From: Scholl, Matthew
To: O"Reilly, Patrick D. (Fed)
Cc: Chen, Lily (Fed)
Subject: Re: FW: new NISTIR for post-quantum cryptography
Date: Tuesday, February 2, 2016 9:42:47 AM

Yes please do.

-------- Original Message --------
From: "O'Reilly, Patrick D." <patrick.oreilly@nist.gov>
Date: Tue, February 02, 2016 9:38 AM -0500
To: "Scholl, Matthew" <matthew.scholl@nist.gov>
CC: "Chen, Lily" <lily.chen@nist.gov>
Subject: FW: new NISTIR for post-quantum cryptography

Matt, (cc: Lily)

Do I have your permission to post Dustin's "new" NISTIR (1st Draft) to CSRC Drafts page?
Here is his announcement – document is attached:

NIST IR 8105

DRAFT Report on Post-Quantum Cryptography

NIST requests public comments on NISTIR 8105, Report on Post-Quantum Cryptography. In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of *post-quantum cryptography* (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks. This Internal Report shares the National Institute of Standards and Technology (NIST)'s current understanding about the status of quantum computing and post-quantum cryptography, and outlines NIST's initial plan to move forward in this space. The report also recognizes the challenge of moving to new cryptographic infrastructures and therefore emphasizes the need for agencies to focus on crypto agility.

The public comment period will close on: March 9, 2016.
Send questions to NISTIR8105-comments@nist.gov with "Comments NISTIR 8105" in the subject line.

Thanks much.
Patrick

From: Moody, Dustin
Sent: Tuesday, February 02, 2016 9:13 AM
To: O'Reilly, Patrick D.; Foti, Jim
Cc: Chen, Lily; Liu, Yi-Kai
Subject: RE: new NISTIR for post-quantum cryptography

Pat,

The NISTIR is attached. The title is “Report on Post-Quantum Cryptography”. The NISTIR number will be 8105. Thanks! Let me know if you need anything else.
Dustin

From: O'Reilly, Patrick D.
Sent: Tuesday, February 02, 2016 9:08 AM
To: Foti, Jim <james.foti@nist.gov>; Moody, Dustin <dustin.moody@nist.gov>
Cc: Chen, Lily <lily.chen@nist.gov>; Liu, Yi-Kai <yi-kai.liu@nist.gov>
Subject: RE: new NISTIR for post-quantum cryptography

Before I can post a “new” draft NISTIR (or other technical series documents) to CSRC, I will need Matt Scholl’s approval to post.
So Dustin, can you send me the title of the NISTIR and the file – I will forward to Matt for his approval.
I’m sure it is okay – but that is how he wants “new” technical series documents to be posted – quality control.
Thanks.
Pat

From: Foti, Jim
Sent: Tuesday, February 02, 2016 9:02 AM
To: Moody, Dustin
Cc: Chen, Lily; Liu, Yi-Kai; O'Reilly, Patrick D.
Subject: RE: new NISTIR for post-quantum cryptography

Hi Dustin-
Thanks for the heads-up. A couple of details we need to take care of first: 1) get a NISTIR #, and 2) get an email alias, if you don’t have one already that you want to use.
I’ll take care of requesting the NISTIR # in a minute (and will CC you).
If you do need an alias, you can send a request to alias@nist.gov. Indicate:
1) the alias that you want, and 2) the emails of people who should receive emails going to the new alias.
You’ll also have to prepare a brief blurb that Patrick can post on CSRC. Please look at the Drafts page for examples. Patrick can also provide you with a spreadsheet where you can select relevant topics and terms for the CSRC publications pages.
Once we get the NISTIR # and the email alias, you can add them to the draft. I’m teleworking today, but we can meet tomorrow and discuss any remaining minor details in the document. Overall it looks good.
Best,
Jim

From: Moody, Dustin
Sent: Monday, February 01, 2016 1:03 PM
To: Foti, Jim <james.foti@nist.gov>
Cc: Chen, Lily <lily.chen@nist.gov>; Liu, Yi-Kai <yi-kai.liu@nist.gov>
Subject: new NISTIR for post-quantum cryptography

Jim,
I’m on the post-quantum cryptography project, and we’ve written a NISTIR report on the topic. Weare ready for it to be published online, and would like for people to be able to submit comments for 30 days. I’ve attached the word file for it. Can you tell me what needs to be done to make this happen? Thanks,

Dustin