

From: [Moody, Dustin \(Fed\)](#)
To: [internal-pqc](#)
Subject: Re: this week - PQC report
Date: Tuesday, June 23, 2020 9:33:59 AM

Actually, I hadn't read Dan's latest message when I wrote my last email. It would be good to discuss it. For those who can, please join.

Dustin

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Tuesday, June 23, 2020 9:27 AM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Re: this week - PQC report

All,

I don't have any major issues to discuss, so I don't think we need to meet at 10am. Nonetheless, I will be there and anybody can join to discuss anything they would like to.

Dustin

From: Moody, Dustin (Fed)
Sent: Monday, June 22, 2020 10:20 AM
To: internal-pqc <internal-pqc@nist.gov>
Subject: this week - PQC report

Everyone,

At our last meeting we cleared up several of the comments. Please take a look at the few remaining ones. It looks like we are getting close to done!

A few last assignments:

- Daniel Apon - please check NTRU. You have a comment about wanting to make sure the text is more positively phrased.
- Ray - please check New Hope. There is a comment there.
- Angela - please see if you can re-word the one sentence Lily commented about.
- Daniel ST - please check Rainbow. We want to make sure the write-up presents the case for it being a finalist.
- Everybody - John reworked the write up for SPHINCS+ in a few places. We need to review his changes.

I don't see a need for a meeting tomorrow, but if anybody would like to meet we could. Please send me an email if you'd like to have a meeting.

Thanks!

Dustin