From: Moody, Dustin (Fed)
To: Dang, Quynh H. (Fed)
Subject: RE: 2nd draft of Submission Merging Guidelines
Date: Thursday, April 26, 2018 2:16:15 PM

We aren't expecting many to merge. And if two teams merge (neither of which is strong enough), well yes, it would be lots of work for no benefit. But we are asking them to tell us first. And also saying that the rest of the merged submission isn't due until later. I suspect that's what will occur. If they tell us they are merging – we can probably give them guidance before they do a lot of work that it might not be necessary

---

From: Dang, Quynh (Fed)
Sent: Thursday, April 26, 2018 2:14 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: 2nd draft of Submission Merging Guidelines

They would be super mad because they would think that you were going to eliminate my algorithms but asked/let me do a lot of extra work like that.

Quynh.

From: Moody, Dustin (Fed)
Sent: Thursday, April 26, 2018 2:11:52 PM
To: Dang, Quynh (Fed)
Subject: RE: 2nd draft of Submission Merging Guidelines

We don't really expect a large number to merge. We do plan for teams to at least tell us they will merge before the 2nd round selection. Yeah, it would be too bad if they merge and they are gone. But if they are gone, they are gone

---

From: Dang, Quynh (Fed)
Sent: Thursday, April 26, 2018 2:08 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: 2nd draft of Submission Merging Guidelines

Hi Dustin,

Do you plan for merging to happen before the second round selection announcement (submitting merges before NOV 30) ? It would be bad if after some submissions get merged then they get eliminated right away.

Quynh.

From: Moody, Dustin (Fed)
Sent: Thursday, April 26, 2018 1:52:24 PM
To: internal-pqc
Cc: daniel-c.smith@louisville.edu
Subject: 2nd draft of Submission Merging Guidelines

I incorporated Jacob's and Ray's comments. Let me know if anybody has any other thoughts….

Dustin

NIST would like to encourage any submissions which are quite similar to consider merging. It would be helpful if any such merger be announced (to NIST) before November 30th. Along with a statement of which schemes are merging, merging teams should submit a separate brief document which highlights which aspects of each of the merged schemes are to be used, referring if possible to the already submitted Supporting Documentation for each of the schemes. The actual specification of the merged scheme should be ready by the deadline for round 2 tweaks to other submissions, and must meet the same standards.

A few points regarding this:

- Schemes should only merge which are similar, and the merged scheme should be in the span of the two original submissions.
- While merging will obviously necessitate some changes, we do not want substantial re-designs. Parameters may be updated, but we will still be considering the parameters from the original submissions.
- Schemes which are KEMs or PKEs can be merged into one scheme. Schemes which are CPA or CCA can also be combined.
- The merged submission should be sent to pqc-submissions@nist.gov, and should satisfy the requirements set forth in the NIST Call For Proposals (available at www.nist.gov/pqcrypto). In particular, the merged submission will need to include a reference and optimized implementation (which can be the same), as well as new signed IP statements.
- NIST will review the merged submission to verify that it meets the acceptability requirements from the Call For Proposals, as well as to check that the changes are not too major and are in scope.
- Teams may contact us at pqc-comments@nist.gov for more specific questions regarding merging.