From: Robinson, Angela Y. (Fed)
To: Moody, Dustin (Fed)
Subject: RE: pqc meeting summary
Date: Tuesday, June 2, 2020 3:49:32 PM

This makes sense. Thank you!

Sent from Mail for Windows 10

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Tuesday, June 2, 2020 3:07:05 PM
To: Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>
Subject: pqc meeting summary

Angela,

Here's a summary of what we discussed today:

- We spent a good amount of time discussing the issues Dan raised in his forum post. It didn't change any of our round 3 decisions. We will continue to work on better understanding lattice security, and after we finish the report we'll do a deeper dive to make sure we have a good understanding. We'll probably communicate with some of the teams in question to have them respond and address this. We can mention some of these types of issues in our report.
- We'll invite Kris Gaj (and maybe others) to give us some presentations on hardware implementation recents. I forwarded you a copy of his recent report.
- We discussed the report, and reminded everybody of their assignments which are to be done by tomorrow. We're good with calling track 1 the "finalists". We don't have a clear name for track 2 yet. We'll explain the reasons for each scheme being there, which are a variety of reasons (high security or backup, niche applications, needs more development, etc). Ask any scheme which doesn't have level 5 parameters to include some. Allow broader tweaks for track 2 schemes, but caution them that larger tweaks slow down their standardization path.

Those are the main points anyway. I don't plan on meeting on Friday right now. Pretty much I just want people working on the report.

Dustin