From:	Chen, Lily (Fed)
To:	Sonmez Turan, Meltem (Fed); Dworkin, Morris J. (Fed)
Subject:	RE: Informing the authors
Date:	Friday, August 6, 2021 3:17:31 PM

That will be great. If it is okay, I can be at one of the meetings so that you do not have to schedule a specific one.

Lily

From: Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>
Sent: Friday, August 6, 2021 3:08 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Subject: RE: Informing the authors

Lily,

Maybe the review board can organize a short meeting to update you and the team about our internal review process. It might be good to get feedback, we are also learning as we do the reviews.

Thanks,
Meltem

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Friday, August 6, 2021 2:48 PM
To: Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Subject: RE: Informing the authors

Thank you Meltem and Morrie,

You already considered this. Very good. Quynh actually got me confused. It sounds like he heard it the first time. Sorry that I misunderstood the situation.

Lily

From: Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>
Sent: Friday, August 6, 2021 2:45 PM
To: Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Informing the authors

Hi Lily,

I am forwarding the email to Quynh (see highlighted part), where we informed him about the upcoming review.

Thanks,
Meltem

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Thursday, May 20, 2021 12:43 PM
To: Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>
Cc: cryptopubreviewboard <cryptopubreviewboard@nist.gov>
Subject: Re: Review process for FIPS 198-1 and SP 800-107

Hi Meltem,

I have checked my records.

I have not received any comments for FIPS 198-1. It is just the spec of HMAC.

The comments I have received for SP 800-107-Rev1 are attached. The commentors just wanted to know where the 2C came from when talking about HMAC key and its equivalent.

Since then (2013) I have not received any comments.

Quynh.

From: Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>
Sent: Monday, May 17, 2021 3:23 PM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Cc: cryptopubreviewboard <cryptopubreviewboard@nist.gov>
Subject: Review process for FIPS 198-1 and SP 800-107

Dear Quynh,

The crypto publication review board is planning to initiate the periodic review process for the following standards that you have authored:

- FIPS 198-1 *The Keyed-Hash Message Authentication Code (HMAC)* and
- SP 800-107 *Recommendation for Applications Using Approved Hash Algorithms*

To support the review process, we would like to get a copy of the public feedback that you received on the standard after the comment period ended, if any. Are there any other known issues with the standards that would help the review?

We appreciate if you can send your feedback, by May 31, 2021.

Thanks,
Meltem, on behalf of the Crypto Publication Review Board

From: Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Sent: Friday, August 6, 2021 2:33 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>
Subject: Re: PQC Slides

Thanks, Lily,

Communicating with the authors is on our checklist to do, but it might not have been clear to Quynh that our process now includes initial public comments as well as comments on any decision proposal.

I think Elaine has taken the lead on previous revisions to the HMAC FIPS.

Have a nice weekend,

Morrie

From: "Chen, Lily (Fed)" <lily.chen@nist.gov>
Date: Friday, August 6, 2021 at 2:27 PM
To: "Sonmez Turan, Meltem (Fed)" <meltem.turan@nist.gov>, "Dworkin, Morris J. (Fed)" <morris.dworkin@nist.gov>
Subject: RE: PQC Slides

Hi, Morrie and Meltem,

When we start to open a standard for review, it might be helpful to first talk with the authors, if they are still with NIST or still reachable. Sometimes the authors may have received some questions and comments directly after the standard was published. I should have raised this from very beginning. Sorry that I did not. Who are the editor of HMAC?

Lily

From: Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>
Sent: Friday, August 6, 2021 11:33 AM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>; cryptopubreviewboard <cryptopubreviewboard@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: RE: PQC Slides

Thanks Quynh for your insights on SP 800-107. I am sharing your comments with the review board (CCed). We can discuss more about the next steps later. I will keep you in the loop.

Lily – FYI, the review board announced the new set of documents for review: FIPS 198-1 (HMAC), SP 800-22, SP 800-38D, SP 800-38E and SP 800-107. Comments are due October 1. More info: https://csrc.nist.gov/Projects/crypto-publication-review-project

Best,
Meltem

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Friday, August 6, 2021 10:05 AM
To: Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Cc: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>; Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>
Subject: Re: PQC Slides

Hi all,

I did not know SP 800-107 has been under a public comment period.

My assessment was that the pub was very useful at the time when we constantly received comments/questions about security properties of our hash functions. The pub was used to provide some needed educational information at the time.

I would not be surprised if many people look at it now and say that it should include this and that etc...

Now, security properties/requirements with our approved hash functions are fully specified in other SPs and FIPSs. I think the pub does not have much value anymore.

Regards,
Quynh.

From: Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>
Sent: Thursday, August 5, 2021 2:57 PM
To: internal-pqc <internal-pqc@nist.gov>
Cc: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>; Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>
Subject: PQC Slides

Hi,

I edited the slides a bit further to make the dashed pattern match along the entire length of the branched timeline. It was a manual edit because I don't know how to do something like this

automatically, yet. If you want to change something and it affects the dashed pattern, please let me know and I can manually fix it again.

Also, please check that there is nothing contentious in the listed dates. Thanks!

Cheers,
Daniel ST