From:	Perlner, Ray (Fed)
To:	Moody, Dustin (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Jordan, Stephen P (Fed); Liu, Yi-Kai (Fed); Chen, Lily (Fed); Bassham, Lawrence E. (Fed); Peralta, Rene C. (Fed)
Subject:	RE: My write-up in the PQC call
Date:	Tuesday, March 22, 2016 3:06:46 PM
Attachments:	CFP v2 Ray + Sec4c.docx

Ok. Dustin Convinced me to put something in for section 4c

Please review the attached version.

From: Perlner, Ray (Fed)
Sent: Tuesday, March 22, 2016 2:28 PM
To: Moody, Dustin (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Jordan, Stephen P (Fed); Liu, Yi-Kai (Fed); Chen, Lily (Fed); Bassham, Lawrence E (Fed); Peralta, Rene (Fed)
Subject: RE: My write-up in the PQC call

Here's my first cut on section 4.

Note I haven't written anything for section 4c.

Regarding what was written previously for SHA3

1) I don't think we need to encourage submitters to have MORE tunable parameters (arguably lattice schemes have to many as it is.)
2) Flexibility also seems like something that could get us in trouble. (Do we really want to spend oodles of cycles deciding whether we want to standardize "add ons" as we have for SHA3?)
3) Things like misuse resistance and simplicity are already mentioned in the security section and could probably be expanded upon if needed.

From: Moody, Dustin (Fed)
Sent: Tuesday, March 22, 2016 11:44 AM
To: Perlner, Ray (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Jordan, Stephen P (Fed); Liu, Yi-Kai (Fed); Chen, Lily (Fed); Bassham, Lawrence E (Fed); Peralta, Rene (Fed)
Subject: My write-up in the PQC call

I've attached my parts of the PQC call for submission.

Dustin