From: Chen, Lily (Fed)
To: Moody, Dustin (Fed)
Subject: Re: slides for ISPAB
Date: Wednesday, June 8, 2016 2:46:48 PM

Thanks, Let's discuss tomorrow.

Lily

From: Moody, Dustin (Fed)
Sent: Wednesday, June 8, 2016 2:22:40 PM
To: Chen, Lily (Fed)
Subject: RE: slides for ISPAB

Lily,

I’ve attached some updated slides based on your recommendations. We can discuss them tomorrow. Thanks!

Dustin

From: Chen, Lily (Fed)
Sent: Wednesday, June 08, 2016 9:59 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: slides for ISPAB

Let’s finalize the slides tomorrow.

Lily

From: Dustin Moody <dustin.moody@nist.gov>
Date: Wednesday, June 8, 2016 at 9:41 AM
To: Lily Chen <lily.chen@nist.gov>
Subject: RE: slides for ISPAB

Lily,

I see what you are saying. I will update the slides and send back to you later today. Friday I will be off.

Dustin

From: Chen, Lily (Fed)
Sent: Wednesday, June 08, 2016 9:27 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: slides for ISPAB

Hi, Dustin:

I looked at the slides. They look good. Since you have presented the content once (some part probably a few times), these are probably in the most confortable style and tone. I do not suggest change the slides. But I like to get your attention about the syle difference between a talk to research community/industry forum and a talk to a board. Please take a look of the letter NIST to ISPAB at http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/0906_001.pdf You can see that we NIST specifically ask input from the board on a few aspects. The presentation shall more or less focus on those aspects.

Here are some comments.

1. Background part can shorten and dense a little bit from classical computer vs. quantum computer to sky is falling page.
2. The page on how soon we need to worry, the x, y, z equation was presented by NSA at the previous ISPAB as well. You may want to change it to language.
3. Before observations, I think we shall talk about what shall be replaced in NIST standards (signature FIPS 186, key establishment800-56A/B).
4. Gathering steam page, we need to have a slide focusing on NIST actions. What we did, have been doing, and will do. For example, we have by-weekly seminar, publish research results at conferences (PQcrypto 2013-2016?), Talks at PQCrypto 2014 and PQCrypto2016, presentations at ETSI quantum-safe crypto workshops, and other workshops, like AWACS.
5. Add one slide for "collaberation" or "interaction", like meeting with CFRG in IETF, work with ISO/IEC JTC 1 SC27 to initiate a study period on quantum resistant cryptography, invite speakers/guest researchers, etc.
6. Probably first talk about timeline and then talk about call for proposals. (switch the two slides).
7. Page 16 and page 18 both talked about IPR, shall they merge?
8. Page 20, the font is too small. Maybe you can make a two column page. (The font is not even. We can justify when we consider the content is determined.
9. Questions- Do we like to ask all of these questions to ISPAB or say these are the questions we ask for answers.
10. Concluusion, we might want to say something about we would like to get comments and input from the board. Let's think about it.
(I am still thinking to reduce some details because ISPAB members are not submitters. Too many details are not good for them to see big pictures.)
I am working from home today and will be in the office tomorrow and Friday. We can talk about the slides before we send to Annie.
Thanks,
Lily

ISPAB Received Response from NIST Director, Dr. Willie May

csrc.nist.gov

quantum standards a roadmap and timeline for getting to generally ps, competitions tor necessary algorithms. such a plan. The Board urges the creation of a

From: Moody, Dustin (Fed)
Sent: Tuesday, June 7, 2016 3:36:52 PM
To: Chen, Lily (Fed)
Subject: slides for ISPAB
Lily,
I combined several slides I've used in some of our past presentations into the attached file. Let me

know if you want me to modify anything – like anything from your slides from the Another Workshop on Crypto Standards talk. Thanks!
Dustin