

**From:** [Moody, Dustin \(Fed\)](#)  
**To:** [Bassham, Lawrence E \(Fed\)](#)  
**Cc:** [Liu, Yi-Kai \(Fed\)](#)  
**Subject:** API for post-quantum  
**Date:** Monday, February 29, 2016 3:48:00 PM

---

Larry,

We were at the PQCrypto workshop last week, and gave our announcement that we will be calling for quantum-resistant algorithms later this year. Tanja Lange made the suggestion that our API we give should hopefully align nicely for submitting algorithms into their ebacs site. I assume you've already thought of that, but thought I'd pass it on. Thanks,  
Dustin