From: Moody, Dustin (Fed)
To: Peralta, Rene (Fed)
Subject: RE: CFP v8 - ready to send on
Date: Monday, April 18, 2016 12:16:00 PM

Thanks!

From: Peralta, Rene (Fed)
Sent: Monday, April 18, 2016 12:01 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>
Cc: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu) <daniel-c.smith@louisville.edu>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>
Subject: Re: CFP v8 - ready to send on

OK. A list of small stuff in no particular order. Apologies if all this has been noticed already.

page 2: "...multivariate cryptosystems, hash-based signatures, and many others "

I suggest removing "many"

page 3: "...NIST will solicit proposals ..."

Isn't this the solicitation?

page 6: "If the execution of an algorithm produces intermediate results that are informative (e.g., for debugging an implementation of the algorithm), then the submitter shall include known answers for those intermediate values for the computation for each of the required security strengths. "

I suggest removing "for the computation"

page 6: "To prevent the existence of possible ‘‘trap-doors’’ in an algorithm, the submitter shall explain the provenance of any constants or tables used in the algorithm, with justification of why these were not chosen to make some attack easier."

I suggest removing "with justification of why these were not chosen to make some attack easier"

(if you decide to keep this, you might want to reword).

page 7: "Additionally the statement shall discuss the additional attack scenarios specified in section 4.A.5.

I don't think section 4.A.5 is meant to contain an exhaustive list of attacks. This makes the use of "shall" here a little hard to interpret. How about
"Additionally, the statement may discuss additional attack scenarios (see section 4.A.5.)."

actually, we could still use "shall" in this rewording, but I think "may" is better.

page 12: "The algorithms shall not incorporate major components that are not believed to be secure agains quantum computers."

I suggest removing this. I can imagine a design that does something useful with functions that are not one-way with respect to quantum computation.

If you keep it. Note typo "agains".

page 16: "Likewise, schemes whose design principles can be related to an established body of cryptographic research tend to be better understood than schemes that are completely new, or schemes that were designed by repeatedly patching older schemes which were shown vulnerable to cryptanalysis."

I'm having trouble with the last phrase. I think the intent is to say that "schemes that were designed by repeatedly patching older schemes which were shown vulnerable to cryptanalysis" are not "related to an established body of cryptographic research". Or maybe "schemes .. cryptanalysis" are not "well understood". ??? Either statements would be hard problematic. Maybe it's just me...

page 17: "As noted in section 4.C.5, the most ..."

I think we mean "section 4.A.5"

page 18: "... make (any) final selections ..."

I'm not sure what "(any)" is conveying. I guess we are trying to say that we may not make a final selection? I would just remove it. Ditto with "Any selected ..." on page 20.

page 21: " ... at the Conference. Details of the conference ..."

We probably want to be consistent with capitalization.

Regards, Rene.

From: Moody, Dustin (Fed)
Sent: Monday, April 18, 2016 10:57 AM
To: Peralta, Rene (Fed); Chen, Lily (Fed)

Cc: Liu, Yi-Kai (Fed); Perlner, Ray (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Jordan, Stephen P (Fed); Bassham, Lawrence E (Fed)
Subject: RE: CFP v8 - ready to send on

Sure. If you can send them to me within an hour (or two), that should be fine. Thanks!

Dustin

From: Peralta, Rene (Fed)
Sent: Monday, April 18, 2016 10:56 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>
Cc: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu) <daniel-c.smith@louisville.edu>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>
Subject: Re: CFP v8 - ready to send on

Oops, hold on. I have a number of corrections I need to put in an email.
Do I have an hour? Doing something else now.

Rene.

From: Moody, Dustin (Fed)
Sent: Monday, April 18, 2016 10:55 AM
To: Chen, Lily (Fed)
Cc: Liu, Yi-Kai (Fed); Perlner, Ray (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Jordan, Stephen P (Fed); Peralta, Rene (Fed); Bassham, Lawrence E (Fed)
Subject: CFP v8 - ready to send on

Lily,

Yi-Kai, Ray, and I met and hammered out the last few comments we had left on the Call. I believe we are ready to send it on to more readers for comments. Who do we want to send it to? Andy, Matt, Donna. Who else? The lawyers who will need to sign off? Do we know if we need to put this in the Federal Register? If we do, perhaps we can start the process with this version, and later update to a newer version with any revisions we needed to make. Please let us know.

Dustin

A big THANK YOU to everyone for helping write and edit this document. We'll have plenty of editing to do after we continue to receive comments, but getting this created was a great accomplishment.

Yi-Kai did a great job of spearheading this effort, and thanks also to Ray who did more than his fair share of the writing.