From:	Alperin-Sheriff, Jacob (Fed)
To:	Perlner, Ray A. (Fed); Moody, Dustin (Fed); Kerman, Sara J. (Fed)
Cc:	internal-pqc
Subject:	Re: Posting Our Attack Thoughts?
Date:	Thursday, December 21, 2017 2:14:47 PM

Hey why not?

From: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Date: Thursday, December 21, 2017 at 2:14 PM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, "Kerman, Sara J. (Fed)" <sara.kerman@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: RE: Posting Our Attack Thoughts?

I'm sort of tempted to hold off, just to see how long it takes the community to find exactly the same things we did, but that may be silly.

From: Alperin-Sheriff, Jacob (Fed)
Sent: Thursday, December 21, 2017 2:13 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: Re: Posting Our Attack Thoughts?

That's for conference-type publications only though, no?

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Thursday, December 21, 2017 at 2:12 PM
To: "Kerman, Sara J. (Fed)" <sara.kerman@nist.gov>, "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: Re: Posting Our Attack Thoughts?

I suppose we should keep in mind what Daniel was discussing yesterday as well, in regards to this.

From: Kerman, Sara J. (Fed)
Sent: Thursday, December 21, 2017 2:11:19 PM
To: Alperin-Sheriff, Jacob (Fed); Moody, Dustin (Fed)
Cc: internal-pqc
Subject: RE: Posting Our Attack Thoughts?

I think that would qualify as an "OFFICIAL COMMENT". So yes, you should click the link so it's

“official”. Periodically I will compile them into a PDF and link via the “View Comments”.

Does that help?
Sara

From: Alperin-Sheriff, Jacob (Fed)
Sent: Thursday, December 21, 2017 2:01 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: Posting Our Attack Thoughts?

I assume we’ll post them under “Submit Comment?” Or are we posting them elsewhere? Let us know.

—Jacob Alperin-Sheriff