[redacted]

From: dig-comments@list.nist.gov on behalf of Matt Hickford [redacted]
Sent: Friday, September 27, 2024 2:54 AM
To: dig-comments@nist.gov
Subject: [dig-comments] Clarify recommendations about password expiration

Hi. Please could you edit draft https://pages.nist.gov/800-63-4/sp800-63b.html#passwordver to make it clearer that password expiration is recommend against. The current language isn't clear enough.

> Verifiers and CSPs SHALL NOT require users to change passwords periodically.

Better would be to write in plain English.

> Verifiers and CSPs SHALL NOT require users to change passwords periodically. Passwords SHALL NOT expire.

This is important because many security professionals I've worked with still think NIST recommends password expiration as in the 2000s.

For comparison, UK National Cyber Security Centre has password policy advice in plain English "Don't enforce regular password expiry ... Regular password changing harms rather than improves security" https://www.ncsc.gov.uk/collection/passwords/updating-your-approach#tip4-password-collection . This is great because it explains why.

Kind regards
-Matt