

**From:** [Chen, Lily](#)  
**To:** [Moody, Dustin](#); [Perlner, Ray](#)  
**Cc:** [Liu, Yi-Kai](#)  
**Subject:** RE: PQC timeline  
**Date:** Wednesday, January 13, 2016 9:01:31 AM

---

Hi, Dustin:

The timeline is fine. Here are some points we may add or some changes we may think.

Feb '16 – informal announcement at PQCrypto

- o Late '16 – more formal Call For Proposals [do we want to call for public comments on the criteria? Do we need to include that details?]
- o Late '17 – Deadline for submissions
- o 3-5 years later? We will report on our **summary on the** analysis received on the submitted candidates ~~of submissions?~~
- o 2 years later? We will ~~have~~ [release?] (draft) standards **for public comments** ready?
- o We can accept submissions on ongoing basis anytime after our deadline, but we won't promise when we'll get to them? [what do we mean by "but we won't promise when we'll get to them"? I think what we mean is to post for public analysis. The period of public analysis depends on the responses and the acceptance of the draft standards.]
- We should schedule some workshops throughout the process

Lily

---

**From:** Moody, Dustin  
**Sent:** Tuesday, January 12, 2016 2:34 PM  
**To:** Perlner, Ray  
**Cc:** Liu, Yi-Kai; Chen, Lily  
**Subject:** PQC timeline

Ray,

I think it would be good to mention some of our timeline in Section 4 as well. Here's our estimated timeline so far:

Feb '16 – informal announcement at PQCrypto

- o Late '16 – more formal Call For Proposals
- o Late '17 – Deadline for submissions
- o 3-5 years later? We will report on our analysis of submissions?
- o 2 years later? We will have (draft) standards ready?
- o We can accept submissions on ongoing basis anytime after our deadline, but we won't promise when we'll get to them?
- We should schedule some workshops throughout the process

Dustin