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

Please submit responses to dig-comments@nist.gov by March 24 April 14, 2023

Organization:	*Department of Internal Affairs New Zealand*
Name of Submitter/POC:	*Joanne Knight*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	All				Audience of the standards is unclear. In places it refers to federal agencies implementing digital identity systems, sometimes CSPs and also Relying Parties. As there are different needs and different requirements for each of these parties it should be much more clearly established as what applies to which.	Suggest that the standards should generally apply to Relying Parties and more specifically Federal Agencies if the standards are to remain at such a high and restrictive level. An additional standard should address RPs who wish to use the result of their enrolment process for the purposes of issuing a credential on which other RPs will rely.
2	All				The structure of these standards leaves the party wanting to comply having to go on a treasure hunt to find the normative references.	Clearly separate informative and normative statements. Ideally ensure each requirement has a unique reference.
3	All				Due to a still heavy focus on the digital channel these standards contain a large amount of datable technology references and include material related to the delivery channel that would better addressed in a separate standard.	Distinctly separate out the identification elements from elements related to the security or operation of the delivery of the processes in the digital channel.
4	63A	1	2		The last 2 sentences contradict each other.	The process of identifying someone should be carried out in what ever manner suits the situation (in-person or digitally). Not focussing on all manners will result in the ones not addressed becoming avenues for fraud. It also does not meet the goal of inclusiveness that is desired.
5	63A	2	2		In the second paragraph it refers to establishing the relationship between the subject and the real-life person as if these are not one in the same.	Suggest that this means establishing the relationship between information and the subject in the real world.
6	63A	2.1	3		The expected outcome of identification is to prevent identity theft and the fraud that results. The remainder is what needs to happen in order to achieve this.	Differentiate between why and how.
7	63A	2.2	3		While identity continues to be defined as a set of attributes, then it follows that assurance of a set of attributes does not include any element of trying to establish a link to a person in the real-world. As such the levels of assurance make no sense.	Suggest that assurance of information and establishing the relationship to the subject in the real world be dealt with as two separate topics. The levels of assurance should be written to reflect the increase in both these and their mutual exclusiveness.
8	63A	3	3		Across all these standards there is inconsistent use of the definitions	Review all the standards for the way they use the defined terms and correct any that are incorrect.
9	63A	4	3		Refers to the claimed identity existing in the real world. This is confusing as it is the person who exists in the real world. The identity is a set of attributes (according to the definitions). If this is meant to mean that the information is true, then this becomes a subjective statement as in many cases this is more than may be required.	Be clear around what is 'in the system' and what is 'in the real world'. What is representation vs what is physical.
10	63A	4.1	3&4		Using the term identity to mean personal information (as it is by definition) is problematic as many read this to mean name and dob. Then when this is reinforced by example, as it is in this section, means that most readers will not read this standard in the context it is hopefully evolving to mean.	Don't try to change the perception of what identity is by using a definition. Use words that better describe what you mean. As this standard seems to be focussed on people then personal information is a better term than 'identity'.
11	63A	4.1	4		Why is the future use limited to digital identity? If a federal agency (rather than CSP) is the party enrolling the person, there may be many uses for the result of the process. For example providing them a benefit. This is an example of not identifying the audience for the standards properly.	Do not presume the reason for undertaking of the enrolment.
12	63A	4.1	4		The last sentence does not make sense. The proofing process is applied to any information collected. The degree the process gets applied at depends on the criticality that information serves.	
13	63A	4.1.1	4		The diagram implies that there is one process to be applied to one set of information and another to other information. This not logical and dangerous.	
14	63A	4.1.1	4		The validation process here is over the top. It does not represent the levels previous described.	If this informative section does not accurately represent the range of levels it may be better to remove it.
15	63A	4.1.1	4		The verification process is still only a digital example. If this can be done in-person or over the phone then the description needs to be more representative.	If this informative section does not accurately represent the range of delivery options it may be better to remove it.
16	63A	4.3	4		Why does the evidence have to be unexpired? Expired credentials makes the not valid for the purpose they were issued, it does not make them not valid for evidence for identification. This is unnecessarily exclusive.	Add in mitigations for the acceptance of expired documents.
17	63A	4.3	5		Contains a SHALL requirement that does not recognise the various levels of assurance and is subjective	Re write the requirement to address the different levels of assurance and to be more definitive.
18	63A	4.3.1	5		Earlier in the document name was an option, now it is a requirement.	Either take a position that this standard is setting a national id requirement or that information is only what is required for the task.
19	63A	5.3	12		The requirements for level 1 and the other levels do not reconcile with the descriptions in section 2.2	Major rework is required to ensure that process are not over cooked. Too many issues to list.
20	63B	All			By only focussing on the digital channel it will enable weaknesses in authenticators for other channels and thereby create attack vectors for account takeover.	Expand to look at all channels for access to services..
21	63B	All			While this standard discusses and advocates MFA it does not accurate represent the impacts of each factor on the others used in an event. Nor does it address the threats to authenticators from a human perspective.	Suggest that more thought is put into the relationship between threats and mitigations and the factor combinations. Also how to deal with - Biometric match probability rather than just not use them, collusion, authenticator sharing etc.
22	63B	6.1			Authenticator binding does not discuss the relationship between the binding of the person to the information and the level of authentication assurance	The level of authenticator cannot be changed without considering the level of person information binding that was done. Add this consideration to the section.
					Note: I had insufficent time to fully comment on every aspect that requires feedback, but have chosen some key items. I have provided a link to a resource that may provide some suggestions for resolving some of the comments.	https://www.digital.govt.nz/standards-and-guidance/identification-management/