

From: [Moody, Dustin](#)
To: [Dodson, Donna F](#)
Cc: [Liu, Yi-Kai](#); [Chen, Lily](#)
Subject: RE: PQC NISTIR version 2
Date: Thursday, January 28, 2016 9:20:00 AM
Attachments: [PQC NISTIR v3.docx](#)

Donna,

Thank you for your comments. I've incorporated them in. You mentioned having Ed Roback reviewing the NISTIR before we publish. We're pretty much ready to publish, so if you think it's a good idea, could you forward it to him? I have met Ed once, but don't really know him. Thanks,

Dusitn

From: Dodson, Donna F
Sent: Monday, January 25, 2016 9:00 PM
To: Moody, Dustin <dustin.moody@nist.gov>; Perlner, Ray <ray.perlner@nist.gov>; Peralta, Rene <rene.peralta@nist.gov>; Chen, Lily <lily.chen@nist.gov>; Find, Magnus G. <magnus.find@nist.gov>; Jordan, Stephen P <stephen.jordan@nist.gov>; Liu, Yi-Kai <yi-kai.liu@nist.gov>; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu) <daniel-c.smith@louisville.edu>; Bassham, Lawrence E <lawrence.bassham@nist.gov>; Regenscheid, Andrew <andrew.regenscheid@nist.gov>; Scholl, Matthew <matthew.scholl@nist.gov>
Subject: Re: PQC NISTIR version 2

Dustin,

I added a few comments in the attached for your consideration. Thanks for sharing this.

Donna

From: "Moody, Dustin" <dustin.moody@nist.gov>
Date: Thursday, January 14, 2016 at 9:38 AM
To: Ray Perlner <ray.perlner@nist.gov>, Rene Peralta <rene.peralta@nist.gov>, Lily Chen <lily.chen@nist.gov>, "Find, Magnus G." <magnus.find@nist.gov>, "Jordan, Stephen P" <stephen.jordan@nist.gov>, "Liu, Yi-Kai" <yi-kai.liu@nist.gov>, "Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)" <daniel-c.smith@louisville.edu>, "Bassham, Lawrence E" <lawrence.bassham@nist.gov>, Andrew Regenscheid <andrew.regenscheid@nist.gov>, "donna.dodson@nist.gov" <donna.dodson@nist.gov>, Matthew Scholl <matthew.scholl@nist.gov>
Subject: PQC NISTIR version 2

Everyone,

I've incorporated the revisions and edits we discussed regarding the comments received from Donna and the NSA. Ray also included some new text in section 4. I've highlighted most of the changes to make it easy to see. Please review and make any comments by next Wednesday, January 20th. We want to publish this NISTIR by the end of the month if possible. Thanks!

Dustin