From:	Chen, Lily (Fed)
To:	Moody, Dustin (Fed); Liu, Yi-Kai (Fed); Regenscheid, Andrew R. (Fed); Scholl, Matthew A. (Fed)
Subject:	RE: Update - CFP-PQC
Date:	Tuesday, July 19, 2016 1:21:31 PM
Attachments:	llc-PQC-Call for Proposals-Draft v1.docx

Dustin:

Take a look the suggested changes in 2.D.

Lily

From: Moody, Dustin (Fed)
Sent: Tuesday, July 19, 2016 11:47 AM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>; Scholl, Matthew (Fed) <matthew.scholl@nist.gov>
Subject: RE: Update - CFP-PQC

Andy/Lily,

I made some of the changes, but had a few questions which I put in the comments. Let me know what you think.

Dustin

From: Chen, Lily (Fed)
Sent: Tuesday, July 19, 2016 11:23 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>; Scholl, Matthew (Fed) <matthew.scholl@nist.gov>
Subject: RE: Update - CFP-PQC

Hi, Dustin:

Please notice that for the January 2, 1997 version of AES CFP the IP is included in the minimum acceptability part.

The draft minimum acceptability requirements and evaluation criteria are:
A.1 AES shall be publicly defined.
A.2 AES shall be a symmetric block cipher.
A.3 AES shall be designed so that the key length may be increased as needed.
A.4 AES shall be implementable in both hardware and software.
A.5 AES shall either be a) freely available or b) available under terms consistent with the American National Standards Institute (ANSI) patent policy.

Then in the final version of FRN, the IP is not included in the minimum acceptability. In SHA-3 FRN, it is also not in the minimum acceptability. Therefore, we can consider to put them to IP section not in minimum acceptability.

Lily

From: Moody, Dustin (Fed)
Sent: Tuesday, July 19, 2016 10:04 AM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>; Scholl, Matthew (Fed) <matthew.scholl@nist.gov>
Subject: Re: Update - CFP-PQC

I have some text ready that says we prefer royalty free, but I don't know exactly how I should modify the IPR statements. I will try and do it, and then send it to you and Andy.

Dustin

From: Chen, Lily (Fed)
Sent: Tuesday, July 19, 2016 10:02:41 AM
To: Moody, Dustin (Fed); Liu, Yi-Kai (Fed); Regenscheid, Andrew (Fed); Scholl, Matthew (Fed)
Subject: Update - CFP-PQC

Hi, Dustin:

It turned out that Henry is on leave this week. Instead of waiting, let's try to generate some text based on Henry's suggestion to incorporate the option of claiming IPR under the ANSI term. I think Andy has passed the hardcopy of AES draft CFP with the term. We will try to be clear about our strong preference on RF.

If you need any more information, please let me know. When you get the text there, please send to me and Andy. We will do a couple of passes before we send to Jennifer.

Thanks, I apologize for not determining to generate the text earlier. I should know better.

Lily