From:	Liu, Yi-Kai (Fed)
To:	Peralta, Rene C. (Fed); Moody, Dustin (Fed); Chen, Lily (Fed); Perlner, Ray A. (Fed); Jordan, Stephen P (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)
Subject:	Re: "Shall" vs "must" in the PQC CFP
Date:	Friday, May 6, 2016 11:05:50 AM

Hi Dustin,

This is more of a stylistic issue, but I think it's not great to overuse "shall" and "must," because then people stop paying attention to them. I wonder if we can use "will" when talking about minor details, and only use "shall" and "must" when it's really important?

For instance, in the first sentence of a paragraph, use "shall": submitter SHALL include a complete description of the algorithms. But in the rest of the paragraph, use "will": this description WILL include a list of recommended parameter settings, etc.

Obviously this is a judgement call...

Other specific notes:

- On page 1, "Submission packages should be sent to:" -> SHALL

- On page 7, "a set of KAT vectors shall be included to exercise every table entry" -> maybe we want to relax this requirement? This requirement makes sense when we're talking about S-boxes, but may be tedious and unhelpful when it's a lookup table for sampling from a gaussian distribution.

- In general, I think we should leave the designers a fair amount of freedom in how they design the KAT tests, since it will probably vary a lot from one scheme to another. Maybe we can just have one strongly-worded sentence at the beginning: "Each scheme must be accompanied by a complete set of KATs that exercise all functionalities, all parameter settings and all sub-components of the scheme. Completeness of the KATs will be considered in evaluating the suitability of the scheme." After that, we give specific but non-binding advice using the word "should."

Obviously this is also a judgement call...

Cheers,

--Yi-Kai

From: Peralta, Rene (Fed)
Sent: Thursday, May 5, 2016 2:14 PM
To: Moody, Dustin (Fed); Chen, Lily (Fed); Perlner, Ray (Fed); Liu, Yi-Kai (Fed); Jordan, Stephen P (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)
Subject: Re: "Shall" vs "must" in the PQC CFP

Your judgment on this is fine with me. Don't we still need to run this by the lawyers? If so, we might as well let them tell us if any specific language should be used.

Regards, Rene.

From: Moody, Dustin (Fed)
Sent: Thursday, May 5, 2016 1:12 PM
To: Chen, Lily (Fed); Perlner, Ray (Fed); Liu, Yi-Kai (Fed); Jordan, Stephen P (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Peralta, Rene (Fed)
Subject: "Shall" vs "must" in the PQC CFP

Everyone,

A few of the comments we received back last week dealt with using the terms “shall” and “must”. I believe “shall” has a very strict meaning for our standards documents. To my mind, the word “must” means the same thing, but maybe isn’t quite as strong. In the attached (cleaned-up) version of the CFP, we have 60 uses of “shall” and 19 of “must”. Can everyone search through the document, using CONTROL+F, and see if any of the “shall”s or “must”s cause us any problems? Or if we should switch any of the “shall”s to “must”s, or even to “should”? I read through them all, and they seemed fine to me. Thanks,

Dustin