From: Moody, Dustin (Fed)
To: Barker, Elaine B. (Fed)
Subject: RE: FY 2018 work
Date: Tuesday, November 14, 2017 8:48:00 AM

There is an ongoing revision of FIPS 186. It will also include a new SP 800-186, which will be on elliptic curves.

And of course we are doing a major PQC project, but it isn't tied to a FIPS or SP (yet)

From: Barker, Elaine B. (Fed)
Sent: Tuesday, November 14, 2017 8:25 AM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Dang, Quynh (Fed) <quynh.dang@nist.gov>; Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>; Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Miller, Carl A. (Fed) <carl.miller@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>; Cooper, David A. (Fed) <david.cooper@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>; McKay, Kerry A. (Fed) <kerry.mckay@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: FY 2018 work

Donna has asked Curt for a list of our projects for this fiscal year and their status. I think this is intended to make sure that there's no duplication with the cybersecurity projects and the support is provided when and where needed (e.g., by NCCoE and NICE).

Make additions and corrections to the partial list below, and send back to me to coordinate.

Thanks, Elaine

Block Ciphers
SP 800-38? (Morrie?)
SP 800-67 (TDEA) revision: should be posted as complete this week or next week

RBGs
SP 800-90B (entropy sources):going through WERB
SP 800-90C (RBG Constructions): trying to complete this year

Key Establishment
SP 800-56A (FFC DH and MQV): addressing public comments; should be completed this quarter
SP 800-56B (RSA key establishment): beginning a revision
SP 800-56C (KDFs for 56A and 56B): addressing public comments; should be completed this quarter
SP 800-108 (KDFs) revision: beginning

General Key Management

SP 800-57, Part 2 (best key management practices for organizations): revision in progress
SP 800-57, Part 1 (general key management guidance): will revise to conform with SP 800-131A revision
SP 800-57, Part 3/new SP (Ipsec key management guidance) revision/new SP:
SP 800-71 (symmetric key management): resuming the project
SP 800-131A (transitions): will be beginning a revision this quarter
New SP (organizational key storage and recovery): in progress

Protocols
SP 800-77 (IPsec) revision: beginning

Research