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

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

Organization:	*Tracepoint, LLC*
Name of Submitter/POC:	*Adam Bryer*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63-Base	2	3	361	Period belongs outside the parenthetical.	Replace "persons.)" with "persons)."
2	63-Base	4.1	13	654	The term "service provider" is mentioned but it's unclear what entity is meant. I see that Fig. 1 indicates "service provider functions", but it might be better to explicitly indicate that RP, Verifier, and CSP are all "service providers".	Add a definition for 'service provider" in A.1 and also state in this paragraph in 4.1 what service provider(s) are meant.
3	63-Base	4.3.1	17	750	On p. 18 line 790, "out-of-band device" may refer to an authenticator that issues a OTP every 60 seconds. On p. 17 line 750, however, the wording indicates that digital authenticators are limited to key pairs or shared secrets. Is OTP an example of a shared secret along with symmetric keys and memorized secrets? OTP seems to be very common, and therefore it might be good to mention OTP explicitly on p. 17 in the context of a "what you have" authenticator. OTP is mentioned in A.2, but should probably be defined in A.1.	Mention OTP explicitly on p. 17 in the context of a "what you have" authenticator. Define "One-time-Password (OTP)" in A.1.
4	63-Base	4.3.1	18	778	Although it may be a shared secret, should the blocklist include "OTP given through text messaging"?	Include "OTP via text messaging" on the blocklist.
5	63-Base	5.1.3	27	1092	For the two groups of impacts, should there be subheadings "Reputation" and "Confidentiality" to indicate the nature of the two groups?	Add a subheading for each of the two groups of low-moderate-high.
6	63-Base	5.2.3.1	33	1270	In this paragraph, a 'duty of care risk analysis (DoCRA)' (see CIS RAM at https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method) would be helpful as well...to determine not only whether more rigorous controls will exacerbate associated impacts to mission delivery, but also whether any of the controls under consideration will introduce _new_ risks to mission delivery.	Discuss the evaluation of new risks that would be encountered with the placement of identified controls and how these risks should figure into the assessment.
6.5	63-Base	5.2.3.1	33	1285		Replace 'should' with 'SHOULD'.
7	63-Base	5.2.3.2	34	1311	See comment 6.	See comment 6.
7.5	63-Base	5.2.3.2	35	1326		Replace 'should' with 'SHOULD'.
7.6	63-Base	5.2.3.2	35	1328		Replace 'should' with 'SHOULD'.
8	63-Base	5.2.3.3	35	1354	See comment 6.	See comment 6.
8.5	63-Base	5.2.3.3	35	1359		Replace 'may' with 'MAY'.
8.6	63-Base	5.2.3.3	36	1369		Replace 'should' with 'SHOULD'.
9	63-Base	5.3.1	37	1414	The essence of DoCRA (see comment 6) is also captured in this section regarding privacy, equity, and usability. But the last point in section 5.3.1, 'threats', is not worded like the other points since it excludes "determine unintended consequences" and "will result in challenges" and instead focuses on "will address". The "will address" aspect is already covered in earlier sections on the selection of xAL's. Hence I suggest that the point about 'threats' in 5.3.1 cover the unintended consequences and new risks introduced by selected controls.	Rework the wording of 'threats' to cover unintended consequences to the mission.
10	63-Base	References	40	1512		Add '.' at end of sentence.
11	63-Base	References	40	1527		Add '.' at end of sentence.
12	63-Base	References	40	1530		Add '.' at end of sentence.
13	63-Base	A.1			The suggested definitions to add should help to clarify some points in an otherwise very well constructed set of definitions.	Define 'controls'. The different types of controls are itemized briefly on p. 37 line 1422 (management, operational, technical). A general definition of the procedures in question and the subtypes would be helpful. Define 'digital identity'. May base the definition on that given on p. 3 line 355. Define 'endpoint'. Define 'entity'. May be possible to base the definition on implicit definitions in the first 6 paragraphs of section 4.1, and on section 5.1.1. Define 'identifier'. It's used in several definitions and as parts of compound terms. Define 'individual' as 'a person'. ('Person' is defined circularly on p. 3 line 361. Might want to find a way to remove the circularity on p. 3 and also copy the definition of 'person' into A.1.) 'Individual' appears in several definitions, for example, 'Identity Resolution'. Define 'insider' (this term is used in the definition of 'attacker'). Define 'MAY', 'SHALL', and 'SHOULD'. Maybe RFC 2119 would be helpful to reference (https://www.rfc-editor.org/rfc/rfc2119.txt), if the use of these terms in 800-63 conforms to that RFC. Define 'One-Time-Password (OTP)'. Define 'party'. It and its plural are used in several senses in the definitions of 'Attacker', 'Identity Provider (IdP)', 'Practice Statement', and 'Session Hijack Attack', and those uses are not likely to be easily replaceable with a single substitution like 'individual' or 'entity'. Define 'registrant' most likely as 'applicant' ('registrant' is used in the definition of 'Attacker-in-the-Middle Attack (AitM)'). Define 'service provider'. Define 'system' and 'user'.
14	63-Base	A.1	45	1672		Replace 'MitM' with 'AitM'.
15	63-Base	A.1	46	1692	It doesn't appear as if 'subscriber' adds any critical distinction to the definition.	Replace "subscriber's" with "claimant's".
16	63-Base	A.1	49	1801	This will match the heading style elsewhere.	In the heading replace "site" with "Site".

17	63-Base	A.1	49	1809	This will match the heading style elsewhere.	In the heading replace "site" with "Site".
18	63-Base	A.1	49	1817	Does 'endpoint' refer to the authenticator? Either way, maybe explicitly state in the definition what endpoint is being referred to. The term 'endpoint' is also used in the definition of 'Session', and therefore 'endpoint' should probably be defined in A.1 for general clarity.	State what endpoint is being referred to. Define 'endpoint' in A.1.
19	63-Base	A.1	51	1874		Add '.' at end of defnition.
20	63-Base	A.1	51	1888	This suggested change will match the style used elsewhere, although in my opinion it is clearer to change the style in the rest of the document to match the instance currently in this definition and leave the '.' outside the quotes.	Change ' "brokers". ' to ' "brokers." '
21	63-Base	A.1	52	1914		Replace "e.g." with "e.g.," (two instances). Replace 'driver' with 'drivers'.
22	63-Base	A.1	53	1939		Replace 'NISTIR 8062' with the link '[NISTIR8062]' as was done in definitions of 'Disassociability' and 'Predictability'.
23	63-Base	A.1	54	1986		Replace 'one' with 'One' to match the style for compound words elsewhere.
24	63-Base	A.1	55	2007		Replace "memorized secret" with "Memorized Secret" to match the 'see' style elsewhere.
25	63-Base	A.1	60	2152		Remove the redundant heading.
26	63-Base	A.1	60	2162	For clarity, you might want to reiterate that in 800-63, the subjects in question are persons, based on the second paragraph in section 4.1.	Mention that in this SP, the subjects in question are persons.
27	63-Base	A.1	60	2176		Replace 'identity' with 'Identity' and 'fraud' with 'Fraud'.
28	63-Base	A.1	61	2195		Replace "e.g." with "e.g.,".
29	63-Base	A.2	62	2238		Replace 'site' with 'Site' (to match style in similar hyphenated terms elsewhere in A.2).
30	63-Base	A.2	62	2240		See comment 29.
31	63-Base	A.2	63	2260		Replace 'One-to-one' with 'One-to-One' (to match style in similar hyphenated terms elsewhere in A.2).
32	63-Base	A.2	66	2340		Replace 'over' with 'Over' (to match style in similar hyphenated terms elsewhere in A.2).