From: Moody, Dustin (Fed)
To: Miller, Carl A. (Fed)
Subject: Re: PQC meeting recap
Date: Friday, June 19, 2020 2:09:59 PM

Thanks, Carl. I appreciate it.

Dustin

From: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Sent: Friday, June 19, 2020 1:43 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: PQC meeting recap

Hi Dustin –

I finished going through our descriptions of each of the 26 submissions. Overall, it looks like we've followed the desired format (summary, round 2 happenings, etc.) pretty well. I pointed out a couple places where I thought one component of a description was missing or unusually short.

I also made some minor comments about how we can make the descriptions more consistent. (One thing I suggested is that we always say explicitly that either "X was selected as a [finalist/alternate]" or "X was not selected" – a few of the descriptions only imply the status and don't say it outright.)

Let me know if I should help with anything else.

-Carl

From: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>
Date: Wednesday, June 17, 2020 at 4:07 PM
To: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Subject: Re: PQC meeting recap

Hi Dustin –

That sounds good to me – I can finish what you assigned to me by Friday.

-Carl

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Wednesday, June 17, 2020 at 11:52 AM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Re: PQC meeting recap

Everyone,

I'd like to suggest we set a deadline of Friday, June 26th to finish our report. Without a deadline, we can endlessly revise and revise. If we get to that day, and we don't think we're ready, we can of course take more time. But I feel if we keep focused we can have it done then (or even before) - thanks to the efforts of everybody.

I'm working on speeding up the publication process (WERB, etc...) where possible, but it still may take up to two or three weeks after we're done until we actually have it published. That would mean we'd likely announce everything (together with the report being published) within the first two weeks of July. I hope that sounds good.

To facilitate this - please complete your current assignments promptly - and not later than this Friday. If I didn't give you a concrete assignment, please try and help somebody complete theirs.

Thank you everybody!

Dustin

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Tuesday, June 16, 2020 2:07 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: PQC meeting recap

Everybody,

We're making good progress on the 2nd round report. Here are a few assignments.

- David
    - revise Section 2.3 Selection of the Third Round Candidates. In addition, Morrie suggested it would be helpful to add a paragraph about our decision making process.
- Carl
    - go through all the write-ups and check they have the same rough format: overall summary (including security and performance), round 2 happenings, possible concerns, and explanation of our decision and possibly their path to standardization. Flag what doesn't follow that via comments.
- Quynh

    - find places where we intend to have a citation, but don't have anything listed yet. Get the references listed in Appendix A in a uniform format. Don't worry about the order yet. We'll fix that once we know we have all the references. Thinh said he would also help out with this.

- Daniel ST
    - check for 2nd round happenings for NTRU, NTRUprime, 3 Bears, Classic McEliece, BIKE, Picnic, Sphincs+. Look in their updated specification/changelog at the beginning of round 2 to see what they changed from round 1. Check official comments. Search the pqc-forum for their scheme name and see if there are any relevant posts. Add these in, either directly or just put a comment at the appropriate place with a list of the 2nd round happenings.

- Angela
    - add in some text to describe the path to standardization for schemes. John has already put an informal path at the end of most write-ups. This shouldn't be lengthy, and may already be evident for some schemes. Not needed for those not moving on. Delete John's [[ ]] comments when done.

- Ray and Daniel A
    - revise NTRUprime, New Hope, LAC, Three Bears, and Round 5

- Dustin
    - All of the above. Plus add in comments from Morgan.

Let's see if we can get the above done by Friday. Thanks!

Dustin

-path to standardization
- Morgan's comments
- LAC, New Hope, NTRU Prime, Round5, Three Bears, GeMSS a bit long,