draft-ietf-tls-oldversion-deprecate-00
https://github.com/tlswg/oldversions-deprecate

Kathleen Moriarty
kathleen.moriarty.ietf@gmail.com
Stephen Farrell
stephen.farrell@cs.tcd.ie

IETF-103

Issues

- What list of RFCs does this update/obsolete?
  - Could be a long or short list, not sure
  - Section 9 updates RFC7525 (a BCP) - might mean this becomes part of BCP195?
  - Suggestion: authors do bureaucracy with chairs/ADs/IESG (inevitable anyway:-)
- Sections 3 & 4 – some info on deprecation annoucements and measurements
  - Leave in RFC or not? More welcome in any case
  - Suggest: leave in - (correct:-) factual statements seem useful even for posterity
- Section 8 – (PR from Hubert Kario) Don’t use SHA-1 as a signature hash
  - Keep or separate out? Could be better handled elsewhere maybe? (Or ignored for now?)
  - Suggestion: Leave it in unless some better document turns up for that text

Timeline

- Bigger issue is when to progress this
  - Are email, etc., are sufficiently different from web?
- Happy to leave that to chairs but no harm to get a sense of what folks think at the moment
  - Authors are happy to try finish the text quickly if that’s what the WG want