From:	Moody, Dustin
To:	Liu, Yi-Kai; Perlner, Ray; Peralta, Rene; Chen, Lily; Bassham, Lawrence E; Jordan, Stephen P; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)
Subject:	Outline for PQC announcement
Date:	Thursday, January 14, 2016 1:11:59 PM

Everyone,

Sorry for yet another email, but we have much to get done this month. I'm going to start working on the slides for our announcement at PQCrypto. I put together an outline to guide me. Please let me know if I'm missing something. Thanks,

Dustin

1) Motivation (not a lot needed for this audience)
    a. Quote estimate of time til quantum computers, "Mosca's Theorem" (as to why we need to start now)
    b. Impact on PKC / (NIST) standards
        i. Can mention our NISTIR
    c. Mention NSA's statement? (not sure about this) EU's project?
2) NIST Call
    a. Idea of Rene's statement (we want to manage process, hopefully help community to identify good choices…)
        i. Talk about similarities/differences between this and AES/SHA-3 competitions? (not sure about this)
    b. Timeline
        i. Formal call out by late 2016. (SHOULD WE PICK A DATE?)
        ii. Deadline for Submissions, late 2017 (DATE?)
        iii. Workshop ?? not too long after deadline
        iv. Analysis phase, 3-5 years
            1. Do we want rounds?? Announce workshops?
            2. We will issue report at end (or after round? Or halfway through?)
        v. Draft standard for public comment, 2 years later (DATE?)
        vi. Can accept submissions on ongoing basis (like modes), but…
    c. Maybe here would be better to talk about difference from competition? (if we want to)
3) More details
    a. Detailed instructions will be similar to SHA-3
        i. Parameter sets, target security levels
        ii. Specification/code
            1. API instructions?
            2. Call approved symmetric primitives?
            3. Implementations
                a. C code
                b. Known answer / Monte-Carlo tests
    b. Evaluation criteria (will be open for public comment?)
        i. Security analysis

1. What are the right security definitions?
2. Algorithm complexity definitions
3. Security proofs not required?
4. Quality of prior cryptanalysis

ii. Performance analysis
1. Parameters & key sizes
2. Time to perform operations

iii. Practical deployment
1. Ease of implementation, ease of use, misuse resistance

iv. IPR stuff (not sure if here or in 3a)
1. If can make license free than it's a big advantage, but not required

v. Questions we have
1. How is the timeline? Too fast? Too slow?
2. Should all the proposals be on the same schedule, or should we try to "fast-track" those proposals that seem more mature?
3. Should we just focus on encryption and signatures, or should we also consider other functionalities like stateful signatures and key establishment?
4. How many "bits of security" do we need against quantum attacks?
5. How can we encourage more work on quantum cryptanalysis? Maybe we could pose some more "challenge problems"?
6. If we want to standardize some post-quantum cryptosystem that has worse parameters (such as key length) than our currently-deployed crypto, this may have consequences for higher-level protocols and applications. How can we encourage people to study these issues? For instance, I would feel more confident if we had some more prototype implementations of post-quantum TLS and IKE protocols.
7. Etc….

4) Conclusion
a. Restate our role in managing process
b. We don't have all the answers. We want feedback
c. Contact info (pqc@nist.gov – NSA gets this email as well. Need new email?)
i. Mention pqc – forum for discussion