

**From:** [Moody, Dustin \(Fed\)](#)  
**To:** [Dang, Quynh H. \(Fed\)](#)  
**Subject:** RE: CFRG: The Transition from Classical to Post-Quantum Cryptography  
**Date:** Monday, August 14, 2017 1:28:25 PM

---

Thanks Quynh. It seems accurate enough – doesn't say too much. Probably just intended to give people who haven't been paying attention a heads-up, or quick update.

---

**From:** Dang, Quynh (Fed)  
**Sent:** Monday, August 14, 2017 12:50 PM  
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>  
**Subject:** CFRG: The Transition from Classical to Post-Quantum Cryptography

<https://tools.ietf.org/html/draft-hoffman-c2pq-02>

Hi Dustin,

The CFRG has been working on a post quantum document for a while. The document does not specify which algorithms for usage, but it does discuss various issues about post quantum crypto.

Quynh.