From: Mike McCormick
Sent: Monday, June 22, 2020 4:55 PM
To: dig-comments-RFC <dig-comments-rfc@nist.gov> **Subject:**
Comments on Digital Identity Guidelines RFC

NIST editors,

The following comments apply to the latest draft of SP800-63B:

4.2.2 While it makes sense to disqualify smartphone unlock as a factor, please clarify whether proving possession of the smartphone that was bound to the user during enrollment allows the device to qualify as a SYH factor.

4.3.2 Same smartphone comment as 4.2.2.

5.1.3.2 We are pleased that the threat to deprecate OOB using SMS has been removed. However some warning that SMS is an insecure channel would still be appropriate.

5.2.2 A ceiling of 100 consecutive failed attempts is too high, well in excess of industry best practice and most organizations' policies.

5.2.3 Fixing the FMR limit globally at 1:1000 does not allow for consideration of risk. Set a different limit for each AAL instead.

5.2.3 We agree liveness testing (PAD) should be mandatory at all AAL levels.

7.1.1 In the spirit of CCPA and GDPR, session cookies should not contain cleartext PII. Their contents should generally be limited to an opaque session ID or token.

7.2 Session secrets should also not persist after a user logoff.

10.1 Under User experience (first bullet) offer the option to unmask display text *after* entry as well as during entry. This may be accompanied by a warning that unmasking facilitates shoulder surfing.

Thanks for the opportunity to comment on SP800-63.

Taproot Security is a cybersecurity consulting firm providing guidance to leaders of business and government agencies.

Michael McCormick.