From: Chen, Lily (Fed)
To: Perlner, Ray (ray.perlner@nist.gov); Kelsey, John M. (john.kelsey@nist.gov)
Subject: FW: Review for SP 800-106 Randomized Hashing for Digital Signatures
Date: Friday, March 4, 2022 9:21:00 AM

Hi, Ray and John,

I fully understand that you both have your plates full and even overflow. Hopefully, after we have the PQC report stable, we can have some time to look into this.

800-106 is about randomized hashing, which was generated when we were dealing with SHA1 collision attacks. We need one expert to look into it with strong knowledge and also know the history to help us to make a decision. Therefore, I do not suggest new person to review this document. Would one of you to schedule a time to review it? We have more reviews to go. If one of you review 106 then another will review the next. Or maybe let Chris know when you can schedule a time to review.

Thanks,
Lily

From: Celi, Christopher T. (Fed) <christopher.celi@nist.gov>
Date: Tuesday, February 22, 2022 at 4:03 PM
To: Kelsey, John M. (Fed) <john.kelsey@nist.gov>, Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Cc: Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>, Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Review for SP 800-106 Randomized Hashing for Digital Signatures

Hi Ray and John,

The Crypto Pub Review Board is looking for a reviewer for SP 800-106. Would either of you have time to review this document over the next few months? If a different timeline works better, let me know. If you do not have time to review the document, also let me know so the board can look elsewhere within the group for a reviewer.

When you are ready I can provide the public comments for the document, and additional information from the CAVP.

Thanks,
Chris Celi