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:	*Myself :-)*
Name of Submitter/POC:	*Steven Hespelt*
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63B	3.1.1.2	13	732	I agree 99% - these are weak methods if the answers are publicly discoverable (eg. first grade teacher, city I was born in, etc.). 1% disagreement is because I heard a great suggestion years ago that I've adopted - the use use of junk/nonsense answers - as these answers only need to match, I keep the nonsense answers in an encrypted password manager vault, so that I have them for recovery purposes. In someways this notion of nonsense answers is quite similar to long multi-word passphrases: non-dictionary, uncommon strings, not easily guessed. So the advice I've given people is to only use nonsense answers as we as users are often not given the option of bypassing the use of these KB auth questions. But we can control how secure the responses are... If we are careful.	
2	63B	3.1.1.2	13	727	If I recall correctly, Boeing had published a paper on the dangers of forcing periodic password changes (I've worked in places that did so every 30 days. crazy) in the late 1980s in a IEEE publication I used to get. Pretty quickly, people will write the latest password down, shades of Ferris Beuller hacking his school's grades by using a written down password on the secretary's desk... Not ideal. Why forece a reset if there is no indication the current password is either weak or has been compromised?	