From: Scholl, Matthew A. (Fed)
To: Romine, Charles H. (Fed)
Cc: Stine, Kevin M. (Fed)
Subject: FW: draft Status Report on the 2nd Round of the NIST PQC Standardization Process
Date: Friday, June 26, 2020 4:03:59 PM

Some relevant language in our draft report.

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Friday, June 26, 2020 at 1:39 PM
To: "Scholl, Matthew A. (Fed)" <matthew.scholl@nist.gov>, "Regenscheid, Andrew R. (Fed)" <andrew.regenscheid@nist.gov>
Cc: "Chen, Lily (Fed)" <lily.chen@nist.gov>
Subject: Re: draft Status Report on the 2nd Round of the NIST PQC Standardization Process

Relevant lines in the report:

- in the SPHINCS+ writeup:

  NIST sees SPHINCS+ as an extremely conservative choice for standardization. If NIST's confidence in better performing signature algorithms is shaken by the end of the third round, SPHINCS+ could provide an immediately available algorithm for standardization. Further, if NIST sees the need for an additional signature algorithm for applications that need very high security and can tolerate larger and slower signatures, NIST may decide to standardize SPHINCS+ in the future.

  (note that we say it could be immediately available if needed)

- in a few places we mention the alternate candidates are still being considered for standardization, although "most likely after another round". We were careful to not exclude the possibility of standardizing one after the 3rd round.

- In our announcement, we have the line:

  "Note – These are NIST's current plans. NIST reserves the right to modify the process in the future."

  I added the sentence "NIST also reserves the right to modify the process in the

future, should circumstances warrant." into the conclusion of the report.

Does this seem sufficient for what we expect?

Dustin