From:	Alperin-Sheriff, Jacob (Fed)
To:	(b) (6) ; Bassham, Lawrence E. (Fed); Chen, Lily (Fed); Jordan, Stephen P (Fed); Liu, Yi-Kai (Fed); Miller, Carl A. (Fed); Moody, Dustin (Fed); Peralta, Rene C. (Fed); Perlner, Ray A. (Fed); Smith-Tone, Daniel C. (Fed)
Subject:	Re:
Date:	Wednesday, November 30, 2016 11:53:58 AM

I believe the incoming administration will likely disapprove of any use of British spelling and grammar by a US government agency. Just a hunch.

From: (b) (6)

Date: Wednesday, November 30, 2016 at 11:36 AM

To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>, "Chen, Lily (Fed)" <lily.chen@nist.gov>, "Jordan, Stephen P (Fed)" <stephen.jordan@nist.gov>, "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>, "Miller, Carl A. (Fed)" <carl.miller@nist.gov>, "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, "Peralta, Rene (Fed)" <rene.peralta@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, "Smith-Tone, Daniel (Fed)" <daniel.smith@nist.gov>

Subject: Re:

Hello,

I've further edited the FAQs and have attached the revised document under the name "FAQ 2.4.1." The last period in the previous sentence was the full stop at the end of the sentence and is not actually part of the file name. As mentioned in the previous email, I believe that in the US we recognize the rule that punctuation falls within quotation marks, even though I agree that this practice is not good. Some of my edits are modifications of this nature. I list my edits:

In question 2, I made two punctuation changes, placing punctuation inside of quotation marks.

In questions 3 and 5, I edited the choice of punctuation "A:" to be consistent with the rest of the document.

In questions 1 and 2, I want to explicitly note that there is an odd indentation on the second line of the questions which is absent from the rest of the document. I didn't edit this bit, because I think that it is likely that the formatting will be different anyway online. When we finish our edits we might consider the possible appearance of the document when justified at various widths. I think that there could be some ugliness in the answer to question 10.

In question 5, I modified the language to reject the criticism of the Microsoft team that our process could be considered a competition or parallel competitions. I removed text that included punctuation outside of quotation marks.

In question 9, I changed the period at the end of the question to a question mark.

In question 10, I changed the wording of the question slightly to respect Dustin's suggestion that the wording is too suggestive of permanence. The question I removed had no punctuation.

Also in question 10, I added a paragraph discouraging the belief that the proposed security levels are inescapable, alleviating the fear that future changes to post-quantum security metrics may penalize submitters, and emphasizing the necessity of establishing the categorization. This edit should be a particular point of focus in your review of my suggestions.

Next in question 10, I added the word "however," to indicate that it is with clear knowledge of the context of our choices for security categories that we make the statement of confidence in their specification.

Still is question 10, I changed the phrase "clearly overkill" to "likely excessive." I agree with Dustin that using the phrase "clearly overkill" is akin to saying, "just to waste your time."

In question 12, I removed the capitalization on the word "for" in Call for Proposals. The word "for" shouldn't be capitalized in a title even if used in an abbreviation.

Thanks, and let's get this done!

Cheers,
Daniel

On Wed, Nov 30, 2016 at 7:40 AM, (b) (6) [redacted] wrote:

> There are still some punctuation and grammar mistakes in the FAQ. I'll correct it when I get to a PC.
>
> There is also a statement that, if I recall properly, is incorrect in the document. Regarding the NISTIR, I don't recall it mentioning that a competition must necessarily have a single winner. Even if I am wrong and it did mention that there is a single winner, Microsoft complained that having multiple winners is not sufficient cause to abandon the competition structure. I will suggest a minor edit of the wording which I will then submit for your review.
>
> Additionally, I have my own question. Are we using American grammatical practices or British? My grammar is not the pinnacle of human achievement, but I thought that in the US that the convention is to place punctuation inside of quotation marks even when it makes absolutely no sense to do so. So, for example, we might in the US write:
> Did you say, "My name is Joe?"
> This, of course, makes no sense. Is this not the standard, however, in the US? In the UK they may write something like:
> Did you say, "My name is Joe."?
> This is also a bit offensive.
>
> The short point is that, unless I'm wrong, in US practice we place periods inside quotes. So option (1) below is the standard, I think.
> (1) She called the ride "bumpy."
> (2) She called the ride "bumpy".
> (I like option (2) better, though.) (I'm glad we don't have issues like this with parentheses.)...)

What do you "think?"

Cheers,
Daniel

On Tue, Nov 29, 2016 at 2:52 PM Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:

> I made some comments/revisions on Ray's FAQ's.
>
> ---
>
> **From:** Perlner, Ray (Fed)
> **Sent:** Tuesday, November 29, 2016 1:43 PM
> **To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>; Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Daniel Smith-Tone <daniel-c.smith@louisville.edu>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Miller, Carl A. (Fed) <carl.miller@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>; Smith-Tone, Daniel (Fed) <daniel.smith@nist.gov>
> **Subject:**
>
> Provided answers for:
>
> Q: What will happen to a submitted algorithm if some or all of the provided parameters fail to meet their claimed security strength categories.
>
> And
> Q: For which security strength categories does NIST plan to standardize parameters