From: Moody, Dustin (Fed)
To: Kelsey, John M. (Fed); Cooper, David (Fed)
Cc: internal-pqc
Subject: Re: Report
Date: Thursday, June 11, 2020 10:37:27 PM

It's in the report, section 4.

From: Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Sent: Thursday, June 11, 2020 3:59 PM
To: Cooper, David A. (Fed) <david.cooper@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: Re: Report

We should probably put that into the report, as well.

--John

From: "David A. Cooper" <david.cooper@nist.gov>
Date: Thursday, June 11, 2020 at 15:55
To: "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: Re: Report

On 6/11/20 3:38 PM, Kelsey, John M. (Fed) wrote:

> Should we state that we see some of these algorithms as direct competitors? (That is, we're unlikely to standardize Kyber, Saber, and NTRU, or Falcon and Dilithium.)

Hi John,
I can't remember if this is mentioned in the report, but the following appears in the current announcement text:

> As CRYSTALS-KYBER, NTRU, and SABER are all structured lattice schemes, NIST intends to select at most one for the standard. The same is true for the signature schemes CRYSTALS-DILITHIUM and FALCON.