| | |
|---|---|
| **From:** | Moody, Dustin (Fed) |
| **To:** | Kerman, Sara J. (Fed) |
| **Subject:** | RE: PQC Comments that we will want to post |
| **Date:** | Wednesday, November 2, 2016 8:54:58 AM |

---

Looks good.
Yes – hold off on posting.

---

**From:** Kerman, Sara J. (Fed)
**Sent:** Wednesday, November 02, 2016 8:43 AM
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
**Subject:** RE: PQC Comments that we will want to post
OK, all bold codes have been removed and anywhere someone used blue. The only fonts remaining are the syntax-like code and if people used italics.
We holding off posting this until the new FNR/CFP comes out, right?

---

**From:** Moody, Dustin (Fed)
**Sent:** Wednesday, November 02, 2016 8:00 AM
**To:** Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
**Subject:** RE: PQC Comments that we will want to post
I think for Jintai's, we can un-bold. Looking through the rest, a few times a heading has been bolded. We can un-bold those, unless you think it's a bad idea.
Dustin

---

**From:** Kerman, Sara J. (Fed)
**Sent:** Tuesday, November 01, 2016 3:46 PM
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
**Subject:** RE: PQC Comments that we will want to post
If someone has certain things bolded, should I leave? Or not? i.e., Jintai Ding
omments and questions on the NIST call for PQC standards.

**Proposed Minimum Acceptability Requirements**

**For Part 2,**

**what if the submission infringes on others' patent or patent application and does not disclose it?**

**In Part 4, it says:**

"The submission package shall provide concrete values for any parameters and settings required to meet or exceed (to the best of the submitter's knowledge) the relevant security targets in Section 4.A.4, for the appropriate security models in Sections 4.A.2 and 4.A.3."

---

**From:** Moody, Dustin (Fed)
**Sent:** Tuesday, November 01, 2016 2:48 PM
**To:** Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
**Subject:** Re: PQC Comments that we will want to post
For the code, we can probably leave the text as is. But maybe make all the rest the same font and size.

---

**From:** Kerman, Sara J. (Fed)
**Sent:** Tuesday, November 1, 2016 2:46:39 PM

**To:** Moody, Dustin (Fed)
**Subject:** RE: PQC Comments that we will want to post
I can, I was worried about Microsoft and Atkins (because he did that syntax code looking text)

---

**From:** Moody, Dustin (Fed)
**Sent:** Tuesday, November 01, 2016 2:27 PM
**To:** Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
**Subject:** Re: PQC Comments that we will want to post
It looks good. Do you think we should make the text all the same font and font size? Some of the different submissions stand out a bit because of this.
Dustin

---

**From:** Kerman, Sara J. (Fed)
**Sent:** Tuesday, November 1, 2016 2:22:42 PM
**To:** Moody, Dustin (Fed)
**Subject:** RE: PQC Comments that we will want to post
How's this (it includes the Microsoft info too)? There are bookmarks on the side to jump to that particular comment.
Sara

---

**From:** Moody, Dustin (Fed)
**Sent:** Monday, October 31, 2016 12:49 PM
**To:** Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
**Subject:** RE: PQC Comments that we will want to post
Try this. I don't know what happened.

---

**From:** Kerman, Sara J. (Fed)
**Sent:** Monday, October 31, 2016 12:47 PM
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
**Subject:** RE: PQC Comments that we will want to post
These are both docx files (with the same filename). The first one (>400KB) I can't open. The second one (66KB), I could.

---

**From:** Moody, Dustin (Fed)
**Sent:** Monday, October 31, 2016 12:01 PM
**To:** Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
**Subject:** PQC Comments that we will want to post
Sara,

When we publish our 2nd FRN, and our final CFP, we also want to publish the comments received on our draft CFP, just like we did for our PQC NISTIR. I've attached the comments to this email, although they are not formatted. (I just copy/pasted). I also attached Microsoft's comments in pdf, because when I copy/pasted, much of the formatting was lost. Anyways, just wanted to get these to you, so you can get them ready. Let me know if you have any questions. Thanks!
Dustin