[redacted]

**From:** 'MitchellAnderson' via DIG-Comments <DIG-Comments@list.nist.gov>
**Sent:** Saturday, September 28, 2024 12:31 PM
**To:** dig-comments@nist.gov
**Subject:** [dig-comments] Comments regarding NIST SP 800-63B

Hi,

From news I've learned that the NIST SP 800-63B, which is colloquially known to help dictate practices regarding identity and password management, is being updated.

I want to say that the complete depreciation of security questions may prove counterproductive in some certain situations, such as when users lose/damage their multi-factor devices or are otherwise living in authoritarian countries like China and so on where devices that are linked multi-factor to any accounts where dissident contents are posted, could invite great dangers.

Instead, I want to suggest the following for Section 8 of 3.1.1.2. (Password Verifiers):

> Verifiers and CSPs **SHALL** discourage the use of knowledge-based authentication (KBA) prompts (e.g., “What was the name of your first pet?”) or security questions for password creation. In situations warranting the use of KBA prompts or security questions, verifiers and CSPs **SHALL** provide the ability for users to self-customize the KBA prompts or security questions, along with their answers. Answers to the security questions **SHALL** be stored as cryptographic hashes.

Thank you and have a nice day.

Regards,
Mitchell

Sent with Proton Mail secure email.
--