From: Moody, Dustin (Fed)
To: Bassham, Lawrence E. (Fed)
Subject: RE: KATs on SIKE
Date: Tuesday, October 17, 2017 1:40:31 PM

Noted.

From: Bassham, Lawrence E (Fed)
Sent: Tuesday, October 17, 2017 1:40 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: KATs on SIKE

You could let them know that the modified version of my file that they are using called "PQCtestKAT.c" needs to be slightly modified. The "../../KAT/PQCkemKAT" is three levels up. It needs to be "../../../KAT/PQCkemKAT".

Larry

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Monday, October 16, 2017 at 3:23 PM
To: "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>
Subject: KATs on SIKE

Larry,
Could you double check something for me? Jacob checked the KATs for SIKE, and the checklist says they didn't match on our end. They have a very experienced team, so I just wanted to double check that we didn't miss anything. Let me know. Thanks,

Dustin