

**From:** [Scholl, Matthew \(Fed\)](#)  
**To:** [Folk, Alex R. \(Fed\)](#)  
**Subject:** An item for the weekly  
**Date:** Thursday, July 28, 2016 8:57:27 AM

---

On August 1, CSD will post in the federal register a request for comments on a the process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Current algorithms are vulnerable to attacks from large-scale quantum computers. The purpose of this notice is to solicit comments on the draft minimum acceptability requirements, submission requirements, evaluation criteria, and evaluation process of candidate algorithms from the public, the cryptographic community, academic/research communities, manufacturers, voluntary standards organizations, and Federal, state, and local government organizations