From:	Moody, Dustin (Fed)
To:	Cornwell, David [USA]
Subject:	RE: [External] RE: Comment on PQC algorithms
Date:	Thursday, January 31, 2019 10:55:00 AM

It would probably need to wait until after we get the tweaks from those submissions moving on. That deadline is March 15.

From: Cornwell, David [USA] <Cornwell_David@bah.com>
Sent: Thursday, January 31, 2019 10:54 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: [External] RE: Comment on PQC algorithms

Thanks Dustin for the information, link and consideration of the idea!

Thank you!

David Cornwell, PhD
CSTL Technical Director
Lead Engineer
Booz Allen Hamilton

Cyber Assurance Test Laboratory
1100 West Street
Laurel, MD 20707
(240) 547 5106
cornwell_david@bah.com

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Thursday, January 31, 2019 10:50 AM
To: Cornwell, David [USA] <Cornwell_David@bah.com>
Subject: [External] RE: Comment on PQC algorithms

David,
Thank you for the suggestion. We have included some such tables in presentations we have given (which are available on our website). But you are correct in that a table having all that info in a prominent place would be useful to observers. There are some other websites which do have this sort of information (for example https://www.safecrypto.eu/pqclounge/). When you start to create it, it turns out that there is a lot of data to represent, since each scheme can have multiple parameters for different security levels. We'll see what we can do.

Dustin

From: Cornwell, David [USA] <Cornwell_David@bah.com>
Sent: Thursday, January 31, 2019 10:45 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Comment on PQC algorithms

Hi Dustin,

NIST just announced the 26 candidates for Round 2. It would be really great to see a table with the following information on the NIST website:
Algorithm name, algorithm type (i.e. lattice, Code, Quadratic Equation) and key sizes. I think this would really help observers of the “competition” like me.

Thank you!

David Cornwell, PhD
CSTL Technical Director
Lead Engineer
Booz Allen Hamilton

Cyber Assurance Test Laboratory
1100 West Street
Laurel, MD 20707
(240) 547 5106
cornwell_david@bah.com