Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Announcing Request for Comments on Lightweight Cryptography Requirements and Evaluation Criteria

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 lightweight cryptographic algorithms. Current NIST cryptographic standards were designed to perform well on general-purpose computing platforms, and may not be suitable for some constrained computing environments. The draft requirements and evaluation criteria are available on the NIST Computer Security Resource Center Web site: https://csrc.nist.gov/Projects/Lightweight-Cryptography.

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 lightweight-crypto@nist.gov with “Comment on Lightweight Cryptography Requirements and Evaluation Criteria” in the subject line. Written comments may also be submitted by mail to Information Technology Laboratory, ATTN: Lightweight 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 https://csrc.nist.gov/Projects/Lightweight-Cryptography, 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. Kerry McKay, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899-8930, email: kerry.mckay@nist.gov, by telephone (301) 975-4969. Technical inquiries regarding the proposed draft acceptability requirements, submission requirements, or the evaluation criteria should be sent electronically to lightweight-crypto@nist.gov.

A public email list 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 https://csrc.nist.gov/Projects/Lightweight-Cryptography.

SUPPLEMENTARY INFORMATION: The deployment of small computing devices such as RFID tags, industrial controllers, sensor nodes and smart cards is becoming much more common. The shift from desktop computers to small devices brings a wide range of new security and privacy concerns. It is challenging to apply conventional cryptographic standards to small devices, because the tradeoff between security, performance and resource requirements was optimized for desktop and server environments, and this makes the standards difficult or impossible to implement in resource-constrained devices. Therefore, when current NIST-approved algorithms can be engineered to fit within the limited resources of constrained environments, their performance may not be acceptable.

There are several emerging areas in which highly-constrained devices are interconnected, working in concert to accomplish some task. Examples of these areas include: automotive systems, sensor networks, healthcare, distributed control systems, the Internet of Things (IoT), cyber-physical systems, and the smart grid. In recent years, there has been increased demand for cryptographic standards that are tailored for constrained devices. NIST has decided to create a portfolio of lightweight cryptographic algorithms, designed for limited use in applications and environments where cryptographic operations are performed by constrained devices that are unable to use existing NIST standards.

Lightweight cryptography is a subfield of cryptography that aims to provide solutions tailored for resource-constrained devices. There has been a significant amount of work done by the academic community related to lightweight cryptography; this work includes efficient implementations of conventional cryptography standards, and the design and analysis of new lightweight primitives and protocols. 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 and 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 lightweight cryptography standards. The draft requirements and evaluation criteria are available on the NIST Computer Security Resource Center Web site: https://csrc.nist.gov/Projects/Lightweight-Cryptography.

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 Federal Information Processing Standards. 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 A. Kimball,
Chief of Staff.

[FR Doc. 2018-10127 Filed: 5/11/2018 8:45 am; Publication Date: 5/14/2018]