From:	Boutin, Chad T. (Fed)
To:	Moody, Dustin (Fed)
Cc:	Huergo, Jennifer L. (Fed)
Subject:	RE: Is this right?
Date:	Thursday, August 15, 2019 5:00:33 PM

Thanks Dustin. I've contacted one of their editors, who is working on it.
CB

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Thursday, August 15, 2019 9:49 AM
To: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Subject: RE: Is this right?

Chad,
Good catch. We don't foresee selecting algorithms that quickly. We have been saying more like 2022 for when we publish draft standards documents for quantum-resistant public-key crypto algorithms.

Dustin

From: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Sent: Thursday, August 15, 2019 9:46 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Is this right?

Hey Dustin—In this news article https://sg.channelasia.tech/article/665324/what-happens-when-cyber-attackers-reach-quantum-advantage/?fp=2&fpid=1 there's a paragraph saying NIST is developing "common frameworks that would enable "quantum-resistant" cryptographic algorithms. This is set to be released in early 2020."

Is that accurate? I'll send the editor a correction request if not, with any rewording you suggest.

Thanks,
Chad

Chad Boutin
Science Writer
NIST Tech Beat
National Institute of Standards and Technology
301.975.4261

*

"Ah," said Arthur. "This is obviously some strange usage of the word 'safe' that I was previously unaware of."