

**From:** [Moody, Dustin \(Fed\)](#)  
**To:** [Alperin-Sheriff, Jacob \(Fed\)](#); [Bassham, Lawrence E. \(Fed\)](#); [Chen, Lily \(Fed\)](#); [Daniel Smith-Tone](#); [Jordan, Stephen P \(Fed\)](#); [Liu, Yi-Kai \(Fed\)](#); [Miller, Carl A. \(Fed\)](#); [Moody, Dustin \(Fed\)](#); [Peralta, Rene C. \(Fed\)](#); [Perlner, Ray A. \(Fed\)](#); [Smith-Tone, Daniel C. \(Fed\)](#)  
**Subject:** (preliminary) final versions of CFP and FAQ  
**Date:** Friday, October 28, 2016 9:41:43 AM  
**Attachments:** [FAQ 2.2.docx](#)  
[final CFP v4.4.docx](#)

---

Everyone,

Ray and Yi-Kai came to consensus on the quantum security section of the CFP. Yay!

As a result, we've now resolved all the comments. See the attached versions of the CFP and FAQ. We plan to post on our approach to quantum security, our change regarding KEMs, and the API on the pqc-forum today. We'll see what feedback we get, which may prompt us to do one more round of editing as a result.

Thank you everyone.

Dustin