

From: [Moody, Dustin \(Fed\)](#)
To: [Kerman, Sara J. \(Fed\)](#)
Subject: Re: PQC main document draft
Date: Tuesday, July 5, 2016 12:39:25 PM

Correct.

(omitting comment about how much I like lawyers)

From: Kerman, Sara J. (Fed)
Sent: Tuesday, July 5, 2016 12:38:37 PM
To: Moody, Dustin (Fed)
Subject: RE: PQC main document draft

OK, so the FRN has not been completely finalized right? I don't want to start taking information from that document if the wording may get changed (I know the lawyers are fine-tooth combing so I want the wording on the web page to be exactly what they want).

Sara

From: Moody, Dustin (Fed)
Sent: Tuesday, July 05, 2016 12:35 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: Re: PQC main document draft

Sara,

I don't see a problem with putting them in pdf format. I'll check with Larry to see if he has any complaints. As for the title, yeah. I think we probably just have to go with something generic like "post-quantum cryptography standardization". That probably doesn't help much! We've tried to come up with a good name, but haven't found one yet.

As for the timing, I'm hoping it's soon, but I just had an email from Lily suggesting it might not be until next week.

Dustin

From: Kerman, Sara J. (Fed)
Sent: Tuesday, July 5, 2016 12:10:26 PM
To: Moody, Dustin (Fed)
Subject: RE: PQC main document draft

Dustin,

I have some time so I'm starting to tackle the PQC web page stuff. Couple questions:

- The .rtf files ((API, IntermediateValues_2048, KAT) – should they be left in their native format? Or PDF'd
- Is there an actual "title" for this work that I should make a menu item under "Post-Quantum Cryptography Project"? I know it's not a competition ☺; but it probably has something more descriptive. I didn't see anything in the draft FRN and the Call for Submissions didn't have any kind of title either.

Thanks,

Sara

From: Moody, Dustin (Fed)
Sent: Wednesday, June 29, 2016 12:23 PM

To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>

Subject: PQC main document draft

Sara,

I'm attaching the current version of the main document. It is not yet ready for being posted, as there are still several lawyer comments. But I thought it might be helpful for you to see it.

Thanks!

Dustin