From:	Scholl, Matthew
To:	Chen, Lily; Moody, Dustin; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Perlner, Ray; Jordan, Stephen P; Liu, Yi-Kai; Peralta, Rene
Cc:	Dworkin, Morris J.
Subject:	Re: IPR question for PQC
Date:	Friday, January 29, 2016 10:56:23 AM
Attachments:	Third Draft NIST ITL Patent Process for Its Publications February 6 2015.docx

This is draft but has some good thoughts on this issue IMO.

From: "Chen, Lily" <lily.chen@nist.gov>
Date: Friday, January 29, 2016 at 10:43 AM
To: "Moody, Dustin" <dustin.moody@nist.gov>, "Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)" <daniel-c.smith@louisville.edu>, "Perlner, Ray" <ray.perlner@nist.gov>, "Jordan, Stephen P" <stephen.jordan@nist.gov>, "Liu, Yi-Kai" <yi-kai.liu@nist.gov>, "Peralta, Rene" <rene.peralta@nist.gov>
Cc: "Dworkin, Morris J." <morris.dworkin@nist.gov>, Matt Scholl <matthew.scholl@nist.gov>
Subject: RE: IPR question for PQC

I include Morrie. Morrie has discussed with lawyers on IPR issues for some modes. I also include Matt since I think we need to talk with NIST general council. We need to format our question and find a right person to talk with the lawyers.

Lily

From: Moody, Dustin
Sent: Friday, January 29, 2016 9:47 AM
To: Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Chen, Lily; Perlner, Ray; Jordan, Stephen P; Liu, Yi-Kai; Peralta, Rene
Subject: IPR question for PQC

Everyone,

We have (it seems to me) two possible ways we can approach the IPR issue in our call:

1) Require that there is no royalties, no IPR, require patent disclosures, etc.. during our process. Right will be returned to the submitters if we do not standardize their algorithm. This is similar to what was done with SHA-3, which then returned the rights to the submitters of the algorithms that weren't selected. If we do it this way, when would we return the rights? We're describing this as kind of like the modes process, where even if we don't initially choose to standardize an algorithm, it doesn't meet that it is "out".

2) We could ask for patent disclosures, but not require algorithms be royalty-free. We would need to warn submitters that it is obviously a big advantage to submit IPR free algorithms, as it will be a big factor in our decision.

Any thoughts? Do we need to get the advice of Matt/Donna/lawyers?

Dustin