From: Moody, Dustin (Fed)
To: Chang, Shu-jen H. (Fed)
Subject: RE: Post-Quantum Crypto - Call For Submissions - comments requested
Date: Thursday, April 28, 2016 9:02:00 AM

Shu-jen,
Thank you so much for taking the time to go through it. We really appreciate it.
Dustin

From: Chang, Shu-jen H. (Fed)
Sent: Wednesday, April 27, 2016 6:15 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Barker, Elaine B. (Fed) <elaine.barker@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>; McKay, Kerry A. (Fed) <kerry.mckay@nist.gov>; Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>; Dang, Quynh (Fed) <quynh.dang@nist.gov>; Cooper, David A. (Fed) <david.cooper@nist.gov>; Bill Burr (b) (6) (b) (6) ; Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>
Cc: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu) <daniel-c.smith@louisville.edu>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>
Subject: Re: Post-Quantum Crypto - Call For Submissions - comments requested

I added my comments on top of Meltem's. Most of these are editorial comments except for the one that I shared yesterday.
From past experience, I suspect this CFS will need a review from the NIST Counsel. If that's the case, you probably need to make the text more accessible for the lawyers. I can imagine what kind of a process it will be like. Good luck.
Shu-jen

From: "Chang, Shu-jen H. (Fed)" <shu-jen.chang@nist.gov>
Date: Tuesday, April 26, 2016 at 6:08 PM
To: Dustin Moody <dustin.moody@nist.gov>, Elaine Barker <elaine.barker@nist.gov>, "Chang, Shu-jen H. (Fed)" <shu-jen.chang@nist.gov>, John Kelsey <john.kelsey@nist.gov>, Morrie Dworkin <morris.dworkin@nist.gov>, "McKay, Kerry A. (Fed)" <kerry.mckay@nist.gov>, "Sonmez Turan, Meltem (Assoc)" <meltem.turan@nist.gov>, Quynh Dang <quynh.dang@nist.gov>, "Cooper, David A. (Fed)" <david.cooper@nist.gov>, (b) (6) Andy Regenscheid <andrew.regenscheid@nist.gov>
Cc: "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>, "Chen, Lily (Fed)" <lily.chen@nist.gov>, Ray Perlner <ray.perlner@nist.gov>, "Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)" <daniel-c.smith@louisville.edu>, "Jordan, Stephen P (Fed)" <stephen.jordan@nist.gov>, Rene Peralta <rene.peralta@nist.gov>, Larry Bassham <lawrence.bassham@nist.gov>
Subject: Re: Post-Quantum Crypto - Call For Submissions - comments requested

Dustin,
I'm not done with my review yet, but I'd like to share my first non-editorial comment with you now, so you can think about how to address it.

Regarding the determination of whether a submission is “complete and proper”, I feel the point of having the "minimum acceptability requirements” might have been missed. For the SHA-3 competition, we set up these requirements so we could quickly run through each submission and decide whether it is an “Yes" for further evaluation, or “No". So the minimum acceptability requirements should be something that are easy to assess, not something that require time to analyze. I feel what you have listed in the draft may be more involved than necessary.

For the SHA-3 competition, we “evaluated” 64 submissions in less than five weeks, and posted the first-round candidates five weeks after the submission deadline. So there wasn’t much time to look into the specifics of each candidate. Our goal then was to accept all that merit a look, and reject only the “hopeless” submissions.

So, perhaps your team should think about what you plan to do for the first screening, and reflect that in the CFS.

Thanks,

Shu-jen

From: Dustin Moody <dustin.moody@nist.gov>

Date: Monday, April 18, 2016 at 12:34 PM

To: Elaine Barker <elaine.barker@nist.gov>, "Chang, Shu-jen H. (Fed)" <shu-jen.chang@nist.gov>, John Kelsey <john.kelsey@nist.gov>, Morrie Dworkin <morris.dworkin@nist.gov>, "McKay, Kerry A. (Fed)" <kerry.mckay@nist.gov>, "Sonmez Turan, Meltem (Assoc)" <meltem.turan@nist.gov>, Quynh Dang <quynh.dang@nist.gov>, "Cooper, David A. (Fed)" <david.cooper@nist.gov>, (b) (6) Andy Regenscheid <andrew.regenscheid@nist.gov>

Cc: "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>, "Chen, Lily (Fed)" <lily.chen@nist.gov>, Ray Perlner <ray.perlner@nist.gov>, "Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)" <daniel-c.smith@louisville.edu>, "Jordan, Stephen P (Fed)" <stephen.jordan@nist.gov>, Rene Peralta <rene.peralta@nist.gov>, Larry Bassham <lawrence.bassham@nist.gov>

Subject: Post-Quantum Crypto - Call For Submissions - comments requested

Everyone,

As you hopefully know, we are going to be calling for submissions for quantum-resistant algorithms to replace the current public-key algorithms in our standards. Our PQC team has written the attached Call for submissions, which we plan to release for public comments shortly. We’ve edited it pretty extensively in our group, but would like some more eyes to take a look, since this will be a pretty big undertaking.

Can you all please review the Call, and submit comments back by Friday, April 29th? We would greatly appreciate it. Any questions, just let me know. Thanks!

Dustin