From:	Moody, Dustin (Fed)
To:	Miller, Carl A. (Fed); Chen, Lily (Fed)
Subject:	RE: Inquiries about PQC competition
Date:	Wednesday, January 11, 2017 8:40:00 AM

Carl,

Sounds to me like you got it.

Dustin

From: Miller, Carl A. (Fed)
Sent: Tuesday, January 10, 2017 5:17 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Inquiries about PQC competition

Hi Dustin & Lily –

Today I was at a conference, and I had a long conversation with a guy who asked me (among other things) a bunch of questions about the PQC competition. He seemed to be advocate for multi-variate crypto methods, and wanted to convince me that they were effective, as well as to find out who Is else is involved in the PQC project. He seemed a little pushy (though it was generally an ok conversation).

I just wanted to know if there's any pitfalls that I should watch out for if someone is asking information about one of our competitions. My assumption is that the general process & personnel are public knowledge, so there's not much of a risk in talking about that stuff (though I should be careful not to reveal anything too early). And that we need to watch out for any unfair influence on the outcome of the competition. Let me know if you have any other thoughts. Talk to you later!

-Carl

———

Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD