From:	Foti, James (Fed)
To:	Moody, Dustin (Fed)
Subject:	RE: modifying a NISTIR?
Date:	Monday, April 8, 2019 9:13:52 AM

Sounds good!

From: Moody, Dustin (Fed)
Sent: Monday, April 8, 2019 9:07 AM
To: Foti, James (Fed) <james.foti@nist.gov>; Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: RE: modifying a NISTIR?

Thanks, Jim.

Let's leave things as they are, as you suggest. We'll talk it over amongst the team, and let you know if there is some reason to think differently.

Dustin

From: Foti, James (Fed)
Sent: Monday, April 8, 2019 9:05 AM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Cc: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: RE: modifying a NISTIR?

Hi Dustin-

I can understand both angles. Since this is a NISTIR and not a policy document, we can easily make an argument that that statement applied to the PQC standardization effort *_at the time that it was written_* , and we always have the option to change our minds based on unforeseen changes (e.g., in technology, law, policy, etc.).

IMO, I would lean towards keeping it as-is, unless you all think it's critical to have it changed. Slipping it in there might also raise some eyebrows—I'm sure there will be detail-oriented people who notice the change. Another option is to put some brief remark clarifying this in the PQC FAQ and/or at https://csrc.nist.gov/publications/detail/nistir/8240/final as a "planning note". But once again, even doing something as minor as that might raise questions among your stakeholders that lead to speculation that we're going to add one of those algorithms to the 2nd round, mid-stream. Seems high-risk, low reward to me.

Jim

From: Kerman, Sara J. (Fed)
Sent: Monday, April 8, 2019 8:51 AM

To: Foti, James (Fed) <james.foti@nist.gov>
Cc: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: FW: modifying a NISTIR?

From: Moody, Dustin (Fed)
Sent: Monday, April 08, 2019 8:48 AM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: RE: modifying a NISTIR?

I'm not sure if it was accidentally omitted. What we wrote is and was correct. Daniel is suggesting we add this on to potentially cover our bases in the future. In the case that after our "competition", we later decide we like something that we eliminated. It's probably not a likely scenario, but it doesn't hurt anything to me.

Dustin

From: Kerman, Sara J. (Fed)
Sent: Monday, April 8, 2019 8:44 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: RE: modifying a NISTIR?

Jim's response:

We can probably get them to swap the file without having to do an errata. Is it safe to say that this phrase was accidentally omitted from the document?

Jim

From: Moody, Dustin (Fed)
Sent: Monday, April 08, 2019 8:17 AM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: modifying a NISTIR?

Sara and Lily,

Daniel Smith-Tone asked me if it would be possible to slightly modify our NISTIR 8240 (Status Report on 1st Round). I didn't know if this is possible? He wants us to add "at this time" to the end of the sentence "The algorithms which were not selected to advance to the next round are not under consideration for standardization by NIST." Is this something we can do?

Dustin