From: Chen, Lily (Fed)
To: Barker, Elaine B. (Fed)
Subject: RE: NIST-NSA TWG notes
Date: Thursday, March 9, 2017 11:28:00 AM

Elaine:

1. When IETF work on hash based signature is finalized NIST is planning to pull in them to a SP and look into issues. It is still open on which hash based signature among XMSS and LMS or both will be included.
2. We will give presentations at BITS (March 16, 2018), National Academy of Science (March 24), ICMC (May 17), IAS (June 18-21), PQCrypto (June 26-28)
3. NISTIR 8114 is a technical report on lightweight cryptography. It will be published in the next few days. We have call for proposals on profiles. The algorithms will be required to target specific profiles.

Lily

From: Barker, Elaine B. (Fed)
Sent: Thursday, March 09, 2017 11:18 AM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: NIST-NSA TWG notes

Could you please send me a summary of the following:

1. Hashed-based signature into NIST format
2. Varous PQ C talks planned: CFRG, IAS, ITS, PQ crypto (where and when)
3. NISTIR 8114 to be published soon: what's in it
4. Call for proposals for profiles; implementation environments

Thanks, Elaine