RFC 8447bis and IANA TLS
Recommended Column

Joe Salowey, Sean Turner
Addition of a recommended column for most TLS registries

- ‘Y’ - Generally recommended for an implementation to support
- ‘N’ - Not generally recommended for an implementation to support
Feedback Received

Two values are not enough as “N” could result from various

- Not evaluated
- Not Recommended in any Circumstance
- Recommended only in specific cases
RFC 8447bis

RFC 8447bis - https://tools.ietf.org/id/draft-salowey-tls-rfc8447bis-00.txt

Proposal -

‘Y’ = Parameters that are Recommended for general use

‘N’ = Parameters that are Discouraged for general use

   Also include a reference to the document and section which describes
   the limitation of the parameter.

‘ ’ = Parameters that are Unevaluated (Not Recommended)

Also added a note that designated expert granting a code point does not necessarily mean
endorsement of the value
Request for Feedback

Is this approach is of general interest to the IETF Security Area?
Comments on 8447bis proposal?
Other RFC 8447bis Changes

Reserve Experimental Codepoint Range

- Temporary allocation for larger scale experiments (1 year)
- Allocation requested through github
- Policy is “specification required”

Discussion on the list suggest we treat the entire unassigned space as an experimental range that can have temporary allocations

- Should IANA just manage these allocations?
- Allocation should not be sequential

Should the registry add an expiry date (perhaps reuse the recommended column)?
Next Steps

Adoption call for RFC 8447-bis