This document is scheduled to be published in the
Federal Register on 08/02/2016 and available online at
http://federalregister.gov/a/2016-18150, and on FDsys.gov

Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Request for Comments on Post-Quantum Cryptography Requirements and Evaluation Criteria

Docket No. [160606494-6494-01]

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice; Request for Comments

SUMMARY: The National Institute of Standards and Technology (NIST) is 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 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

so that their needs can be considered in the process of developing new public-key cryptography standards. The draft requirements and evaluation criteria are available on the NIST Computer Security Resource Center website: http://www.nist.gov/pqcrypto.

DATES: Comments must be received on or before [INSERT DATE 45 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Comments may be sent electronically to *pqc-comments@nist.gov* with "Comment on Post-Quantum Cryptography Requirements and Evaluation Criteria" in the subject line. Written comments may also be submitted by mail to Information Technology Laboratory, ATTN: Post-Quantum Cryptography Comments, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899-8930.

Comments received in response to this notice will be published electronically at http://www.nist.gov/pqcrypto, so commenters should not include information they do not wish to be posted (e.g., personal or confidential business information).

FOR FURTHER INFORMATION CONTACT: Dr. Lily Chen,
National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899–8930, email: Lily.Chen@nist.gov, by telephone (301) 975–6974.

Technical inquiries regarding the proposed draft acceptability requirements, submission requirements, or the evaluation criteria should be sent electronically to pqc-comments@nist.gov.

A public email list-serve has been set up for announcements, as well as a forum to discuss the standardization effort being initiated by NIST. For directions on how to subscribe, please visit http://www.nist.gov/pqcrypto.

SUPPLEMENTARY INFORMATION:

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will compromise the security of many commonly used cryptographic algorithms. In particular, quantum computers would completely break many public-key cryptosystems, including those standardized in FIPS 186–4, Digital Signature Standard (http://dx.doi.org/10.6028/NIST.FIPS.186-4), SP 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (http://dx.doi.org/10.6028/NIST.SP.800-56Ar2), and SP 800-56B Revision 1, Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography (http://dx.doi.org/10.6028/NIST.SP.800-56Br1).

Due to this concern, many researchers have begun to investigate post-quantum cryptography (PQC) (also called quantum-resistant cryptography). The goal of this research is to develop cryptographic algorithms that would be secure against both quantum and classical computers. A significant effort will be required in order to develop, standardize, and deploy new post-quantum algorithms. In addition, this transition needs to take place well before any large-scale quantum computers are built, so that any information that is later compromised by quantum cryptanalysis is no longer sensitive when that compromise occurs.

NIST has taken a number of steps in response to this potential threat. On April 2-3, 2015, NIST held a public workshop on Cybersecurity in a Post-Quantum World to solicit input on public-key cryptographic policy in the time of quantum computers. NIST also published NISTIR 8105, Report on Post-Quantum Cryptography (http://dx.doi.org/10.6028/NIST.IR.8105), in April 2016 which shares NIST's understanding of the status of quantum computing and post-quantum cryptography.
As a result of study and public feedback, NIST has decided to develop additional public-key cryptographic algorithms through a public standardization process, similar to the development processes for the hash function SHA-3 and the Advanced Encryption Standard (AES). To begin the process, NIST has drafted a set of minimum acceptability requirements, submission requirements, and evaluation criteria for candidate algorithms. The draft document containing these requirements and criteria is available at the Web site: http://www.nist.gov/pqcrypto. NIST seeks comments on these draft minimum acceptability requirements, submission requirements, evaluation criteria, and the evaluation process, as well as suggestions for other criteria and for the relative importance of each individual criterion in the evaluation process. Since neither the submission requirements nor the evaluation criteria have been finalized, and may evolve over time as a result of the public comments that NIST receives, candidate algorithms should NOT be submitted at this time.

AUTHORITY: In accordance with the Information Technology Management Reform Act of 1996 (Pub. L. 104-106) and the Federal Information Security Management Act of 2002 (Pub. L. 107-347), the Secretary of Commerce is authorized to approve FIPS. NIST activities to develop computer security standards to protect federal sensitive (unclassified) information systems are undertaken pursuant to specific responsibilities assigned to NIST by Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3), as amended.

Dated: July 27, 2016

Kent Rochford
Associate Director for Laboratory Programs

[FR Doc. 2016-18150 Filed: 8/1/2016 8:45 am; Publication Date: 8/2/2016]