From: Keller, Sharon (Fed)
To: Cooper, Michael Joseph (Fed)
Cc: Keller, Sharon (Fed); Chen, Lily (Fed)
Subject: RE: Draft meeting minutes
Date: Monday, April 25, 2016 8:06:44 AM

Hi,

Elaine sent out the meeting notes for the NIST-NSA TWG Meeting from last week. Under the section "SP800-56A revision", the following bullet was included:

- The IKE groups will be approved for the ephemeral-ephemeral schemes, probably by listing in FIPS 140 Annex A.

I wasn't sure if this was similar to the XPN issue. Is FIPS140 Annex A supposed to be used for this or is this something that needs to be added to an SP?

It's possible it's ok, I just wanted to get your opinion.

Please let me know what you think.

Thanks,

Sharon

From: Barker, Elaine B. (Fed)
Sent: Friday, April 22, 2016 10:17 AM
Subject: Draft meeting minutes

Comments would be appreciated.

Elaine