From: Dang, Quynh (Fed)
To: Moody, Dustin (Fed)
Subject: Re: PQC CFP draft
Date: Wednesday, May 25, 2016 8:42:25 AM

That makes sense!

Quynh.

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Wednesday, May 25, 2016 at 8:40 AM
To: 'Quynh' <Quynh.Dang@nist.gov>
Subject: Re: PQC CFP draft

Quynh,
Thanks. Can you add something about the fact that passing FIPS validation doesn't say anything about the PQC algorithm. (i.e. having FIPS validation doesn't mean that the PQC part received any kind of scrutiny from NIST, which it won't since the testing won't do anything with it)

Dustin

From: Dang, Quynh (Fed)
Sent: Wednesday, May 25, 2016 8:25:18 AM
To: Moody, Dustin (Fed)
Subject: Re: PQC CFP draft

Hi Dustin,

The current text is : " First, as an interim solution, NIST allows the use of "hybrid modes," which combine a currently approved cryptographic algorithm with a post-quantum algorithm, in such a way that the combined system is at least as secure as the stronger of the two components. Such hybrid modes can be approved for use under existing NIST guidelines.", my proposed replacement is below.

"First, as an interim solution, NIST allows the use of any "hybrid mode" which combines a currently approved cryptographic algorithm with a post-quantum algorithm when the module that contains the hybrid mode passes the FIPS 140 validation. Noted that: currently, in order to pass the FIPS 140 validation, none of the post-quantum algorithm's components including its input and output makes the implementation of the currently approved cryptographic algorithm fail any of its FIPS 140 requirements (including security properties of the currently approved cryptographic algorithm). Such hybrid modes will be examined by NIST with case-by-case basic."

Quynh.