Thanks Patrick, Sara. The text looks good now.

From: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Sent: Tuesday, May 10, 2022 4:50 PM
To: O'Reilly, Patrick D. (Fed) <patrick.oreilly@nist.gov>; Moody, Dustin (Fed)
<dustin.moody@nist.gov>; Foti, James (Fed) <james.foti@nist.gov>
Subject: RE: PQC Announcement - Date Updates

Thanks Patrick. Yes, I just looked to see how it was set up and if those dates were indeed included. I
didn't want to change information unless I received the ok from you.

I think it all looks good now. We still do NOT have the green light to post. Dustin will let us know.

Thank you everyone,
Sara

From: O'Reilly, Patrick D. (Fed) <patrick.oreilly@nist.gov>
Sent: Tuesday, May 10, 2022 4:40 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Foti, James (Fed) <james.foti@nist.gov>
Cc: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: RE: PQC Announcement - Date Updates

Dustin –
Sorry about that – I thought that Sara changed the dates for she checked out the news item earlier
before I did so I initially thought she took care of updating the dates. I think she only looked to see
how the news item was set up.

Yes, you're right the "old" dates were still there – I made the changes to capture the new/updated
dates.
SO take a look at this PREVIEW URL/page:
https://cms.csrc.nist.gov/preview/news/2022/pqc-candidates-to-be-standardized-and-round-4

Again, need to look at the page behind the NIST VPN.
Let me know if anything else needs to be done.
Thanks.
Pat

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Tuesday, May 10, 2022 3:46 PM

To: O'Reilly, Patrick D. (Fed) <patrick.oreilly@nist.gov>; Foti, James (Fed) <james.foti@nist.gov>
Subject: Re: PQC Announcement - Date Updates

Patrick,

When I click the link, there are still the dates that need to be changed.

"For the algorithms moving on to the fourth round, NIST will allow the submission teams to provide updated specifications and implementations ("tweaks"). The deadline for these tweaks will be July 1, 2022."

should say September 1, 2022.

NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by June 2022

Should say summer 2022, instead of July 2022. Also

Submissions in response to that call will be due by January 1, 2023

Should say March 1, 2023

From: O'Reilly, Patrick D. (Fed) <patrick.oreilly@nist.gov>
Sent: Tuesday, May 10, 2022 3:36 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Foti, James (Fed) <james.foti@nist.gov>
Subject: RE: PQC Announcement - Date Updates

Sara,
I was getting ready to make the update to the News item on CSRC but saw you went into the news item and I guess you made the tweaks to the dates.

Anyway, here is the PREVIEW link which can only be seen when you're logged into the NIST VPN.
https://cms.csrc.nist.gov/preview/news/2022/pqc-candidates-to-be-standardized-and-round-4

I guess let me know if anything needs tweaking, etc.

Thanks.
Pat

From: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Sent: Tuesday, May 10, 2022 3:07 PM
To: O'Reilly, Patrick D. (Fed) <patrick.oreilly@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Foti, James (Fed) <james.foti@nist.gov>
Subject: RE: PQC Announcement - Date Updates

Pat,

I think you are correct. It's coming back to me. Jim requested that the GovDelivery notice be short and sweet with a pointer to the **Full Announcement** (which I think is the News Item).

Nothing needs to be done with the GovDelivery notice based on the draft you sent at 2:23.   We are not announcing anything yet.

I think the only thing that needs to be updated is the News Item with the three new dates. I can update those if you'd like. I think I have access to the CSRC record.

Deadline for tweaks: NEW DATE: September 1, 2022   OLD DATE: July 1, 2022
Call for Proposals: NEW DATE: Summer 2022   OLD DATE: June 2022
Submissions Due: NEW DATE: March 1, 2023   OLD DATE: January 1, 2023

Dustin – feel free to jump in. (he is on travel)
Sara

From: O'Reilly, Patrick D. (Fed) <patrick.oreilly@nist.gov>
Sent: Tuesday, May 10, 2022 2:23 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Foti, James (Fed) <james.foti@nist.gov>; Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: RE: PQC Announcement - Date Updates

Dustin and Sara –
Hi – I went into the saved draft GovDelivery notice for the PQC one I created for you about 3 weeks ago.
I opened up the Word file that Jim forwarded to me and noticed that it is a lot different from the original GovDelivery notice I created several weeks ago. In the bottom of the email it asked to update 3-4 dates, but when I looked at the GovDelivery notice I created for you several weeks ago – there are no dates inlcued in the original email notice.

To help cut down the extra time on this –
1. After you read this email, I am sending you both a TEST message of the notice I did for you several weeks ago and you can compare it with the Word file that was attached in Jim's email earlier today.
2. Once you compare the 2 write-ups – what exactly would you like done in terms of updating the DovDelivery notice?

Is the Word file supposed to be used instead of the original notice I put together several weeks ago? The content in the Word file is twice as long as the original notice I created. If my hunch is correct – Here is some guidance that I will toss at you to consider –

If you want to use all the content in the Word file – I strongly suggest shortening it to about 2-3 paragraphs AND then I can create/update the CSRC News item to include ALL the text in the Word file.
If you/we use all that content in the GovDelivery email notice, our subscribers will not want to read such a long notice – save it for the webpage (long content).

Let me know – I haven't updated anything yet.
Just wanted to run my thoughts and suggestion to you.

I think having a short GovDelivery email notice will go a long way and then I/we can provide a link to the longer announcement either on the CSRC News page and/or maybe a PQC project news page could be created?

Thanks & I will do what ever you want me to do.
Pat

From: Foti, James (Fed)
Sent: Tuesday, May 10, 2022 9:26 AM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Cc: Moody, Dustin (Fed) <dustin.moody@nist.gov>; O'Reilly, Patrick D. (patrick.oreilly@nist.gov) <patrick.oreilly@nist.gov>
Subject: RE: PQC Announcement - Date Updates

Thanks, Sara.

Pat, can you please take a look at the Post-Quantum Crypto GovDelivery and News item you prepared several weeks ago, make the changes below, and then send us the updated Test message (and send a Preview link to the News item)?

Jim

From: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Sent: Tuesday, May 10, 2022 9:06 AM
To: Foti, James (Fed) <james.foti@nist.gov>
Cc: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: PQC Announcement - Date Updates

Hey Jim,
In the PQC announcement, there are a couple of dates that should be changed based on the delay in making the announcement. I think these dates are included in the News Item and the GovDelivery email.

Deadline for tweaks: NEW DATE: September 1, 2022   OLD DATE: July 1, 2022
Call for Proposals: NEW DATE: Summer 2022   OLD DATE: June 2022
Submissions Due: NEW DATE: March 1, 2023   OLD DATE: January 1, 2023

Thank you,
Sara