From:	Moody, Dustin (Fed)
To:	Alperin-Sheriff, Jacob (Fed)
Cc:	Liu, Yi-Kai (Fed)
Bcc:	Moody, Dustin (Fed)
Subject:	RE: internal PQC meeting
Date:	Wednesday, October 5, 2016 9:41:00 AM
Attachments:	final CFP.docx

Jacob,

Here's some notes on our meeting yesterday. We mostly kept to more of the "minor" issues, which I was hoping to get through before tackling things like quantum security and clarifying key exchange/key establishment.

- We agreed to use the term post-quantum in the document for consistency, rather than quantum-resistant.
- Several minor (grammatical) edits in the document, which can be seen in the attached version
- Ignore Brown/Yamada comment for more than one deadline
- Agreed to not require submissions be mailed in (except the IPR statements)
- Agreed we didn't need to make any changes as a result of Gligoroski's comment or Seidl's comment.
- Agreed to Jao's idea to clarify types of submissions. Submitters need not submit all the functionalities we are wanting- they can submit just one if desired. Submissions will be compared against submissions of the same type. We know one such functionality is signatures. We need to have more discussion to clarify encryption/key exchange/key establishment.
- For several of the implementation questions (such as more implementations on smaller processors, assembly language optimizations), Larry will write something up for the FAQ to address them.
- We want to encourage submitters to create benchmarks, and our API is consistent with Dan and Tanja's eBACS site. However, we are not endorsing nor requiring submitters to use their site.
- Regarding constant-time, we will not require it. We are adding a line in to strongly encourage it.
- Tanja's comment on 2.B.6, we aren't sure why she thinks you couldn't just send links to papers. To help with her copyright concerns, we tweaked our statement.
- Skipped the IPR/legal stuff. Lily and I have a meeting with the NIST lawyers to address it.
- Ding's comment on parameters. Ray will clarify the language. Submitters don't have to give parameters for all 5 levels. Especially as parameters for one level are automatically parameters for all lower levels.
- Stehle's comment. Ray will use the answer he replied back to Stehle to create a bullet for our FAQ
- Hars comment on side-channels. We didn't feel we needed to add anything additional on side-channel analysis.
- Meier/Rechberger/Lauridsen. We didn't understand their comment. I will check back with them to see if they can explain more.
- Perfect forward secrecy. We will add a short description of what is meant by this term.
- Multi-key attacks. Ray will clarify the paragraph that discusses this.
- Jao comment on 4.B. We will add a paragraph/bullet to discuss more about key exchange/establishment. Probably need a bit more discussion before doing this.

Let me know if you have any questions.
Dustin

From: Alperin-Sheriff, Jacob (Fed)
Sent: Wednesday, October 05, 2016 8:49 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: internal PQC meeting

Sorry I had to miss yesterday. Can I get a brief fill-in on any important decisions etc. that were made?

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Tuesday, October 4, 2016 at 2:56 PM
To: "Chen, Lily (Fed)" <lily.chen@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, "Peralta, Rene (Fed)" <rene.peralta@nist.gov>, "Alperin-Sheriff, Jacob M. (Fed)" <jacob.alperin-sheriff@nist.gov>, "Jordan, Stephen P (Fed)" <stephen.jordan@nist.gov>, "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>, "Miller, Carl A. (Fed)" <carl.miller@nist.gov>, "Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)" <daniel-c.smith@louisville.edu>, "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>
Subject: internal PQC meeting

We will continue to address the comments on our draft.