From: Foti, James (Fed)
To: Kerman, Sara J. (Fed)
Subject: RE: A new PQC FAQ
Date: Friday, October 20, 2017 3:46:10 PM

It's not ideal, but I went to https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/faqs and right-clicked on the page, then selected View Page Source.

I'm also trying to research Bootstrap Collapse online help to see if there's anything else we can hardwire into the linking <a> tag to tell the panel to expand.

From: Kerman, Sara J. (Fed)
Sent: Friday, October 20, 2017 3:14 PM
To: Foti, James (Fed) <james.foti@nist.gov>
Subject: RE: A new PQC FAQ

Thanks. I'll try it. I will have to do all of that within the answer field though, right? Because I can't go to source in the "Question" section.

How do you know all this??

From: Foti, James (Fed)
Sent: Friday, October 20, 2017 3:10 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: RE: A new PQC FAQ

I've never used that feature before, but it looks like I was just using the wrong id. Here's the code around the your Q19 item:

```
  <div class="panel panel-default">
    <div class="panel-heading" id="heading_87" role="tab">
      <div class="panel-title">
        <strong>
        <a aria-controls="collapse_87"
          aria-expanded="false"
          class=""
          data-parent="#collapse1489775128774"
          data-target="#collapse_87"
          data-toggle="collapse"
          href="javascript:void(0)">
          019.  What advice does NIST have for submitters to ensure their submissions will be
complete and proper?
        </a>
```

```
        </strong>
      </div>
    </div>

    <div aria-labelledby="heading_87"
      class="panel-collapse collapse"
      id="collapse_87"
      role="tabpanel"
      aria-expanded="false">
      <div class="panel-body">
        <p><p><a id="Q19"></a>NIST has completed the reviews for all the submissions received by the preliminary deadline, and has sent back comments to each submission team.&amp;nbsp; We note the reviews were to check if submissions were “complete and proper”, meeting both our submission requirements and minimal acceptance criteria.&amp;nbsp; They were NOT a r…
```

So, your code would look like:
Go to Question 19

Jim

From: Kerman, Sara J. (Fed)
Sent: Friday, October 20, 2017 2:43 PM
To: Foti, James (Fed) <james.foti@nist.gov>
Subject: FW: A new PQC FAQ

Help – I don’t know enough about the div tags. Where do I put “panel-heading”

So at Q19 would my link be <a id=”heading_Q19”>

And then where the user would click to go Go to Question 19

From: Nickel, Christian G. (Assoc)
Sent: Friday, October 20, 2017 2:25 PM
To: Foti, James (Fed) <james.foti@nist.gov>; Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: RE: A new PQC FAQ

Woops, I didn’t see the 2nd part of that, sorry there isn’t a way to expand it currently. That is a feature we could add in the future though.

From: Nickel, Christian G. (Assoc)
Sent: Friday, October 20, 2017 2:24 PM

To: Foti, James (Fed) <james.foti@nist.gov>; Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: RE: A new PQC FAQ

Yes, you can use the ID of the with the "panel-heading" class, like so: text

---

From: Foti, James (Fed)
Sent: Friday, October 20, 2017 2:13 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>; Nickel, Christian G. (Assoc) <christian.nickel@nist.gov>
Subject: RE: A new PQC FAQ

Good question, Sara. I tried going to the id=`collapse_54`
By using https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/faqs#collapse_54, but it didn't work.

Christian—is there a way to modify a URL so that it goes to a specific anchor on the FAQ page *and* expand the particular FAQ? If not, this is something we should look into.

Jim

From: Kerman, Sara J. (Fed)
Sent: Friday, October 20, 2017 12:44 PM
To: Foti, James (Fed) <james.foti@nist.gov>
Subject: FW: A new PQC FAQ

Question regarding FAQs – can I do a direct link from https://csrc.nist.gov/Projects/Post-Quantum-Cryptography to a specific FAQ within the project – by using the ID and NAME tag? Like an anchor type link? Or is there some other way (I remember this being an issue with bootstraps).

From: Moody, Dustin (Fed)
Sent: Friday, October 20, 2017 12:28 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: A new PQC FAQ

Sara,

We completed the check for "complete and proper" submissions for all the submitters who submitted early. Based on what we learned, we created some advice to submitters for the final deadline. We posted it on the pqc-forum, but it would probably be nice to have on our webpage as well. Looking, it seemed to make the most sense to put it as a new FAQ. So I put it below.

Maybe on the project home page, somewhere in the Project Overview text we could put a plug for it. Something like a linked "Advice for Submitters". Although I think the link would only go to the

FAQ and not the specific question. So maybe we could add “see Question 19” or something to that effect. Does that seem reasonable?

Dustin

Q. What advice does NIST have for submitters to ensure their submissions will be complete and proper?

A. NIST has completed the reviews for all the submissions received by the preliminary deadline, and has sent back comments to each submission team. We note the reviews were to check if submissions were “complete and proper”, meeting both our submission requirements and minimal acceptance criteria. They were NOT a review on the technical merits. Submissions which had elements missing will need to revise their submissions, and re-submit by the final deadline of November 30, 2017.

After going through this process, we have some suggestions we think will help submitters to make their submissions complete and proper, as well as help NIST with a more efficient review process following the final deadline.

- Clearly provide ALL of the information on the cover sheet which is asked for in our Call for Proposals (CFP) section 2.A.
- Please clearly and explicitly state which of our five security strength categories your proposed parameter sets meet. See CFP 2.B.4 and 4.A.5.
- Some submissions can be submitted as either a KEM or a public-key encryption scheme, or both. Please clearly indicate which functionality (or functionalities) you want NIST to consider, and include the appropriate required algorithms. See CFP 2.B.1.
- We are interested in qualitative statements about the possible tradeoffs between security and efficiency. That is, besides stating which of the five security strength categories are met, we would like submitters to describe what kind of flexibility there is when adjusting the parameters in their cryptosystem. See CFP 2.B.1.

With regards to the implementations and KATs:

- Please make sure your implementation is platform-independent. See NIST FAQ #3, at https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/faqs
- Please follow our guidance on following the NIST API and generating KATs as posted on our webpage: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization/Example-Files
- In addition to the requirement that the README file “shall be a plain text file and list all files that are included on the disc with a brief description of each”, it would be useful if the file also contains some basic information about what is being provided. This includes things like how to compile the code, what is produced by the Makefile, and any information necessary to run

the files created by the Makefile. On the subject of Makefiles, it would be very useful to have the genKAT and rng files included in the submissions as a concrete example of how to compile the algorithm source code. This will also help facilitate checking of the packages for completeness.

Thank you, and let us know if you have any questions. Specific questions on a submission should be sent to us at pqc-comments@nist.gov. General questions may be posted on the forum, or sent to us the email address just given.