From:	Boutin, Chad T. (Fed)
To:	Foti, James (Fed); Moody, Dustin (Fed); Kerman, Sara J. (Fed)
Subject:	RE: announcement details
Date:	Tuesday, January 29, 2019 11:03:43 AM
Attachments:	2nd round announcement.docx

Thanks Jim – always glad to have this awareness.

FYI I have admin approval (from Chuck on down) for our own NIST Tech Beat story, so I plan to have it ready this afternoon (might be pushing it) or tomorrow morning (more realistic).

Also, Dustin sent me the text he plans to send out on the mailing list (attached). As he mentioned a moment ago in a separate post:

Will the text go up on a new/unique webpage, or will it merely get added to an existing page? If the former, what is the (not-yet-live) URL you will be using? If the latter, can you direct me to the existing page where it will appear?

Chad

From: Foti, James (Fed)
Sent: Tuesday, January 29, 2019 10:00 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Cc: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Subject: RE: announcement details

OK, thanks—although I'll still need to get confirmation from Matt, just to triple-check that he's given Jim Olthoff a heads-up.

Also, let's please include Chad Boutin on this thread with us, instead of just a separate thread, so that we're all singing from the same sheet of music regarding the timing of the release.

Thanks,
Jim

From: Moody, Dustin (Fed)
Sent: Tuesday, January 29, 2019 9:55 AM
To: Foti, James (Fed) <james.foti@nist.gov>; Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: RE: announcement details

FYI, Lily and Matt tell me that likely this afternoon we'll be good to go on our announcement this afternoon.

Dustin

From: Foti, James (Fed)
Sent: Monday, January 28, 2019 3:00 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: RE: announcement details

Thanks, Dustin.

Having reviewed the text, it's not a good idea to include the DOI in this announcement, since it will not be active. People will click on it, regardless, and will contact the Library, you, may, and anyone they can, if it's not working.

Instead, I would suggest that you point to https://csrc.nist.gov/publications and indicate that when NISTIR 240 is published, it will be posted at that location. I would suggest changing it as follows:

From:
To better explain our decision process and rationale for our selection, we have released a short report which will soon be available at:

https://doi.org/10.6028/NIST.IR.8240

and on our webpage www.nist.gov/pqcrypto.

To:
To better explain our decision process and rationale for our selection, we are finalizing a short report, NIST Internal Report (NISTIR) 8240. It will soon be available at https://csrc.nist.gov/publications and on our PQCrypto webpage https://www.nist.gov/pqcrypto.

Please also make sure that Chad's article does not include that DOI, either.

If you want to make some changes, I'll then forward the updated document to Matt. He'll turn it around quickly.

Jim

From: Moody, Dustin (Fed)
Sent: Monday, January 28, 2019 2:58 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>; Foti, James (Fed) <james.foti@nist.gov>
Subject: RE: announcement details

Got it. You're correct – I was mistaken. Thanks!

From: Kerman, Sara J. (Fed)
Sent: Monday, January 28, 2019 2:56 PM

To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Foti, James (Fed) <james.foti@nist.gov>
Subject: RE: announcement details

But you also asked, in the email, that they be posted to "www.nist.gov/pqcrypto page as well, as soon as we can after the announcement". The announcement makes sense as being a "news" worthy item (as far as CSRC layout is concerned).

Sara

From: Moody, Dustin (Fed)
Sent: Monday, January 28, 2019 2:52 PM
To: Foti, James (Fed) <james.foti@nist.gov>; Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: RE: announcement details

I don't know if he has seen that exact version. It was intended just to be a message on our pqc-forum mailing list. But you can certainly post it as a news item.

Fine with me if Matt ok's it (assuming that doesn't add on any time).

Dustin

(latest version attached)

From: Foti, James (Fed)
Sent: Monday, January 28, 2019 2:49 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: RE: announcement details

Dustin-
As far as the announcement that you just sent to us, which we'll be posting as a news item, has Matt seen that exact version? If not, I'll just need for him to review and confirm that it's ok.
Thanks,
Jim

From: Moody, Dustin (Fed)
Sent: Monday, January 28, 2019 2:27 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Cc: Foti, James (Fed) <james.foti@nist.gov>
Subject: RE: announcement details

Thanks, Sara.

Lily says we need to wait for Matt's meeting with Chuck tomorrow. She thinks probably tomorrow afternoon, or Wednesday the latest.

As far as the news item bit – yeah, I've been in contact with Chad Boutin before the shutdown. He'd sent me a draft of an article they would publish at the time of our announcement. I'm just now sending him back comments on it.

From: Kerman, Sara J. (Fed)
Sent: Monday, January 28, 2019 2:23 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: Foti, James (Fed) <james.foti@nist.gov>
Subject: RE: announcement details

Hey Dustin,
Getting the information onto the website should not be an issue. What time do you plan to send the announcement of the Round 2 PQC candidates to the listserv? This afternoon? Or tomorrow? As far as posting the report, it is still in the WERB process – only ones left to "approve" are Donna and ITL and then it will go to WERB.

I'm cc'ing Jim Foti - for information - since the 2nd round announcement.doc will be a news item also.
Jim – I can put this together, I just wanted you aware because I know there was concern over news items being quickly posted before vetting prior to the shutdown. I know Dustin has worked closely with the PQC team, Lily and Matt it preparing all the announcement details.

Sara

From: Moody, Dustin (Fed)
Sent: Monday, January 28, 2019 2:03 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: announcement details

Sara,
Okay we met today. We are okay to announce the 26 submission teams moving on to the next round, without the Report being done quite yet. Lily wants us to wait a little bit so that Matt can meet with Chuck. That is happening tomorrow morning apparently, and she hopes we can post later tomorrow.

To announce, I'll send a message to the forum. The message I'll send is in the "2nd round announcement.doc" attached. In it, I also reference the Call for the 2nd NIST PQC workshop and Guidelines for submitting tweaks. I'll send those to the forum also. We should probably post them on our www.nist.gov/pqcrypto page as well, as soon as we can after the announcement. Is that doable? If it takes a little while, I don't see that as a problem, as the main thing for everybody to know right now is which submissions are moving on. We're already going to wait and publish the report later anyway.

Does this all seem okay? Thanks,

Dustin

(I've attached the latest version of the Report, but it isn't final. Andy just sent me some minor changes to make.)