From:	Moody, Dustin (Fed)
To:	Perlner, Ray A. (Fed)
Date:	Friday, October 28, 2016 1:10:59 PM

We certainly do not intend to disqualify Diffie-Hellman type PQC key exchange algorithms from being submitted to us. If you look at the API we are suggesting to use, we believe that schemes such as New Hope and the SIDH can fit the KEM framework.
Dustin