A draft about using OOB outside the original threat model

- Assumes the CPS is not an untrusted third-party service
  - Instead something operated by (or for) the originating or terminating domain, or some sort of authorized gateway
  - i.e., what if the entity operating the CPS would already see the non-SIP call signaling?
    - And hence learn the called/calling party numbers

- Descriptive of emerging efforts in the deployment of STIR
  - Not a science project, aiming for PS
Updates and Next Steps

• Some changes in response to Simon Castle’s comments
  – Clarifying that advertising an SPC isn’t super helpful when there’s no TN->SPC mapping available to the system
  – Added a disambiguation for SPCs vs TNs in advertisements
    • Basically borrowing the TNEntry values from RFC8226 as a prefix
  – Some future proofing for potential advertisement of URIs
    • In case want to do non-TN based STIR (which RFC8224 allow)

• We had a WGLC (no other comments)

• Time to ship?
  – (Does entail a downref for IETF LC)