From: Chen, Lily (Fed)
To: Barker, Elaine B. (Fed)
Subject: RE: NIST-NSA TWG meeting
Date: Tuesday, June 28, 2016 2:54:36 PM

There is a hybrid mode update. An IETF draft specifies a hybrid cipher suite https://tools.ietf.org/html/draft-whyte-qsh-tls12-01. The final premaster secret is the concatenation of all the secret values, established by classical method and by quantum-safe method. To Validate the Hybrid mode, the key derivation test will need to be modified to allow form the final premaster secret. William Whyte from Security Innovation also suggested another method to input the secret values established through quantum-safe algorithm in the SuppPrivInfo portion of key derivation function. Claim that it will not require any change of the current testing. NIST decision on whether to approve such hybrid mode will be rely on the acceptance of IETF community. The discussion at the meeting indicated that the impact on the performance, in particular, the data size, may prevent from a general acceptance of the hybrid mode.
Lily

From: Barker, Elaine B. (Fed)
Sent: Tuesday, June 28, 2016 10:44 AM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: NIST-NSA TWG meeting
Could I have a short writeup for what you reported today about the hybrid approach for quantum crypto?
Thanks, Elaine