From: Foti, James (Fed)
To: O"Reilly, Patrick D. (Fed)
Cc: Chen, Lily (Fed); Kerman, Sara J. (Fed)
Subject: News item for post-quantum crypto
Date: Tuesday, August 2, 2016 8:01:11 AM

Hi Pat-

I'm sure you saw today's FRN about the post-quantum crypto draft criteria:
https://federalregister.gov/a/2016-18150

Besides posting it on the FRN page, could you please also post it as a CSRC News item and send it out via GovDelivery?

Thanks,

Jim

> Subject: 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.

Jim Foti | IT Security Specialist | P:301.975.8018 | jfoti@nist.gov
NIST | 100 Bureau Drive, Stop 8930 | Bldg. 222, Room B349 | Gaithersburg, MD 20899-8930