From: Scholl, Matthew (Fed)
To: Goldstein, Barbara L. (Fed)
Subject: Re: Some PQC Slides
Date: Friday, February 8, 2019 11:45:29 AM

We have a long history of working with this community and we kind of galvanized them to work with us on these projects. I have luxury of others successes since the late 70s when NIST was the first to open cryptographic algorithms. If an algorithm is standardized by NIST it also "makes" the submitters in this field. So, its mostly precedent of the work being the defaults in global products that gains them the notoriety and the trust and belief in NIST that drives folks to submit.

We were not allowed to ask for only un-encumbered submissions by OGC. We specifically state that we will have a bias to open submissions. We have folks sign a Reasonable and Non Discriminatory agreement as a submission requirement.

The third item is a longer issue but we can point you to papers and staff who can go much deeper on the different types and families if you want

Matt

From: "Goldstein, Barbara L. (Fed)" <barbara.goldstein@nist.gov>
Date: Thursday, February 7, 2019 at 5:45 PM
To: "Scholl, Matthew (Fed)" <matthew.scholl@nist.gov>
Subject: RE: Some PQC Slides

Thanks Matt!

I was curious about:

- What motivates organizations to submit proposals?
- I was surprised that people could submit patented ideas – how would that really work?
- Is there somewhere easy to deepen my understanding of the types of proposals submitted, like code-based, lattice-based, KEM, hash, etc?

Thnx,
-b.

****

Barbara Goldstein
Associate Director, Physical Measurement Laboratory, NIST
Cell (preferred): 240-994-0452
Boulder: 303-497-6593 / Gaithersburg: 301-975-2304
bgoldstein@nist.gov

From: Scholl, Matthew (Fed)

Sent: Thursday, February 7, 2019 5:21 PM
To: Goldstein, Barbara L. (Fed) <barbara.goldstein@nist.gov>
Subject: Some PQC Slides