From:	Scholl, Matthew A. (Fed)
To:	Chen, Lily (Fed); Moody, Dustin (Fed)
Cc:	Regenscheid, Andrew R. (Fed)
Subject:	Re: PQC next step
Date:	Wednesday, June 3, 2020 9:09:45 AM

Yes, sounds good. Having them as external werb should satisfy their desire to see an early copy as well but, if we can share before then that would put them at ease as well

---

From: "Chen, Lily (Fed)" <lily.chen@nist.gov>
Date: Wednesday, June 3, 2020 at 9:08 AM
To: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, "Scholl, Matthew A. (Fed)" <matthew.scholl@nist.gov>
Cc: "Regenscheid, Andrew R. (Fed)" <andrew.regenscheid@nist.gov>
Subject: Re: PQC next step

That will be fine.

Lily

On: 03 June 2020 09:07,
"Moody, Dustin (Fed)" <dustin.moody@nist.gov> wrote:

In addition, we had mentioned that maybe somebody at NSA could be one of the WERB reviewers, since they would likely have more technical background to make comments. So I guess that's one thing we were wondering. We could also just have internal reviewers. Andy says the NSA doesn't need pre-pub for WERB reviews, so that shouldn't be a problem in terms of delaying anything.

We feel confident in our expertise, but getting more eyes never hurts. From our last call with them, they said they are happy with our current plan. But they could provide some comments on more of the details in the report, which could be useful.

We should have a VERY rough 1st draft today, but we'll work to polish it up pretty quick.

Dustin

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Wednesday, June 3, 2020 8:59 AM
To: Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>
Cc: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>
Subject: PQC next step

Hi, Matt,

We will announce our 3rd round decision when a report is completed. We have selected readers for ERB process and will share “work-in-progress” draft to the readers and approvers. Hopefully, everything can be done in a few weeks.

Here is a question, shall we send the report to NSA for review? The time is a concern if they need pre-pub release for their comments. The report is released as a final version. That is, no public comments period like other standards. Their comments will not need to be released to the public, unless …. In this case, do they need pre-pub?

I might miss the points. Andy and Dustin?

Thanks,
Lily