Billing Code:

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms

Docket No. 161116999-6999-02

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

ACTION: Notice and request for nominations for candidate post-quantum algorithms

SUMMARY: This notice solicits nominations from any interested party for candidate algorithms to be considered for public-key post-quantum standards. The submission requirements and the minimum acceptability requirements of a "complete and proper" candidate algorithm submission, as well as the evaluation criteria that will be used to appraise the candidate algorithms, can be found at http://www.nist.gov/pqcrypto.

DATES: Proposals must be received by November 30, 2017. Further details are available at http://www.nist.gov/pqcrypto.

ADDRESSES: Algorithm submission packages should be sent to Dr. Dustin Moody, Information Technology Laboratory, Attention: Post-Quantum Cryptographic Algorithm Submissions, 100 Bureau Drive – Stop 8930, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930. Submissions may also be sent by email to: pqc-submissions@nist.gov. Note that for email submissions, some of the supporting documentation requires a signature and must be physically mailed to the above address. See http://www.nist.gov/pqcrypto for complete submission instructions.

FOR FURTHER INFORMATION: For general information, send email to pqc-comments@nist.gov. For questions related to a specific submission package, contact Dr. Dustin Moody, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899–8930, email: dustin.moody@nist.gov, or by telephone: (301) 975-8136.

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: The National Institute of Standards and Technology (NIST) has initiated a process to develop and standardize one or more additional public-key cryptographic algorithms to augment FIPS 186–4, Digital Signature Standard, as well as special publications SP 800-56A, Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, and SP 800-56B, Recommendation for Pair-Wise Key-Establishment Schemes Using Integer

Factorization Cryptography. It is intended that the new public-key cryptography standards will specify one or more additional unclassified, publicly disclosed digital signature, public-key encryption, and key-establishment algorithms that are capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers.

As a first step in this process, NIST solicited public comment on draft minimum acceptability requirements, submission requirements, and evaluation criteria for candidate algorithms. The comments received are posted at http://www.nist.gov/pqcrypto, along with a summary of the changes made as a result of these comments.

The purpose of this notice is to announce that nominations for post-quantum candidate algorithms may now be submitted, up until the final deadline of November 30, 2017. Complete instructions on how to submit a candidate package, including the minimal acceptability requirements, are posted at http://www.nist.gov/pqcrypto. The finalized evaluation criteria which will be used to assess the submissions are also posted at the same website.

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 (FISMA) (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.

Kevin Kimball
NIST Chief of Staff

[FR Doc. 2016-30615 Filed: 12/19/2016 8:45 am; Publication Date: 12/20/2016]