

**From:** [Regenscheid, Andrew \(Fed\)](#)  
**To:** [Moody, Dustin \(Fed\)](#); [Chen, Lily \(Fed\)](#)  
**Subject:** Re: NIST Director remarks at RSA  
**Date:** Monday, February 11, 2019 11:12:35 AM

---

What you gave me is good. I don't need anything else for now.

---

**From:** "Moody, Dustin (Fed)" <dustin.moody@nist.gov>  
**Date:** Monday, February 11, 2019 at 11:10 AM  
**To:** "Regenscheid, Andrew (Fed)" <andrew.regenscheid@nist.gov>, Lidong Chen <lily.chen@nist.gov>  
**Subject:** RE: NIST Director remarks at RSA

How much do you want? (measured in either time or # of slides I guess)

---

**From:** Regenscheid, Andrew (Fed)  
**Sent:** Monday, February 11, 2019 11:08 AM  
**To:** Chen, Lily (Fed) <lily.chen@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>  
**Subject:** Re: NIST Director remarks at RSA

Thanks!

Matt Heyman is putting together his remarks. I ran into him in the hallway and offered to send him some material he could work in. We should get a draft of the remarks.

This will just be a very small part of what he will say.

-Andy

---

**From:** Lidong Chen <[lily.chen@nist.gov](mailto:lily.chen@nist.gov)>  
**Date:** Monday, February 11, 2019 at 10:59 AM  
**To:** "Moody, Dustin (Fed)" <[dustin.moody@nist.gov](mailto:dustin.moody@nist.gov)>, "Regenscheid, Andrew (Fed)" <[andrew.regenscheid@nist.gov](mailto:andrew.regenscheid@nist.gov)>  
**Subject:** Re: NIST Director remarks at RSA

Hi, Andy,

That is also the number I can think about. I think we need to provide him with objective of the project. Some straightforward statement may help. e.g. to develop cryptographic tools for cybersecurity in quantum time, to deal with quantum threats to cybersecurity, etc. We can also provide him some statement of NIST role, e.g. promote, manage, accommodate research and development of quantum resistant cryptosystems, etc.

Are you going to put together a paragraph or a bullet? If you need anything else, please let us know.

Lily

---

**From:** Dustin Moody <[dustin.moody@nist.gov](mailto:dustin.moody@nist.gov)>  
**Date:** Monday, February 11, 2019 at 10:47 AM  
**To:** "Regenscheid, Andrew (Fed)" <[andrew.regenscheid@nist.gov](mailto:andrew.regenscheid@nist.gov)>, Lily Chen <[lily.chen@nist.gov](mailto:lily.chen@nist.gov)>  
**Subject:** RE: NIST Director remarks at RSA

We had 82 total submissions, 69 accepted. 26 advancing to the 2<sup>nd</sup> round.

We had a total of 278 people who formed part of the submission teams, from 6 continents, including 26 countries and 16 states.

That's probably the best numbers. I could give you the number of people signed up on the pqc-forum (about 1300) or the number of official comments, but those aren't as interesting.

As for what to say, maybe just that we invite the cryptographic community to evaluate the 26 second round candidates, as we need all the help we can get. They are a diverse group of algorithms, which requires experts from many different fields.

Dustin

---

**From:** Regenscheid, Andrew (Fed)  
**Sent:** Monday, February 11, 2019 10:42 AM  
**To:** Chen, Lily (Fed) <[lily.chen@nist.gov](mailto:lily.chen@nist.gov)>; Moody, Dustin (Fed) <[dustin.moody@nist.gov](mailto:dustin.moody@nist.gov)>  
**Subject:** NIST Director remarks at RSA

Lily, Dustin,

Director Copan is going to be giving a keynote at the RSA conference. They're going to work a short statement about the PQC effort. Do you have any numbers/talking points that emphasize the breadth of involvement in the process? It's not worth coming up with anything new- we could just highlight the number of submissions- I was just wondering if there was anything else that were already saying in your own talks.

And on this topic, is there anything in particular you'd like Walt to say on PQC?

-Andy

