

**From:** [Perlner, Ray \(Fed\)](#)  
**To:** [Liu, Yi-Kai \(Fed\)](#); [Moody, Dustin \(Fed\)](#)  
**Cc:** [Chen, Lily \(Fed\)](#); [Daniel C Smith \(daniel-c.smith@louisville.edu\)](#) ([daniel-c.smith@louisville.edu](#)); [Jordan, Stephen P \(Fed\)](#); [Peralta, Rene C. \(Fed\)](#); [Bassham, Lawrence E. \(Fed\)](#)  
**Subject:** RE: Final revisions of the CFP for our first draft  
**Date:** Tuesday, April 12, 2016 3:02:59 PM  
**Attachments:** [CFP v6 Ray YKL RayComments.docx](#)

---

Thanks Yi-Kai.

I read through your changes and provided comments. I took your statement that the section on quantum cryptanalysis still needs a bit more work as an invitation to edit it extensively. I also moved a paragraph of text in section 3. I think everything else is intact aside from some comments and replies to your comments.

Cheers,  
Ray

---

**From:** Liu, Yi-Kai (Fed)  
**Sent:** Monday, April 11, 2016 8:24 PM  
**To:** Perlner, Ray (Fed) <[ray.perlner@nist.gov](mailto:ray.perlner@nist.gov)>; Moody, Dustin (Fed) <[dustin.moody@nist.gov](mailto:dustin.moody@nist.gov)>  
**Cc:** Chen, Lily (Fed) <[lily.chen@nist.gov](mailto:lily.chen@nist.gov)>; Daniel C Smith ([daniel-c.smith@louisville.edu](mailto:daniel-c.smith@louisville.edu)) ([daniel-c.smith@louisville.edu](mailto:daniel-c.smith@louisville.edu)) <[daniel-c.smith@louisville.edu](mailto:daniel-c.smith@louisville.edu)>; Jordan, Stephen P (Fed) <[stephen.jordan@nist.gov](mailto:stephen.jordan@nist.gov)>; Peralta, Rene (Fed) <[rene.peralta@nist.gov](mailto:rene.peralta@nist.gov)>; Bassham, Lawrence E (Fed) <[lawrence.bassham@nist.gov](mailto:lawrence.bassham@nist.gov)>  
**Subject:** Re: Final revisions of the CFP for our first draft

Hi everyone,

I went through the CFP and made a bunch of edits. I think it's in pretty good shape.

The section on quantum cryptanalysis still needs a bit more work, but I think it is converging to a good solution. Ray, thanks for your work on that!

Cheers,  
--Yi-Kai

---

**From:** Perlner, Ray (Fed)  
**Sent:** Friday, April 8, 2016 2:12:55 PM  
**To:** Moody, Dustin (Fed); Liu, Yi-Kai (Fed)  
**Cc:** Chen, Lily (Fed); Daniel C Smith ([daniel-c.smith@louisville.edu](mailto:daniel-c.smith@louisville.edu)) ([daniel-c.smith@louisville.edu](mailto:daniel-c.smith@louisville.edu)); Jordan, Stephen P (Fed); Peralta, Rene (Fed); Bassham, Lawrence E (Fed)  
**Subject:** RE: Final revisions of the CFP for our first draft  
[Here are my edits to section 3 and 4.](#)

---

**From:** Moody, Dustin (Fed)  
**Sent:** Thursday, April 07, 2016 3:00 PM  
**To:** Perlner, Ray (Fed) <[ray.perlner@nist.gov](mailto:ray.perlner@nist.gov)>; Liu, Yi-Kai (Fed) <[yi-kai.liu@nist.gov](mailto:yi-kai.liu@nist.gov)>  
**Cc:** Chen, Lily (Fed) <[lily.chen@nist.gov](mailto:lily.chen@nist.gov)>; Daniel C Smith ([daniel-c.smith@louisville.edu](mailto:daniel-c.smith@louisville.edu)) ([daniel-c.smith@louisville.edu](mailto:daniel-c.smith@louisville.edu)) <[daniel-c.smith@louisville.edu](mailto:daniel-c.smith@louisville.edu)>; Jordan, Stephen P (Fed) <[stephen.jordan@nist.gov](mailto:stephen.jordan@nist.gov)>; Peralta, Rene (Fed) <[rene.peralta@nist.gov](mailto:rene.peralta@nist.gov)>; Bassham, Lawrence E (Fed) <[lawrence.bassham@nist.gov](mailto:lawrence.bassham@nist.gov)>  
**Subject:** Final revisions of the CFP for our first draft

Ray, Yi-Kai,

Please use the attached to make your revisions. I believe Ray is going to address some things in

Section 3 and 4. Yi-Kai will work on the remaining few comments. They plan on being done by next Monday, COB.

Starting next Tuesday, we want everyone to read the CFP and provide feedback by Friday. We can then send the CFP to Andy, Matt, Donna, etc... the following week.

Thanks everyone!

Dustin