From: Moody, Dustin (Fed)
To: Kerman, Sara J. (Fed)
Cc: Chen, Lily (Fed); Foti, James (Fed)
Subject: RE: PQC forum
Date: Monday, February 29, 2016 11:37:44 AM
Attachments: PQCrypto 2016 v3.pptx

Sara,

Thanks. As for the webpage, I agree we can incorporate the research-project info into the new page. There's no rush on creating the webpage, as we are only at the beginning stage. As for what should be on it, We can have a link to our previous workshop. We have NISTIR 8105 that's out for public comment right now. We can have a link to the pqc-forum archives (and instructions how to subscribe). I gave a presentation at PQCrypto that is basically our announcement and outline of our Call for Submissions that we will be doing later this year. So we could put those slides (attached), or take information off of them and include it. We can have our email (pqc-comments@nist.gov) for contact. We will host a workshop in 2018, but we don't have all the details for that yet.

Dustin

From: Kerman, Sara J. (Fed)
Sent: Monday, February 29, 2016 11:29 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>; Foti, James (Fed) <james.foti@nist.gov>
Subject: RE: PQC forum

Hey Dustin,

Yes, I can send an email out to last years attendees. Not a problem—I'll send it out today.

I can do the page too (I'm looping Jim Foti in for information). There is currently a "Post-Quantum Cryptography" informational blurb at: http://csrc.nist.gov/groups/ST/crypto-research-projects/#PQC. I'm assuming you want a page dedicated to PQC and upcoming work/events, in which case, I believe we should remove the information found at the link I provided and incorporate it into the new site. We should discuss what information you anticipate including on the site (workshops, documents, etc.).

Sara

From: Moody, Dustin (Fed)
Sent: Monday, February 29, 2016 11:12 AM
To: Kerman, Sara J. (Fed)
Cc: Chen, Lily (Fed)
Subject: PQC forum

Sara,

Two things for you related to PQC.

- First, I set up a pqc-forum mailing list, and announced that at the PQCrypto Workshop last week. Unfortunately, I didn't learn from my experience with the ecc-forum, and didn't correctly tell people outside of NIST how to subscribe. Can we send an email to all the participants of our PQC workshop and let them know about the forum and how to subscribe? I'll contact the PQCrypto workshop people and see if I can get them to do the same. The instructions we need to give are below.
- Second, we should probably have a web page that will be devoted to the PQCrypto project, since we will be doing something somewhat akin to the SHA-3 contest (albeit on a slightly smaller scale). Who do I work with to get one created?

Thanks,
Dustin

PQC Workshop Attendees,

NIST has set up an pqc-forum@nist.gov mail listserve. You must be subscribed to send email to the listserve. For those outside of NIST, please use the instructions below to subscribe.

> To join:
> mailto:pqc-forum-request@nist.gov?subject=subscribe
> You will receive a response message from pqc-forum-request@nist.gov. Please reply to that message to confirm your subscription request.
> To unsubscribe:
> mailto:pqc-forum-request@nist.gov?subject=unsubscribe

The pqc-forum@nist.gov will be used to discuss the standardization and adoption of secure, interoperable and efficient post-quantum algorithms. In particular, the listserve will facilitate discussions about our upcoming Call for Submissions (see http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf and https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf). The messages from the mailing list will be archived online, and available to everyone at: https://email.nist.gov/pipermail/pqc-forum/.