From:	Moody, Dustin (Fed)
To:	Barker, Elaine B. (Fed)
Subject:	Key establishment/agreement/transport in the PQC Call
Date:	Thursday, May 5, 2016 1:08:32 PM
Attachments:	CFP v9.docx

Elaine,

Thanks again for your comments on our PQC call for submissions. We've been working through the comments, and I wanted to take you up on your offer to help with the terminology we use for key-exchange in the call. We understand that we probably should use the correct terms from 56A/B, however, we worry that many of our target audience are not as familiar with the term key agreement as they are with key exchange. So we wonder what we should do. If would be nice to use key exchange if we can, as more people understand what we mean by that.

Also, we are seeking to replace our key establishment algorithms from 56A/B. Currently, there is not a good option for a direct replacement for Diffie-Hellman. We're still asking for key exchange (key agreement), because it would be nice if someone comes up with a good scheme, however it might not happen. The main reason we're asking for PQC encryption is to use it for key transport, as we are not sure we will have a good PQC key agreement scheme. We don't want to standardize PQC encryption for general encryption usage.

Having said that, would you mind going through the document once again and suggesting what terms to use for key establishment/agreement/transport? I left your comments about them in place, so you should hopefully be able to find the right spots quickly. Thanks,

Dustin