From: Regenscheid, Andrew
To: Moody, Dustin
Subject: Re: Final call for changes to NISTIR
Date: Friday, January 29, 2016 10:16:49 AM
Attachments: PQC NISTIR v3-arr.docx

Thanks, Dustin.

I identified a few relatively simple things in the attached document.

1) In section 4 you started indenting paragraphs, which isn't usually done in our documents.

2) On page 6 you referred to changes to "Suite B." If they didn't comment on this, then I have no problem with it. But, until yesterday it escaped me that they're not calling the new guidance "Suite B" anymore. Did they want to change it something else? Guidance on the use of public cryptographic algorithms for protecting national security systems?

3) This is on the sentence:
*While this process will have many commonalities with the processes that led to the standardization of AES [19] and SHA3 [20], this is not a competition with NIST as judge. (*On page 7)

For some reason I cringe every time I read/hear this. I was going to comment on this during your walkthrough yesterday, too. First, while we might informally say it, I don't think we usually formally refer to ourselves as "judges" in our crypto competitions. And in any event, I think what you describe about NIST's role is pretty much the same thing we do in competitions. I think I'd just drop the "judge" part of this sentence.

Thanks,
Andy

From: "Moody, Dustin"
Date: Friday, January 29, 2016 at 8:33 AM
To: Andrew Regenscheid
Subject: Fw: Final call for changes to NISTIR

Andy,
If you wish to make any comments on our PQC NISTIR - it is attached. On Monday, I'd like to give it to Jim Foti who will post it for 30 days of public comment (per Matt's instruction).

Dustin

From: Moody, Dustin
Sent: Thursday, January 28, 2016 3:43 PM

To: Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Perlner, Ray; Peralta, Rene; Chen, Lily; Liu, Yi-Kai; Jordan, Stephen P (stephen.jordan@nist.gov)
Subject: Final call for changes to NISTIR

Everyone,

I've tried to incorporate in the suggestions received. On Monday I'm going to send the NISTIR out to Jim Foti, who will prepare it for publication. Matt has suggested that we put it out for 30 days of public comments. So, any last comments need to be given before Monday. Thanks! I appreciate all the help and input from everyone.

Dustin

Reminder – next Tuesday we meet with Michael Groves and Wednesday is our crypto club talk. Please send me your slides by the end of the day tomorrow (Friday). Thanks!