Yes, we've run the code through already, and I'm writing up notes of what's lacking.

Larry

On: 27 February 2019 15:30,
"Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov> wrote:

Oh you dealt with the code already?

From: "Bassham, Lawrence E. (Fed)" <lawrence.bassham@nist.gov>
Date: Wednesday, February 27, 2019 at 3:17 PM
To: "McKay, Kerry A. (Fed)" <kerry.mckay@nist.gov>, "Alperin-Sheriff, Jacob (Fed)"
<jacob.alperin-sheriff@nist.gov>, "Sonmez Turan, Meltem (Assoc)" <meltem.turan@nist.gov>
Subject: Re: Which Submissions Should I do?

We've looked over the code portion. I think we can use more help in the documentation portion of the reviews.

From: "McKay, Kerry A. (Fed)" <kerry.mckay@nist.gov>
Date: Wednesday, February 27, 2019 at 2:24 PM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Sonmez Turan, Meltem (Assoc)" <meltem.turan@nist.gov>
Cc: "Bassham, Lawrence E. (Fed)" <lawrence.bassham@nist.gov>
Subject: Re: Which Submissions Should I do?

Jacob,

Thanks for helping out with this. I think that Meltem wanted to make a couple minor tweaks to the checklist. She is in another meeting at the moment, but hopefully we can get that done and assign everyone submission packages to review today or tomorrow. You can start looking at those that you named.

Thanks!
-Kerry

From: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>

Date: Wednesday, February 27, 2019 at 2:18 PM
To: "Sonmez Turan, Meltem (Assoc)" <meltem.turan@nist.gov>, "McKay, Kerry A. (Fed)"
<kerry.mckay@nist.gov>
Cc: "Bassham, Lawrence E. (Fed)" <lawrence.bassham@nist.gov>
Subject: Which Submissions Should I do?

https://nistgov.sharepoint.com/:w:/r/sites/LightweightCrypto/_layouts/15/Doc.aspx?
sourcedoc=%7B393755A9-A056-4D84-9A9B-
641655D36F26%7D&file=Checklist%20for%20Submissions.docx&action=default&mobileredirect=true

I assume I should just do something like what we did with PQC and fill one of these out for the
Source Code and Test Vectors section?

I've read through the CFP and the requirements seem identical or close to it.

I guess for now I can take the first 10
(ace,ascon,bleep64,cilipadi,clae,clx,comet,drygascon,elephant,estate) unless I hear back differently

—Jacob Alperin-Sheriff