	2 associated with each attribute bundle.	We recommend including digital trust registries or public blockchain addresses as normative examples.
					Does "remove" in this section mean removal of certain attributes, or removal (deletion) of the	
117	63C	5.11	77	2739-27	0 subscriber account overall?	Clarification needed.
					Is this a recommendation that this practice be used, even though it turns IdPs into centralized	
118	63C	6.1	78	2768-27	0 honeypots for attackers?	Clarification needed.
119	63C				4 We greatly appreciate the inclusion of a full section on privacy, and applaud NIST in this regard.	
					We greatly appreciate the inclusion of this section on privacy, data minimization, and user	
120	63C	8.2.1	88	3033-30	8 expectations.	
					This is a potentially rare occurrence, but it is still necessary to cover and provide guidance on in this	
121	63C	8.2.1	89	3062-30	3 document. We applaud NIST for catching this.	
					We applaud NIST for including this section on user control and authority over their data. This is	
					especially key as more US states pass laws that require that users have paths to request and ensure the	
122	63C	8.2.1	89	3065-30	8 deletion of their data held by external parties.	
					We applaud NIST for including this provision in ensuring users have sufficient privacy options, and by	
					extension, recognizing that there are valid circumstances where user anonymity and pseudonymity are	
123	63C	8.2.1	89	3071-30	5 appropriate and valid.	
123	030	U.L.I.I	- 03	3071 30	We applied NIST for including this section on user control and authority over their data. This is	
					especially key as more US states pass laws that require that users have paths to request and ensure the	
124	63C	8.2.2	90	3090-30	1 exportability and correction of their data held by external parties.	-
124	030	0.2.2	30	3030 30	We applaud NIST for including this provision on informed user experience and the role it plays in digital	1
125	63C	8.2.2	٩n	3098-316	0 identity.	·
123	030	0.2.2	30	3030 310	o menter.	We recommend adding to this list the capacity for users to present derived attribute values in place of full data when derived
126	63C	0	ດາ	2172.21	1 We applaud this provision for user consent and allowance of selective disclosure of attributes.	attribute values meet RP requirements.
126	630	9	93	31/3-31	Tive appliant this provision for user consent and allowance of selective disclosure of attributes.	attribute values meet or requirements.