From: Kerman, Sara J. (Fed)
To: Moody, Dustin (Fed)
Subject: RE: PQC webpage
Date: Thursday, April 14, 2016 3:17:53 PM

No, that would be the link and it would take you direct to: http://csrc.nist.gov/groups/ST/post-quantum-crypto/ Or do you want another page that builds of the "Standardization" only? I have a request in for an alias, that relates the project that would go through 2023-ish. That's the one we will get an alias to.

On that page, we would add more menu links, to whatever is necessary (Federal Register Notices, Submission Requirements, etc.). Here is a link to the Wayback machine to the hash competition stuff in 2008:
http://web.archive.org/web/20080307094319/http://www.csrc.nist.gov/groups/ST/hash/sha-3/index.html
We can talk next week when we are both here.

From: Moody, Dustin (Fed)
Sent: Thursday, April 14, 2016 3:06 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: Re: PQC webpage

I hope you get it fixed soon. By the way - I really like your suggestion to just use the same link throughout the document. That makes a lot of sense. Do you know what the link will be? (I know if we get nist.gov/pqcrypto we can use that one, but what will the other one be?)

From: Kerman, Sara J. (Fed)
Sent: Thursday, April 14, 2016 2:59:59 PM
To: Moody, Dustin (Fed)
Subject: RE: PQC webpage

Cool – hope they approve. Hopefully I'll have my web-editing software back soon. Got a new computer and it didn't transfer! ☹

From: Moody, Dustin (Fed)
Sent: Thursday, April 14, 2016 2:56 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: Re: PQC webpage

Yes, pqcrypto

From: Kerman, Sara J. (Fed)
Sent: Thursday, April 14, 2016 2:55:20 PM
To: Moody, Dustin (Fed)
Subject: RE: PQC webpage

But we are still going for www.nist.gov/pqcrypto? Or something else? pqcrypto is the request I submitted.

From: Moody, Dustin (Fed)
Sent: Thursday, April 14, 2016 2:54 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: Re: PQC webpage

I think it doesn't hurt to try to get the alias. If we don't get it - no big deal. Thanks!

Dustin

From: Kerman, Sara J. (Fed)
Sent: Thursday, April 14, 2016 2:51:33 PM
To: Moody, Dustin (Fed)
Subject: RE: PQC webpage

Dustin,

We will definitely have that, but even in the SHA-3 FRN, all the URLS were the same, www.nist.gov/hash-competition and it pointed to the main "competition" landing page (http://csrc.nist.gov/groups/ST/hash/sha-3/index.html). I will add a menu item "Submission Requirements", but I think it's safer to use the same URL throughout the FRN. (The hash pages look totally different now because we've updated the menu to condense and reflect the finalization of the competition).

If we want to change the alias (if approved), I need to know ASAP. iTAC is running it up the chain of command for approval as of yesterday. My AWS day is tomorrow so I will not be working.

Keep me posted.

Sara

From: Moody, Dustin (Fed)
Sent: Thursday, April 14, 2016 2:21 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: Re: PQC webpage

Sara,

So in looking through our document, I think what we'll want is something very much like what SHA-3 had:

csrc.nist.gov/groups/ST/hash/sha-3/Submission_Reqs/index.html

We just adapt that page to match our document sections. I'll get Larry working on creating a few of the documents that we'll need to post there. Much of the links will simply link to text taken directly from our Call For Proposals.

I don't know the best name we should use. The SHA-3 Competition was a good name, but we are trying to avoid using the word 'competition' in our titles for this thing. So far we've been calling it things like quantum-resistant algorithm evaluation process. Or just PQC standardization.

Still no rush on this yet - we're not releasing it to the public probably until May/June. Thanks,
Dustin

From: Kerman, Sara J. (Fed)
Sent: Monday, April 11, 2016 3:46:41 PM
To: Moody, Dustin (Fed)
Subject: RE: PQC webpage

Hey Dustin,

Yes, we can just continue to build within the /post-quantum-crypto/ directory. For a time, NIST stopped creating URL aliases (www.nist.gov/xxxx). I talked to our information coordinator and she said to submit a ticket to iTAC because they are doing them on a case-by-case basis now. IF, they will allow an alias that points to http://csrc.nist.gov/groups/ST/post-quantum-crypto/ what do you think

it should be. For SHA-3, it was nist.gov/hash-competition.
www.nist.gov/quantum-crypto
www.nist.gov/pqcrypto
Other thoughts?
If Itac says they will no longer do this, I can get a tiny url from go.usa.gov, but they auto select the URL. For Lily's December meeting (SSR2016) the tiny url is http://go.usa.gov/cpage No rhyme or reason, but at least it's smaller.
Sara

From: Moody, Dustin (Fed)
Sent: Thursday, April 07, 2016 3:06 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: PQC webpage

Sara,
We're actively working on finishing our PQC Call for Proposals document (see attached). It's very similar to the call that went out before the SHA-3 competition. Throughout the document, we make reference to several webpages that we currently don't have ready. We hope to send this out for public comment in June, so it would be good to have them ready before then.
I think we want all of them to reside at the page you already created:
In the next week or so, I'll try and figure out exactly which pages we need and what needs to go on them. Just wanted to give you a heads up on all this – since I assume you'll be the one making the webpages? Thanks!!
Dustin