**Guidelines for submitting tweaks for Third Round Finalists and Candidates**
Deadline: October 1, 2020

Finalist and Candidate teams must meet the same submission requirements and minimum acceptability criteria as given in the original Call for Proposals. Submissions must be submitted to NIST at pqc-submissions@nist.gov by October 1, 2020. It would be helpful if submission teams provided NIST with a summary of their expected changes by August 10, 2020. If either of these deadlines will pose a problem for any submission team, they should contact NIST in advance. In particular, submissions should include a cover sheet, algorithm specifications (and other supporting documentation), and optical/digital media (e.g., implementations, known-answer test files, etc.) as described in Section 2 of CFP.

NIST does NOT need new signed IP statements unless new submission team members have been added or the status of intellectual property for the submission has changed. If either of these cases apply, NIST will need new signed IP statements (see Section 2.D of the CFP). These statements must be actual hard copies—not digital scans—and must be provided to NIST by the 3rd NIST PQC Standardization Conference. In particular, NIST will need new signed IP statements for new members of the merged Classic McEliece team.

In addition, NIST requires a short document outlining the modifications introduced in the new submission. This document should be included in the Supporting Documentation folder of the submission (see Section 2.C.4 of the CFP). NIST will review the proposed changes to see if they meet the submission requirements and minimum acceptability requirements, as well as if they would significantly affect the design of the algorithm, requiring a major re-evaluation. As a general guideline, NIST expects any modifications to the seven finalists to be relatively minor while allowing more latitude to the eight alternate candidate algorithms. Note, however, that larger changes may signal that an algorithm is not mature enough for standardization for some time.

As performance will continue to play a large role in the third round, NIST offers the following guidance. Submitters must include the reference and optimized implementation (which can be the same) with their submission package. The reference implementation should still be in ANSI C; however, the optimized implementation is not required to be in ANSI C. NIST strongly recommends also providing an AVX2 (Haswell) optimized implementation and would encourage other optimized software implementations (e.g. microcontrollers) and hardware implementations (e.g. FPGAs).

NIST is aware that some submission packages may be large in size. The email system for pqc-submissions@nist.gov is only set to handle files up to 25MB. For files which are larger, you may upload your submission package somewhere of your choosing and send us the download link when you submit. If that option is not suitable, NIST has a file transfer system that can be used. To find out about this option, please send a message to pqc-comments@nist.gov. NIST will review the submitted packages as quickly as possible and post the candidate submission packages which are “complete and proper” on our webpage www.nist.gov/pqcrypto. Teams are encouraged to submit early. General questions may be asked on the pqc-forum. For more specific questions, please contact us at pqc-comments@nist.gov.