

From: [Scholl, Matthew \(Fed\)](#)
To: [Tabassi, Elham \(Fed\)](#)
Subject: FW: question about quantum cryptography for congressional testimony prep
Date: Tuesday, October 17, 2017 9:07:10 PM
Attachments: [ETSI-2017-update-09062017.pptx](#)
[Crypto in PQ world -DoC.pptx](#)
[Crypto in PQ world -MIT.pptx](#)
[PQC-NAS.pptx](#)
[PQC-NAF-02052017.pptx](#)
[Crypto in PQ world -BITS.pptx](#)

More than you need for PQC info.

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Thursday, October 5, 2017 at 11:02 AM
To: "Gundlach, David (Fed)" <david.gundlach@nist.gov>
Cc: "Chen, Lily (Fed)" <lily.chen@nist.gov>, "Scholl, Matthew (Fed)" <matthew.scholl@nist.gov>
Subject: RE: question about quantum cryptography for congressional testimony prep

Some slide decks attached which we've used on PQC briefings in the past.

From: Scholl, Matthew (Fed)
Sent: Thursday, October 05, 2017 10:52 AM
To: Gundlach, David (Fed) <david.gundlach@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: question about quantum cryptography for congressional testimony prep

David,

Can do. We have a few slide decks we have used to talk PQC as well as:

PQC Overview Web Page; <https://csrc.nist.gov/projects/post-quantum-cryptography>
News Pages on PQC: <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/news>
The IR on the PQC Project: <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/publications>

Let me know when you want to meet. Today is a bit nutty but I am open about 3. I will see if we can get you some slides in the mean time

Matt

From: "Gundlach, David (Fed)" <david.gundlach@nist.gov>
Date: Thursday, October 5, 2017 at 9:36 AM
To: "Scholl, Matthew (Fed)" <matthew.scholl@nist.gov>
Subject: question about quantum cryptography for congressional testimony prep

Hi Matt,

I am working up testimony for Carl Williams re. quantum computing. Part of that testimony will touch on cryptography. Would you have time to chat today. I need to close the document out soon and I think the crypto side still needs the most help. This should not be an exhaustive list of activities or in too much detail but basically pointing out the significant activities at NIST re. quantum crypto, post quantum crypto, and possibly algorithms and applications.

Thanks,

David J. Gundlach

Program Coordination Office
Office of the Under Secretary for Standards & Technology, and NIST Director

National Institute of Standards and Technology (NIST)
100 Bureau Dr. MS-1060
Building 101 / Room A1005
Gaithersburg, MD 20899-1060
Office: 301-975-8085

David.Gundlach@NIST.gov