From:	Perlner, Ray
To:	Regenscheid, Andrew
Subject:	FW: Our Feb 2nd PQC meeting with Michael Groves
Date:	Wednesday, January 27, 2016 1:20:00 PM
Attachments:	QSC(15)004004 (March16)_WI3_Suitability.docx QSC(16)004006_Quantum_Safe_Primitives.docx

---

From: Moody, Dustin
Sent: Wednesday, January 27, 2016 9:24 AM
To: Chen, Lily; Liu, Yi-Kai; Jordan, Stephen P; Perlner, Ray; Peralta, Rene; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)
Subject: Our Feb 2nd PQC meeting with Michael Groves

Everyone,

Reminder - we are meeting on Feb. 2nd with Michael Groves, from the UK. He will update us on ETSI's work on PQC, and we will update him on our project. I'm attaching two documents he has sent in advance. The first is a good summary of most of the potential candidates out there. The second talks more about the challenges in putting these into protocols like TLS, and IPSEC. Note, these documents are for internal use only - not to be shared. Here is how Michael put it:

"Here are three documents for the meeting. The first is the completed visitors form. The others two are draft Work Items from the ETSI ISG which I propose to talk through with you in more detail when I visit. Could you note that these documents are still in preparation and are formally owned by ETSI. In particular you should not show them to anyone outside your immediate NIST (and IAD) colleagues until the final versions are made public sometime later this year."

Thanks,

Dustin