From:	Regenscheid, Andrew (Fed)
To:	Moody, Dustin (Fed)
Subject:	Re: Post-Quantum Cryptography Requirements and Evaluation Criteria FRN Publication Date: 08-02-2016
Date:	Thursday, July 28, 2016 9:47:44 AM

OK. That's what I'll tell them if they call me.

-Andy

From: Moody, Dustin (Fed)
Sent: Thursday, July 28, 2016 9:36 AM
To: Regenscheid, Andrew (Fed)
Subject: Re: Post-Quantum Cryptography Requirements and Evaluation Criteria FRN Publication Date: 08-02-2016

I haven't talked to PBA, and I don't think Lily has either. We can wait until we have a final version.

From: Regenscheid, Andrew (Fed)
Sent: Thursday, July 28, 2016 9:28:40 AM
To: Moody, Dustin (Fed)
Subject: Re: Post-Quantum Cryptography Requirements and Evaluation Criteria FRN Publication Date: 08-02-2016

Great.

After seeing Gail and Jennifer on the distribution list, it occurs to me- did you or Lily talk to PBA about this? They usually want to do their own press release.

I'm not sure it makes sense. They did one for the PQC whitepaper, I think, and we'll certainly have them do one for the final call, but I don't see much value in doing it for this one.

-Andy

From: Moody, Dustin (Fed)
Sent: Thursday, July 28, 2016 9:12 AM
To: Regenscheid, Andrew (Fed)
Subject: Re: Post-Quantum Cryptography Requirements and Evaluation Criteria FRN Publication Date: 08-02-2016

I checked with Sara (who checked with Matt). We'll post the docs on our website on Monday, and the 45 day countdown will start on the official publication date of Tuesday. That puts the

comment period ending Fri, Sep. 16th.

From: Regenscheid, Andrew (Fed)
Sent: Thursday, July 28, 2016 9:09:22 AM
To: Moody, Dustin (Fed)
Subject: Fw: Post-Quantum Cryptography Requirements and Evaluation Criteria FRN Publication Date: 08-02-2016

We have a date- it's going out on Monday.

We obviously still need Henry's text...

-Andy

From: Lieberman, Melissa J. (Fed)
Sent: Thursday, July 28, 2016 8:20 AM
To: Regenscheid, Andrew (Fed); Jillavenkatesa, Ajit (Fed); Gillerman, Gordon (Fed); Scholl, Matthew (Fed); Chen, Lily (Fed); Porter, Gail (Fed); Huergo, Jennifer (Fed)
Cc: Wixon, Henry N. (Fed); Nist, Jennifer (Fed); Nair, Rajesh B. (Fed); Whiting, Jazmine (Fed); Harman, Michelle C (Fed)
Subject: Post-Quantum Cryptography Requirements and Evaluation Criteria FRN Publication Date: 08-02-2016

All,
FYI
Melissa
Melissa J. Lieberman
Deputy Chief Counsel for NIST
Phone: (301) 975-4783
Fax: (301) 926-6241

From: noreply@fedreg.gov [mailto:noreply@fedreg.gov]
Sent: Thursday, July 28, 2016 8:08 AM
To: Lieberman, Melissa J. (Fed) <melissa.lieberman@nist.gov>
Cc: CREID@GPO.GOV
Subject: SCHEDULED: Document Number - 2016-18150

Please do not reply directly to this e-mail. If you have any questions or comments regarding this email, please contact Chipp Reid.

Attention : Melissa Lieberman, (NIST) National Institute of Standards and Technology

Document 2016-18150, Category NOTICES has been scheduled to publish on 08-02-2016. This document will be placed on public inspection on 08-01-2016 08:45:00.

The subject of this document is Post-Quantum Cryptography Requirements and Evaluation Criteria.
The submitting Agency is (NIST) National Institute of Standards and Technology.
The Docket Id is Docket No. 160606494-6494-01.
The RIN is NA.
This document has an effective date of NA.
The comments due date is NA.
The separate part # for this document is NA.
Agency/CFR Title/CFR Part:

Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Request for Comments on Post-Quantum Cryptography Requirements and Evaluation Criteria

Docket No. [160606494-6494-01]

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice; Request for Comments

SUMMARY: The National Institute of Standards and Technology (NIST) is requesting comments on a proposed process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Current algorithms are vulnerable to attacks from large-scale quantum computers. The purpose of this notice is to solicit comments on the draft minimum acceptability requirements, submission requirements, evaluation criteria, and evaluation process of candidate algorithms from the public, the cryptographic community, academic/research communities, manufacturers, voluntary standards organizations, and Federal, state, and local government organizations