From:	Moody, Dustin (Fed)
To:	Bassham, Lawrence E. (Fed)
Cc:	Regenscheid, Andrew R. (Fed)
Subject:	RE: PQC stuff
Date:	Thursday, August 31, 2017 10:03:57 AM

(b) (6) [redacted]

From: Bassham, Lawrence E (Fed)
Sent: Thursday, August 31, 2017 10:03 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>
Subject: PQC stuff

(b) (6) [redacted] I will get some work done, but I won't have everything done tomorrow. The API doc will be done. I don't want to promise more than that. I will work on things this weekend and have stuff to post on Tuesday. I plan to implement ctr_drbg in randombytes() and the seed expander. I'll also have the KAT generation files ready.