From: Moody, Dustin (Fed)
To: Smith-Tone, Daniel (Fed)
Subject: RE: NISTIR 8240
Date: Monday, April 8, 2019 9:02:00 AM

Daniel,

As to the 2nd point, it looks like we can probably change the NISTIR if we want, but Lily wants to talk about it before doing so.

Dustin

From: Smith-Tone, Daniel (Fed)
Sent: Saturday, April 6, 2019 1:15 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: NISTIR 8240

Hi, Dustin,

I have a couple of comments on NISTIR 8240 that I think are relevant for future iterations of our reports.

First, I think that this report should be an interagency report and not an internal report. The purpose of the document is to report to other agencies and the community outside of NIST the status of our project. I may be mistaken, but I think that some of what we called NISTIRs in the past were labeled as interagency reports. Lily would know. I think that we had this before and it would be nice to have this be accurate.

Second, at the end of Section 2, there is a comment," The algorithms which were not selected to advance to the next round are not under consideration for standardization by NIST." I think that this is a completely accurate statement, but perhaps a little strong sounding. I don't have a strong feeling on this, but I would have a slight preference to add, "at this time," at the end of the sentence in future iterations of our documents. This phrasing puts us in the optimal position for making future claims under any circumstance. For example, if there is a major change in the landscape that renders a broad class of schemes unusable, the above phrasing puts us in a better position to move towards standardizing one of the eliminated schemes in a later standardization effort if it then seems more attractive (or has better theoretical justification, or something similar).

I want to have a record of my concerns because I will forget otherwise, hence, the email.

Cheers,
Daniel the Elder