

From: [Kerman, Sara J. \(Fed\)](#)
To: [Moody, Dustin \(Fed\)](#)
Subject: RE: Report on Round 2 of the PQC process
Date: Wednesday, June 24, 2020 3:33:56 PM

Thanks – but we are **all** working as a good team!

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Wednesday, June 24, 2020 3:32 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: Re: Report on Round 2 of the PQC process

As usual, Sara, you are the best! Thanks.

Dustin

From: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Sent: Wednesday, June 24, 2020 3:31 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: Report on Round 2 of the PQC process

OK, I will wait until tomorrow afternoon to reach out to Kevin. I just spoke to Jim and he is going to hop back on line and send to Isabel today.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Wednesday, June 24, 2020 3:30 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: Re: Report on Round 2 of the PQC process

I'd sent him a slightly earlier version. In response to this email, I sent him the version I sent Jim and you.

Dustin

From: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Sent: Wednesday, June 24, 2020 3:29 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: Report on Round 2 of the PQC process

Is the version you sent him the same one you just sent Jim and I?

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Wednesday, June 24, 2020 3:27 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>

Subject: Fw: Report on Round 2 of the PQC process

From: Stine, Kevin M. (Fed) <kevin.stine@nist.gov>
Sent: Wednesday, June 24, 2020 1:27 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Report on Round 2 of the PQC process

Dustin,

I've read through most of the doc. I think it's well written and don't have any substantive comments. If/when you have an updated proposed final draft, feel free to send it my way. I'll do a quick once-over.

Thanks!

Kevin

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Wednesday, June 17, 2020 12:08 PM
To: Stine, Kevin M. (Fed) <kevin.stine@nist.gov>
Subject: Re: Report on Round 2 of the PQC process

We plan on being done with our revising no later than Friday of next week (June 26). Then hopefully the approval/publication process doesn't take too long. We don't have a hard day we want to release. Earlier I'd been hoping for the end of June, but it is fine to be early July. Sooner is better, but it's not an emergency or anything.

Dustin

From: Stine, Kevin M. (Fed) <kevin.stine@nist.gov>
Sent: Wednesday, June 17, 2020 11:58 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Report on Round 2 of the PQC process

Thanks Dustin! I really appreciate the early share. When are you hoping to release?

Thanks,

Kevin

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Wednesday, June 17, 2020 11:56 AM
To: Stine, Kevin M. (Fed) <kevin.stine@nist.gov>
Subject: Report on Round 2 of the PQC process

Kevin,

I'm not sure how much you're aware, but we've reached the end of round 2 of our post-quantum crypto standardization process. We've selected algorithms which will be moving on to the third round, and we're writing a report to document the process and explain our rationale.

I believe you will need to sign off on it for the ERB process. I'm attaching our current version so you can get a look at it, and hopefully facilitate a faster approval. The current version is still a draft, and will change a bit, but not too much.

Thanks,

Dustin