## 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:*** | *Diceware.com* |
| ***Name of Submitter/POC:*** | *Arnold Reinhold* |
| ***Email Address of Submitter/POC:*** | [REMOVED] |

| Comment # | Publication<br>(Base, 63A, 63B, 63C) | Section | Page # | Line # | Comment<br>(Include rationale for comment) | Suggested Change |
|---|---|---|---|---|---|---|
| | | | | | | |
| 1 | 63B | 5.1.1.2 and 5.2.3 | 14 | | These sections are overloaded with important, distinct provisions. See letter submitted separately. | Add another level of outlining. See letter submitted separately. |
| 2 | 63B | 5.2.2 | 31 | | Rate limiting measures can discourage use of complex passwords for fear of being locked out | Add provisions that make entering passwords less scary without reducing security. See next items |
| 3 | 63B | 5.2.2 | 31 | | Hitting return before entering a password is a common user error. There is no benefit to an attacker who does so. | In counting failed attempts verifiers MAY  ignore attempts with a blank password field. |
| 4 | 63B | 5.2.2 | 31 | | Users often enter a password that is the same as the previous attempt's password, typically because they have the wrong | In counting failed attempts verifiers MAY ignore attempts where the password entered is the same as the previous attem |
| 5 | 63B | 5.2.2 | 31 | | Having Caps Lock on is another common user error. An attacker knows the passwords they are trying. | Password verifiers MAY report to users that their Caps Lock key is on |
| 6 | 63B | 5.2.2 | 31 | | Long passwords should be encouraged, but they increase the risk of typing mistakes. Users of long passwords should be gi | Password verifiers MAY allow additional failed attempts when long passwords are entered. [e.g. Allow one additional fail |
| 7 | 63B | 5.2.2 | 31 | | Password throttling can be used to deny service, say by a competitor bricking a presenter's unguarded laptop at a conferen | Password verifiers MAY allow one failed-attempt-count reset using a second authentication method. |
| 8 | 63B | 5.1.1.2 | 16 | 751 | Users should have a way to know the key derivation function and iteration count used to protect their passwords so they c | Password verifiers SHOULD disclose to users the key derivation function and iteration count currently used to protect store |
| 9 | 63B | 5.1.1.2 | 16 | 751 | The pattern "stored_hash = SHAx(password, salt)" is too easily reversed in practice. | The new guidelines should explicitly state that protecting stored passwords using a single pass of a standard fast hash fun |
| 10 | 63B | 5.1.1.2 | 16 | 751 | Password storage security needs to be upgraded from time to time as  computing power available for password cracking i | Verifier user records SHOULD include a version number to allow easy upgrades to stronger hash algorithms. |