From:	Scholl, Matthew A. (Fed)
To:	Moody, Dustin (Fed); Chen, Lily (Fed)
Cc:	Regenscheid, Andrew R. (Fed)
Subject:	Re: Any new comments on PQC report
Date:	Tuesday, June 30, 2020 11:21:09 AM

Understand and thanks Dustin,

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Tuesday, June 30, 2020 at 11:20 AM
To: "Scholl, Matthew A. (Fed)" <matthew.scholl@nist.gov>, "Chen, Lily (Fed)" <lily.chen@nist.gov>
Cc: "Regenscheid, Andrew R. (Fed)" <andrew.regenscheid@nist.gov>
Subject: Re: Any new comments on PQC report

Matt,

Several of the team discussed this topic just now. We agreed to change Andy's sentence to read:

" If new results emerge during the third round which undermine NIST's confidence in some of the finalists, NIST may extend the timeline or make changes to the process."

The rest of the report will be as it has been. It's not quite as specific as Andy was proposing, but he is good with the change.

Basically, we will cross whatever bridge is in the future when we come to it.

Dustin

From: Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>
Sent: Tuesday, June 30, 2020 9:39 AM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Cc: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>
Subject: Re: Any new comments on PQC report

Thanks Lily
Please have the discussion and I generally don't have comments, but if possible to erring on including a finalist or two more to for group consensus and clarity on what might happen between

finalists and alternates would helpful, if possible.
A quick summary after the meeting is good. I will support and defend what the team decides in the end.

From: "Chen, Lily (Fed)" <lily.chen@nist.gov>
Date: Tuesday, June 30, 2020 at 9:35 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: Any new comments on PQC report

Hi, Matt,

It looks like Andy's comment on a possibility of alternative candidates at the end of round 3 triggered a lot of discussions. The possibility may only apply to SPHINCS+ and FRODO (KEM), which is not agreed by everyone. We will have a meeting at 10:00. If you have any new comments, please let us know. If it is needed, we can provide a quick summary about the discussions.

Lily