



Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Announcing Request for Nominations for Lightweight Cryptographic Algorithms

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

ACTION: Notice.

SUMMARY: This notice solicits nominations from any interested party for candidate algorithms to be considered for lightweight cryptographic 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 on the NIST Computer Security Resource Center Web site at: <https://csrc.nist.gov/Projects/Lightweight-Cryptography>.

DATES: Proposals must be received on or before [INSERT DATE 180 DAYS AFTER DATE OF PUBLICATION IN FEDERAL REGISTER]. Further details are available at <https://csrc.nist.gov/Projects/Lightweight-Cryptography>.

ADDRESSES: Algorithm submission packages should be sent to Dr. Kerry McKay, Information Technology Laboratory, Attention: Lightweight 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: [lightweight-crypto@nist.gov](mailto:lightweight-crypto@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 <https://csrc.nist.gov/Projects/Lightweight-Cryptography> for complete submission instructions.

FOR FURTHER INFORMATION CONTACT: For general information, send email to [lightweight-crypto@nist.gov](mailto:lightweight-crypto@nist.gov). For questions related to a specific submission package, 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](mailto:kerry.mckay@nist.gov), or by telephone: (301) 975-4969.

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 increasingly common. The shift in focus from desktop computers to small devices brings a wide range of new security and privacy concerns. In many conventional cryptographic standards, 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.

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.

Previously, NIST solicited public comment on draft minimum acceptability requirements, submission requirements, and evaluation criteria for candidate algorithms (83 FR 22251, May 14, 2018). The comments received are posted at <https://csrc.nist.gov/Projects/Lightweight-Cryptography>, 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 lightweight candidate algorithms may now be submitted, up until the final deadline of [INSERT DATE 180 DAYS AFTER DATE OF PUBLICATION IN FEDERAL REGISTER]. Complete instructions on how to submit a candidate package, including the minimal acceptability requirements, are posted at <https://csrc.nist.gov/Projects/Lightweight-Cryptography>.

AUTHORITY: 15 U.S.C. 278g-3.

Kevin A. Kimball  
Chief of Staff

[FR Doc. 2018-18433 Filed: 8/24/2018 8:45 am; Publication Date: 8/27/2018]