From: Moody, Dustin
To: Chen, Lily (Fed); Peralta, Rene C. (Fed); Perlner, Ray A. (Fed); Jordan, Stephen P; Chen, Lily (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Scholl, Matthew A. (Fed); Dworkin, Morris J. (Fed); Regenscheid, Andrew R. (Fed)
Subject: IPR for PQCrypto Call for Proposals
Date: Thursday, February 11, 2016 2:48:44 PM

Everyone,

After further discussion in our PQC group, we think the best course for IPR for the PQCrypto Call For Proposals is to use the same language as in the SHA-3 competition:

> "Each submitted algorithm must be available worldwide on a royalty free basis during the period of ~~the hash function competition~~. In order to ensure this and minimize any intellectual property issues, the following series of signed statements are required for a submission to be considered complete…."

One of the statements they have to sign has the following text:

> "If my algorithm (or the derived algorithm) is not selected for SHA–3 (including those that are not selected for the second round of public evaluation), I understand that all rights, including use rights of the reference and optimized implementations, revert back to the submitter (and other owner[s], as appropriate). Additionally, should the U.S. Government not select my algorithm for SHA–3 at the time NIST ends the competition, all rights revert to the submitter (and other owner[s] as appropriate)."

So we'd have to modify that a bit. The post-quantum search process will have an end date, where we summarize our findings and decide which (if any) algorithms we will standardize. However, we do not mean to say that any algorithm which has not been selected at that point is no longer to be considered for standardization. Similar to the modes process, we want quantum-resistant algorithms to be able to be considered (and standardized) even after our competition-like search process ends. We can write in our Call that any submitter may withdraw their submission at any time (assuming we haven't selected it), and all rights would be returned. Or we might narrow our focus at some point and publicly state that certain algorithms are no longer under our consideration, and again the rights would be returned.

Please let us know of any comments or concerns. I'm going to be announcing our Call for Submissions at PQCrypto on Feb. 24th. I won't be giving too detailed of a presentation, but need to make sure I correctly describe how we will approach the IPR issue.

Thanks,
Dustin