From: Moody, Dustin (Fed)
To: Sonmez Turan, Meltem (Fed)
Subject: pqc round 2 report
Date: Wednesday, June 17, 2020 9:42:54 AM
Attachments: PQC Report on Round 2 June 16.docx

Meltem,

I'm attaching a current draft of our report. I'm curious your take on a few things. I forget how much I've told you, since we haven't been able to talk much (or practically at all). We are advancing algorithms in 2 tracks. The first are the finalists, which are the most promising ones. We'll likely select 1 (or 2) of both the KEMs and signatures. We then are keeping several alternate candidates into the third round, which have a variety of different reasons for keeping them, but for not being a finalist. Our main explanation of this is in section 2.3.

I was wondering if our rationale makes sense to somebody who is aware of our process, but not into all the details. Let me know what you think. Thanks!

I guess we'll talk this afternoon at our CTG re-group.

Dustin