From: Moody, Dustin (Fed)
To: Perlner, Ray A. (Fed)
Subject: RE: Status update on PQC CFP
Date: Tuesday, October 18, 2016 9:59:23 AM

Ray,
Do we want to add another item near 4.B.3, as suggested by one of the comments?
Also, can you reword the sentence on the top of p. 19?
Dustin

From: Perlner, Ray (Fed)
Sent: Monday, October 17, 2016 4:27 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Ray Perlner (b) (6) ; Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Daniel Smith-Tone <daniel-c.smith@louisville.edu>; 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>; Peralta, Rene (Fed) <rene.peralta@nist.gov>; Smith-Tone, Daniel (Fed) <daniel.smith@nist.gov>
Subject: RE: Status update on PQC CFP
I have added text for the following purposes

- To provide separate security model sections for IND-CCA2 and IND-CPA
- To uniformly use the standard terminology for KEMs in place of previous text about "key exchange"
- To address Yi-Kai and Jacob's requests that we explicitly say we aren't requiring submitters to provide distinct parameters in each of the five security categories, and that we provide a translation table between our security categories and gate counts.

From: Moody, Dustin (Fed)
Sent: Wednesday, October 12, 2016 1:27 PM
To: Ray Perlner (b) (6) ; Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Daniel Smith-Tone <daniel-c.smith@louisville.edu>; 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>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Smith-Tone, Daniel (Fed) <daniel.smith@nist.gov>
Subject: Status update on PQC CFP
Everyone,
Thanks for everybody's time and effort to finalize our CFP. Here's a few notes and assignments following our second internal meeting yesterday.

- I think we resolved most of the minor comments, which have been reflected in the attached updated CFP. Please review it. The changes are marked and easy to see. Let me within a week if anybody sees something that needs to be addressed/fixed.
- Larry and Ray have written some new FAQ questions. See the attached. I will have Sara post them to the FAQ section next week, unless I hear anything back from anyone. Daniel is going to write one on how our process is different than a competition.
- Larry is working on resolving the API comments. For some of that, he will work with Ray. Also

need to make sure how we change our key-exchange/KEM stuff is reflected in the API.

- Yi-Kai will work with Ray to revise the security section (4.A.4). Yesterday, we agreed with Yi-Kai that it might be best to remove security levels 2 and 4. Possibly discuss this on the pqc-forum.
- Jacob will work with Ray to re-write the portions of the CFP dealing with key-exchange. We agreed to add an ephemeral version. Jacob has suggested some text for 4.A.2, which could be split into 2 sections. They also need to look at 2.B.1 and section 3. We need to agree on our terminology. Would probably also be good to discuss on the pqc-forum.
- We had a meeting with the NIST lawyers. They said we need to keep our IPR statements as they currently are (meaning we can't have only royalty free algorithms). There will probably be a few lines added into the CFP strengthening our language that we have a strong preference for royalty-free, and that it will be used as an evaluation criteria. Andy would also like to add a line that we will commit to having at least one algorithm of each type be royalty-free.
- We will need to have a 2nd FRN announcing our final version of the CFP, but it will be very short, just pointing to our webpage. We will also want to have a short report which summarizes the comments received (text of the comments will also be published), and the main changes we made as a result.
- We will have a meeting next Wednesday (10/19), 10am til noon. The main topics of discussion will be the above items.

Thanks!
Dustin