From:	Moody, Dustin (Fed)
To:	Peralta, Rene C. (Fed); Chen, Lily (Fed); Mouha, Nicky W. (Assoc)
Cc:	Kelsey, John M. (Fed); Dang, Quynh H. (Fed); Perlner, Ray A. (Fed); Alperin-Sheriff, Jacob (Fed); Sonmez Turan, Meltem (Fed); Calik, Cagdas (IntlAssoc); Brandao, Luis (IntlAssoc); McKay, Kerry A. (Fed); Regenscheid, Andrew R. (Fed); Dworkin, Morris J. (Fed); Barker, Elaine B. (Fed)
Subject:	RE: Any updates we like to announce at crypto 2017?
Date:	Wednesday, August 16, 2017 8:47:28 AM
Attachments:	pqc crypto rump slides condensed.pptx

I agree with Rene. We shouldn't take too many slots.

I attached condensed PQC slides, which are just 2 slides.

Dustin

From: Peralta, Rene (Fed)
Sent: Wednesday, August 16, 2017 8:34 AM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Mouha, Nicky W. (IntlAssoc) <nicky.mouha@nist.gov>
Cc: Kelsey, John M. (Fed) <john.kelsey@nist.gov>; Dang, Quynh (Fed) <quynh.dang@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>; Calik, Cagdas (IntlAssoc) <cagdas.calik@nist.gov>; Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>; McKay, Kerry A. (Fed) <kerry.mckay@nist.gov>; Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>; Barker, Elaine B. (Fed) <elaine.barker@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Any updates we like to announce at crypto 2017?

I don't know that we should take several slots of the Rump session.

If we can't condense our stuff to a few slides, then maybe we can

put out flyers? do both?

Rene.

From: Chen, Lily (Fed)

Sent: Wednesday, August 16, 2017 8:31 AM
To: Mouha, Nicky W. (IntlAssoc)
Cc: Peralta, Rene (Fed); Kelsey, John M. (Fed); Dang, Quynh (Fed); Perlner, Ray (Fed); Alperin-Sheriff, Jacob (Fed); Sonmez Turan, Meltem (Assoc); Calik, Cagdas (IntlAssoc); Brandao, Luis (IntlAssoc); McKay, Kerry A. (Fed); Regenscheid, Andrew (Fed); Dworkin, Morris J. (Fed); Barker, Elaine B. (Fed); Moody, Dustin (Fed)
Subject: RE: Any updates we like to announce at crypto 2017?

Thank you for the suggestions. Rump session talks are short. We might need to separate to multiple.

1. Lightweight
2. PQC
3. Beacon
4. TDEA (800-67), 56A/C call for public comments.

What do you think? Thanks,

Lily

From: Mouha, Nicky W. (IntlAssoc)
Sent: Monday, August 14, 2017 5:50 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Cc: Peralta, Rene (Fed) <rene.peralta@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>; Dang, Quynh (Fed) <quynh.dang@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>; Calik, Cagdas (IntlAssoc) <cagdas.calik@nist.gov>; Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>; McKay, Kerry A. (Fed) <kerry.mckay@nist.gov>; Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>; Barker, Elaine B. (Fed) <elaine.barker@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Any updates we like to announce at crypto 2017?

Hi all,

It doesn't seem that many people are aware yet of the Triple-DES announcement and of the new Draft SP 800-67r2.

The CRYPTO rump session could be a good opportunity to bring this to the attention of the community.

In case it would be a good idea to talk about this, below is an idea of some slides that could be presented.

Regards,
Nicky

Title: Update on Triple-DES

Slide 1
---

* Announcement
 - "Update to Current Use and Deprecation of TDEA"
 - http://csrc.nist.gov/news_events/

* Plans
 - Plan to decrease data limit per key bundle
 - Plan to disallow Triple-DES for some protocols (e.g.: TLS, IPsec)

* Comments
 - Send to "TDEA_Deprecation@nist.gov" by October, 1

Slide 2
---

* Draft NIST SP 800-67 Rev 2
 - "Recommendation for the Triple Data Encryption Standard (TDEA) Block Cipher"
 - http://csrc.nist.gov/publications/PubsSPs.html

* Main change
 - Data limit to apply the protection (e.g., encrypt) per key bundle
 - Old limit: 32 GiB
 - New limit: 8 MiB

* Comments
 - Send to "SP800-67comments@nist.gov" by October, 2

From: Chen, Lily (Fed)
Sent: Monday, August 14, 2017 10:58 AM
To: Peralta, Rene (Fed); Kelsey, John M. (Fed); Dang, Quynh (Fed); Perlner, Ray (Fed); Alperin-Sheriff,

Jacob (Fed); Sonmez Turan, Meltem (Assoc); Calik, Cagdas (IntlAssoc); Brandao, Luis (IntlAssoc)
Cc: McKay, Kerry A. (Fed); Regenscheid, Andrew (Fed); Dworkin, Morris J. (Fed); Barker, Elaine B. (Fed); Moody, Dustin (Fed)
Subject: Any updates we like to announce at crypto 2017?

As we all know, rump session talks are brief, informal, often funny and sometimes not quite remembered. But if we see anything important we shall make an update there, let's put them together. But if we think the things are already announced and/or people are aware them and/or not really a rump session topic, then we just update interested parties through conversation.

Thanks,

Lily