From:	Moody, Dustin (Fed)
To:	Perlner, Ray A. (Fed); Chen, Lily (Fed); Liu, Yi-Kai (Fed); Jordan, Stephen P (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Peralta, Rene C. (Fed)
Subject:	Latest version of the CFP
Date:	Tuesday, May 31, 2016 11:05:03 AM
Attachments:	CFP v9.4.docx

Everyone,

Hope everyone had a nice long weekend. I've attached the latest version of the CFP, which incorporates some changes to clarify some of the things the NSA comments discussed. Most of them are minor. The biggest addition is to the quantum security section in 4.A.4, which Ray and Yi-Kai wrote. We also removed any mention of FIPS or validation when talking about hybrid modes. We can address that in a FAQ on our website. Let me know if there are any comments on anything. Thanks!

Dustin