From: Perlner, Ray (Fed)
To: Moody, Dustin (Fed)
Subject: RE: PQC post
Date: Thursday, January 12, 2017 11:49:00 AM

Seems fine with me. If it seems fine with you, go ahead and post it.

Thanks!

From: Moody, Dustin (Fed)
Sent: Thursday, January 12, 2017 11:26 AM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Re: PQC post

How about we simply say something like:

Recently we were asked a question about stateful hash-based signatures. Our position remains as described in our FAQ:

NIST plans to coordinate with other standards organizations, such as the IETF, to develop standards for stateful hash-based signatures. As stateful hash-based signatures do not meet the API requested for signatures, this standardization effort will be a separate process from the one outlined in the call for proposals. It is expected that NIST will only approve a stateful hash-based signature standard for use in a limited range of signature applications, such as code signing, where most implementations will be able to securely deal with the requirement to keep state.

From: Perlner, Ray (Fed)
Sent: Thursday, January 12, 2017 9:09:31 AM
To: Moody, Dustin (Fed)
Subject: RE: PQC post

I agree. Do you want to try to write something up, or should I?

From: Moody, Dustin (Fed)
Sent: Thursday, January 12, 2017 8:03 AM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: PQC post

Ray,

Did I hear John in the hallway saying the way he understood Rene's comments, he thought Rene was saying it's okay to submit stateful hash-based signatures? If so, she would do a short post re-iterating that our policy as stated on the FAQ remains our position?

What do you think?

Dustin

(I'm working from home today)