From: Moody, Dustin (Fed)
To: Kerman, Sara J. (Fed)
Subject: RE: A new PQC FAQ
Date: Friday, October 20, 2017 12:30:00 PM

Ok, thanks. No rush on it.

From: Kerman, Sara J. (Fed)
Sent: Friday, October 20, 2017 12:30 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: A new PQC FAQ

Yes, that sounds like a good plan. I'll let you know if I have any questions once I'm in the weeds. ☺

From: Moody, Dustin (Fed)
Sent: Friday, October 20, 2017 12:28 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: A new PQC FAQ

Sara,

We completed the check for "complete and proper" submissions for all the submitters who submitted early. Based on what we learned, we created some advice to submitters for the final deadline. We posted it on the pqc-forum, but it would probably be nice to have on our webpage as well. Looking, it seemed to make the most sense to put it as a new FAQ. So I put it below.

Maybe on the project home page, somewhere in the Project Overview text we could put a plug for it. Something like a linked "Advice for Submitters". Although I think the link would only go to the FAQ and not the specific question. So maybe we could add "see Question 19" or something to that effect. Does that seem reasonable?

Dustin

Q. What advice does NIST have for submitters to ensure their submissions will be complete and proper?

A. NIST has completed the reviews for all the submissions received by the preliminary deadline, and has sent back comments to each submission team. We note the reviews were to check if submissions were "complete and proper", meeting both our submission requirements and minimal acceptance criteria. They were NOT a review on the technical merits. Submissions which had elements missing will need to revise their submissions, and re-submit by the final deadline of November 30, 2017.

After going through this process, we have some suggestions we think will help submitters to make their submissions complete and proper, as well as help NIST with a more efficient review process following the final deadline.

- Clearly provide ALL of the information on the cover sheet which is asked for in our Call for Proposals (CFP) section 2.A.
- Please clearly and explicitly state which of our five security strength categories your proposed parameter sets meet. See CFP 2.B.4 and 4.A.5.
- Some submissions can be submitted as either a KEM or a public-key encryption scheme, or both. Please clearly indicate which functionality (or functionalities) you want NIST to consider, and include the appropriate required algorithms. See CFP 2.B.1.
- We are interested in qualitative statements about the possible tradeoffs between security and efficiency. That is, besides stating which of the five security strength categories are met, we would like submitters to describe what kind of flexibility there is when adjusting the parameters in their cryptosystem. See CFP 2.B.1.

With regards to the implementations and KATs:

- Please make sure your implementation is platform-independent. See NIST FAQ #3, at https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/faqs
- Please follow our guidance on following the NIST API and generating KATs as posted on our webpage: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization/Example-Files
- In addition to the requirement that the README file "shall be a plain text file and list all files that are included on the disc with a brief description of each", it would be useful if the file also contains some basic information about what is being provided. This includes things like how to compile the code, what is produced by the Makefile, and any information necessary to run the files created by the Makefile. On the subject of Makefiles, it would be very useful to have the genKAT and rng files included in the submissions as a concrete example of how to compile the algorithm source code. This will also help facilitate checking of the packages for completeness.

Thank you, and let us know if you have any questions. Specific questions on a submission should be sent to us at pqc-comments@nist.gov. General questions may be posted on the forum, or sent to us the email address just given.