From:	Chen, Lily (Fed)
To:	Perlner, Ray A. (Fed); Moody, Dustin (Fed); (b) (6)
Subject:	Resolution to handle comments on "standardization"
Date:	Tuesday, July 5, 2016 11:36:21 AM
Attachments:	Changes in Call for submissions.docx

Hi, Ray and Dustin:

Attached please see some proposed text to address Ajit comments on “standardization”. These text shall be checked and polished before we include them in the call for submissions.

Lily

[The original paragraphs (1).]

NIST is taking a number of steps with regard to standardizing post-quantum cryptography. For example, NIST is coordinating with other standardization efforts (such as efforts to standardize stateful hash-based signatures). Most importantly, NIST is beginning a process to develop new quantum-resistant standards for key establishment, public-key encryption, and digital signatures. In developing these standards, NIST has two main considerations. First, these cryptosystems should provide strong security against both classical and quantum computers (and combinations thereof). Second, these cryptosystems should be easy to deploy in existing applications and protocols, such as Transport Layer Security (TLS), Internet Key Exchange (IKE), and digital certificates. In particular, these cryptosystems will be used to replace existing NIST standards that are not secure against quantum computers, including Federal Information Processing Standards Publication (FIPS) 186, the Digital Signature Standard (DSS), and NIST Special Publications (SP) 800-56 A/B, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography and Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography.

NIST is soliciting proposals for post-quantum cryptosystems and it will solicit comments from the public as part of its evaluation process. NIST expects to perform multiple rounds of evaluation, over a period of three to five years. The goal of this process is to select a number of acceptable candidate cryptosystems for standardization.

Commented [CL(1]: In fact, this paragraph did not talk about steps.

Commented [CL(2]: After the first sentence, the readers are expecting to see what are those "steps". The example does not go well with any step. Coordinating with other standardization can go with any step.

Commented [CL(3]: Of course, this is the most important part of the paragraph.

Commented [CL(4]: The first part is covered by security requirement 4.A.2 and 4.A.3. The second part is covered by 4.A.2. I suggest we remove this part.

Commented [JA(5]: Do we know that these candidates will be standardized, or would "consideration for standardization" be a better option?

[Suggested replacement]

NIST is beginning a process to develop new quantum-resistant cryptography standards to replace existing NIST standards, including digital signature schemes specified in Federal Information Processing Standards Publication (FIPS) 186 and key establishment schemes specified in NIST Special Publications (SP) 800-56 A and B. The process is referred as *post-quantum cryptography standardization*. The standards will be published as Federal Information Processing Standards (FIPSs) or Special Publications (SPs).

NIST is soliciting proposals for post-quantum cryptosystems and it will solicit comments from the public as part of its evaluation process. NIST expects to perform multiple rounds of evaluation, over a period of three to five years. The goal of this process is to select a number of acceptable candidate cryptosystems to be standardized in FIPS or NIST SPs.

[The original paragraph (2)]

As a result of these complexities, NIST believes that the post-quantum standards development process should not be treated as a competition; in some cases, it may not be possible to make a well-supported judgment that one candidate is "better" than another. Rather, NIST will perform a thorough analysis of the submitted algorithms in a manner that is open and transparent to the public. This analysis will inform NIST's decision on the subsequent development of post-quantum standards.

Commented [JA(6]: Is this a referene to the NIST process alone, or does this extend to the instances where a NIST identified algorithm is taken to a private sector body such as ISO or JTC1 for development as an international standard?

Commented [JA(7]: Does NIST perform the analyses or are other non-NIST experts also included?

[suggested replacement]

As a result of these complexities, NIST believes that the post-quantum standards development process should not be treated as a competition; in some cases, it may not be possible to make a well-supported judgment that one candidate is "better" than another. Rather, NIST will encourage the community to conduct security analysis and suitability evaluation of the submitted algorithms. The results will be made public through NIST organized workshops and other research events. The synopsis of analysis and evaluation will inform NIST's decision on the subsequent development of post-quantum standards in an open and transparent manner.

Commented [LC8]: This shall be explained by the change in the previous paragraph.