From:	Boutin, Chad T. (Fed)
To:	Scholl, Matthew A. (Fed)
Subject:	FW: upcoming crypto releases
Date:	Thursday, September 16, 2021 3:48:51 PM

Matt, are these the three that you mentioned at ITL Mgmt w/r/t deprecation? Just trying to keep my past and future straight.

CB

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Thursday, September 16, 2021 2:45 PM
To: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Subject: Re: upcoming crypto releases

Hi, Chad,

This is the recent announcement https://csrc.nist.gov/news/2021/proposal-to-withdraw-sp-800-15-sp-800-25-sp-800-32. As you can see that these are very old documents. They are out of date. The content has been replaced by other source. If you have any questions, please let me know.

Lily

From: "Boutin, Chad T. (Fed)" <charles.boutin@nist.gov>
Date: Thursday, September 16, 2021 at 1:36 PM
To: Lily Chen <lily.chen@nist.gov>
Cc: Dustin Moody <dustin.moody@nist.gov>
Subject: upcoming crypto releases

Hi Lily,

As the new fiscal year is approaching, I'm trying to get my story calendar together so I can cover ITL effectively. Today at ITL management council I heard that in the next several months, you would be releasing an update to the post-quantum crypto project and also deprecating a few other algorithms. Could you please give me a timeline on both of these?

Also, I know I need to stay in touch with Dustin on the PQC work … who is the point of contact on the deprecated algorithms?

Thanks as always,
Chad Boutin
Science and IT Writer
NIST Tech Beat
National Institute of Standards and Technology

*

“Ah,” said Arthur. “This is obviously some strange usage of the word ‘safe’ that I was previously unaware of.”