At this point I don't know specifically what we would say other than we'd like them to implement as many submissions as possible and give feedback on the efficiency of the algorithms. We may have others doing similar work and more data points is better.

Larry

From: "Apon, Daniel C. (Fed)" <daniel.apon@nist.gov>

Date: Monday, February 11, 2019 at 2:41 PM

To: "Bassham, Lawrence E. (Fed)" <lawrence.bassham@nist.gov>

Subject: FYI

Hi Larry,
(don't know if I've mentioned to you yet)

I am currently in the process of scheduling a trip to FPGA 2019 http://isfpga.org/ in about two weeks, to hand out flyers about NIST's PQC project (looking for more hardware teams interested in helping with evaluation of the 2nd Round candidates and/or helping with later-on optimization-in-hardware of the implementations), plus to be available to speak with anyone who is interested.

Perhaps we will hear back from a couple teams (along with whatever their particular specialties might be) by the end of March. I would love your input about how best we can task them onto interesting aspects of the project..

--Daniel