

**From:** [Miller, Carl A. \(Fed\)](#)  
**To:** [Moody, Dustin \(Fed\)](#)  
**Subject:** Re: Completeness checklists completed  
**Date:** Wednesday, October 18, 2017 4:58:57 PM

---

Hi Dustin --

Ok -- I'll look over the Word doc you sent. Thanks!

-Carl

-----  
Carl A. Miller  
Mathematician, Computer Security Division  
National Institute of Standards and Technology  
Gaithersburg, MD

---

**From:** "Moody, Dustin (Fed)" <dustin.moody@nist.gov>  
**Date:** Wednesday, October 18, 2017 at 3:28 PM  
**To:** internal-pqc <internal-pqc@nist.gov>  
**Subject:** Completeness checklists completed

Everyone,

We have completed all the completeness checklists for the submissions for which we needed to provide feedback for. I have compiled all the information, and written a long word document which includes sample emails to each submission team with what they are missing. It is posted on the sharepoint site, under the main Documents section (and also attached to this email). Please take a look and let me know if you find anything missing, or if I need to change something. I will still add information for each team regarding what signatures we've received to date, but don't worry about that.

We will need to send responses back to each team by the end of the month. I would also like at that time to post a message on the forum with some suggestions for those who will submit before our final deadline. Please let me know if you have any suggestions you think should be passed on. For example, here's a few I've been thinking about:

- Provide all the information on the cover sheet which is asked
- Provide a useful readme file (Larry will give some advice here)
- Please clearly state which of our five security strength categories your parameter sets meet
- Please follow our guidance on following our API and generating KATs as posted on our webpage
- Please make sure your implementation is platform-independent.

The more advice we give to submitters to make our lives easier checking completeness, the better. Thanks everyone!

Dustin