

From: [NIST Computer Security Resource Center](#)
To: [Kerman, Sara J. \(Fed\)](#)
Subject: NIST Seeks Comments for Post-Quantum Cryptography: Proposed Requirements and Evaluation Criteria
Date: Friday, August 5, 2016 11:59:59 AM

NIST is seeking comments on Post-Quantum Cryptography: Proposed Requirements and Evaluation Criteria.

The National Institute of Standards and Technology (NIST) has published a Federal Register Notice <<https://federalregister.gov/a/2016-18150>> requesting comments on a proposed 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 the 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 so that their needs can be considered in the process of developing new public-key cryptography standards.

For the draft requirements and evaluation criteria, visit <<http://www.nist.gov/pqcrypto>>.

Comments due: **September 16, 2016**

Send comments to: <pqc-comments@nist.gov>

A public listserv for announcements and discussion is also available; see: <http://csrc.nist.gov/groups/ST/post-quantum-crypto/email_list.html>.

NIST Computer Security Division
webmaster-csrc@nist.gov (Attn: Pat O'Reilly)

Update your subscriptions, modify your password or e-mail address, or stop subscriptions at any time on your [Subscriber Preferences Page](#). You will need to use your email address to log in. If you have questions or problems with the subscription service, please visit subscriberhelp.govdelivery.com. All other enquiries can be directed to webmaster-csrc@nist.gov.

This service is provided to you at no charge by the National Institute of Standards and Technology (NIST).

This email was sent to sara.caswell@nist.gov using GovDelivery, on behalf of: NIST Computer Security Resource Center · 100 Bureau Drive · Gaithersburg, MD 20899 · (301) 975-6478

