**From:** Chen, Lily
**To:** Scholl, Matthew A. (Fed); Dodson, Donna F; Dworkin, Morris J. (Fed); Regenscheid, Andrew R. (Fed)
**Cc:** Moody, Dustin (Fed); Liu, Yi-Kai (Fed)
**Subject:** shall it be an FRN - call for PQC proposals?
**Date:** Tuesday, February 16, 2016 4:41:05 PM

We plan to distribute a formal “call for PQC proposals” by the end of 2016. The question is whether this formal “call for proposals” must be an FRN.

The reasons to make it an FRN

- AES and SHA-3 were both announced through an FRN.
- It is commonly acceptable format for us, more impact to other government agencies.
- We will have legal to review it, less pressure on our own.

The reasons not to make it an FRN

- PQC standardization is not a competition.
- Modes of operations in 800-38 series are selected without an FRN.
- It will take painfully long time to get an FRN approved.
- We may change the requirements and the rules in the middle of the procedure. It will provide us a lot flexibilities if we can announce it without an FRN.

Any opinions, suggestions, comments?

Lily