From:	Perlner, Ray (Fed)
To:	Moody, Dustin (Fed); Apon, Daniel C. (Fed); Alperin-Sheriff, Jacob (Fed); Bassham, Lawrence E. (Fed)
Subject:	RE: On the pqc-forum thread "On Recommended Hardware"
Date:	Wednesday, February 6, 2019 1:47:00 PM

Seems good to me as well.

From: Moody, Dustin (Fed)
Sent: Wednesday, February 06, 2019 1:45 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>; Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Bassham, Lawrence E. (Fed) <lawrence.bassham@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Re: On the pqc-forum thread "On Recommended Hardware"

Thumbs up from me.

From: Apon, Daniel C. (Fed)
Sent: Wednesday, February 6, 2019 1:44:21 PM
To: Moody, Dustin (Fed); Alperin-Sheriff, Jacob (Fed); Bassham, Lawrence E. (Fed); Perlner, Ray (Fed)
Subject: On the pqc-forum thread "On Recommended Hardware"

Hi Dustin,
CC Jacob, Ray, Larry

After our meeting yesterday, Jacob posted that we want teams to focus on Cortex-M4 and Artix-7: https://groups.google.com/a/list.nist.gov/forum/#!topic/pqc-forum/cJxMq0_90gU

DJB comments that we should specify “Cortex-M4 with all options included.” Alright, sure -- it seems fine to post that we agree.

Further comments in the thread between Oscar, Kevin, Derek, and Markku have debated the virtue of implementations on Cortex-M0 and AVR.
I spoke with Larry briefly about this to get his perspective. It seems worthwhile for us to additional post something along the lines of..

“In order to best enable an ‘apples-to-apples’ comparison between hardware performance data, we recommend that teams generally focus hardware implementation efforts on Cortex-M4 ‘with all options included’ and Artix-7.
These devices were chosen primarily for their ubiquity of use. However, we also believe there is value in understanding the viability of post-quantum public-key crypto on even lighter-weight devices such as the Cortex-M0 or AVR microcontrollers.
We will certainly consider any experimental data gathered on such devices as a part of any candidate-scheme’s portfolio.”

Thoughts?