

**From:** [Moody, Dustin \(Fed\)](#)  
**To:** [Alperin-Sheriff, Jacob \(Fed\)](#)  
**Subject:** RE: PQC comments  
**Date:** Thursday, September 15, 2016 9:31:00 AM

---

Jacob,

That would be great. I think I'll have one file with just all the comments as originally written, but the organized version you created is very useful for how to combine the comments. I appreciate it! Glad you thought of it.

Dustin

---

**From:** Alperin-Sheriff, Jacob (Fed)  
**Sent:** Thursday, September 15, 2016 9:30 AM  
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>  
**Subject:** Re: PQC comments

Let me send you my "organized" version first so you can send that out too (instead?)

---

**From:** "Moody, Dustin (Fed)" <[dustin.moody@nist.gov](mailto:dustin.moody@nist.gov)>  
**Date:** Thursday, September 15, 2016 at 9:23 AM  
**To:** "Daniel C Smith ([daniel-c.smith@louisville.edu](mailto:daniel-c.smith@louisville.edu)) ([daniel-c.smith@louisville.edu](mailto:daniel-c.smith@louisville.edu))" <[daniel-c.smith@louisville.edu](mailto:daniel-c.smith@louisville.edu)>, "Perlner, Ray (Fed)" <[ray.perlner@nist.gov](mailto:ray.perlner@nist.gov)>, "Peralta, Rene (Fed)" <[rene.peralta@nist.gov](mailto:rene.peralta@nist.gov)>, "Liu, Yi-Kai (Fed)" <[yi-kai.liu@nist.gov](mailto:yi-kai.liu@nist.gov)>, "Jordan, Stephen P (Fed)" <[stephen.jordan@nist.gov](mailto:stephen.jordan@nist.gov)>, "Miller, Carl A. (Fed)" <[carl.miller@nist.gov](mailto:carl.miller@nist.gov)>, "Alperin-Sheriff, Jacob M. (Fed)" <[jacob.alperin-sheriff@nist.gov](mailto:jacob.alperin-sheriff@nist.gov)>, "Chen, Lily (Fed)" <[lily.chen@nist.gov](mailto:lily.chen@nist.gov)>, "Bassham, Lawrence E (Fed)" <[lawrence.bassham@nist.gov](mailto:lawrence.bassham@nist.gov)>  
**Subject:** PQC comments

Everyone,

Just a reminder the comment period for our draft PQC requirements ends tomorrow. If you know anyone who you think needs a reminder, then let them know. On Monday, I'll send out all the comments in one file, just to make sure we all have them. We can then begin discussing them by email, and we will have an internal meeting to discuss them on Tuesday, October 4.

Please don't worry about responding back to the authors of the comments we receive. We don't usually write individual responses when we make a public call for comments. We will discuss the comments together, and if we feel we want to reply back to anyone, we can then do so at that point.

Thanks!

We'll need to be pretty busy working on this. We want to have our Final version ready to be sent out publicly at the end of November or early December. Good news is that we don't have to go through the FRN again (although we'll still need to run what we have by the lawyers, who will probably not be very fast).

Dustin