From: Chen, Lily (Fed)
To: Souppaya, Murugiah P. (Fed); Newhouse, Bill (Fed); Stine, Kevin M. (Fed); Barker, William C. (Assoc)
Cc: Moody, Dustin (Fed); Scholl, Matthew A. (Fed)
Subject: Re: Quantum ready project
Date: Wednesday, September 1, 2021 11:21:13 AM

Hi, Murugiah,

Thank you for providing a time estimate about when the implementation will start. We will keep each other posted about our next step. We will make sure you know what we are the most interested at each stage.

Lily

On 9/1/21, 8:16 AM, "Souppaya, Murugiah P. (Fed)" <murugiah.souppaya@nist.gov> wrote:

Hi Lily,

Thanks to Dustin and you for your support and socialization of the NCCoE Q-ready project. We are drawing attention from various groups and we appreciate you are participating on these calls with us.

We were hoping that the Q-ready project can inform the standardization process but due to the slow approval process we were not able to publish the FRN in a timely manner to initiate this project sooner.

Depending on the timing (hopefully we can get started in November) and how we want to prioritize the work, we can focus on tackling the activities that will most inform the standardization process first. We can schedule a call with you to solicit your input and guidance on things that will be of most value to the PQC's team. Then we can present them to the industry collaborators who will participating in the project at kickoff meeting to get consensus.

Murugiah

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Tuesday, August 31, 2021 10:30 AM
To: Newhouse, Bill (Fed); Souppaya, Murugiah P. (Fed); Stine, Kevin M. (Fed); Barker, William C. (Assoc)
Cc: Moody, Dustin (Fed); Scholl, Matthew A. (Fed)
Subject: Quantum ready project

Hi, Kevin, Murugiah, Bill, and Curt,

It is great that our NCCoE Q-ready project has got a lot of attention. The vendors and Canadian initiative reached us. It is indeed great that we started action before NIST PQC team makes selection. From PQC team's point of view, we hope this gives us opportunities to hear what will or will not work. Even in TLS 1.3 case, which algorithms we select may impact some implementation environment in different ways.

We have about another 4-5 months to make the first set of selection. We certainly will never feel that we received enough feedback from vendors, manufactures, and organizations. For any early starters for Q-ready, they may get into different algorithms, do they? Or the Q-ready will make sure no matter what we select, it will work in most of the environment?

Maybe when the solid implementation for the Q-ready project starts, it is the time that the selection is made.

Lily