From: Moody, Dustin (Fed)
To: Dang, Quynh H. (Fed); Perlner, Ray A. (Fed)
Subject: Re: meeting tomorrow at 10 am ?
Date: Thursday, June 25, 2020 2:42:44 PM

Kyber responded to Dan, and explained why they feel they meet category 1. It wasn't immediately obvious to us that they were wrong. In our report we call for more study on this.

We don't want to play Dan's game. This issue has been known for months. He only brings it up right during decision time. If there is some problem with Kyber, then we won't have to standardize it.

If you'd like to talk, why don't you send an email saying you'd like to discuss this tomorrow morning at 10am.

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Thursday, June 25, 2020 2:39 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Subject: Re: meeting tomorrow at 10 am ?

people looking at the forum discussion and the report would see that we were not sure whether or not Kyber-512 met the level 1 security, but still advanced it as a top finalist without publicly asking the Kyber's team to fix the issue.

I can talk more....

That would imply recklessness from us.

Quynh.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Thursday, June 25, 2020 2:34 PM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Subject: Re: meeting tomorrow at 10 am ?

I disagree.

We've stated our position, as has Kyber. We're encouraging them to look at this, as are we. Daniel A is going to communicate to them the suggestion that they might want to increase their noise.

But this doesn't need to all be figured out instantly right now. Every email from people in our group seems to agree with this. Hence, I'm not sure why we need a discussion?

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Thursday, June 25, 2020 2:25 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: meeting tomorrow at 10 am ?

we would be in trouble when we publish the report without doing one of the 2 options that I described.

Quynh.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Thursday, June 25, 2020 2:14 PM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Subject: Re: meeting tomorrow at 10 am ?

I did. But I haven't seen anybody that wants to dwell on this. I think they are okay to post the response we've written. We plan on getting into the weeds of coresvp, etc... but that doesn't have to happen before we respond, or before we release our decision and report. It'll take a little bit of time to do a good study.

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Thursday, June 25, 2020 2:12 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: meeting tomorrow at 10 am ?

Have you not read my first message today ?

Quynh.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Thursday, June 25, 2020 1:58 PM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Subject: Re: meeting tomorrow at 10 am ?

What do we need to discuss?

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Thursday, June 25, 2020 1:40 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: meeting tomorrow at 10 am ?

Hi Dustin,

We need to discuss a couple of things.

Are we going to meet at 10 am tomorrow ?

Quynh.