New Protocols must use TLS 1.3

Rich Salz
Content

- Boilerplate
- Security comparison of TLS 1.2 and 1.3
- "New protocols must use TLS 1.3"

; wc -l draft-rsalz-uta-require-tls13.md
274 draft-rsalz-uta-require-tls13.md
Post-quantum

- The IETF is moving to make sure everything is capable of doing post-quantum
- This helps ensure that
Next steps

● Adoption?

● Fix the nits
  ○ Mainly updates 9325/BCP 195, requires some wording changes

● Short review

● WGLC