Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Announcing Draft Federal Information Processing Standard (FIPS) 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, and Draft Revision of the Applicability Clause of FIPS 180-4, *Secure Hash Standard*, and Request for Comments

Docket No.: [130917811-3811-01]

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

ACTION: Notice; request for comments.

SUMMARY: The National Institute of Standards and Technology (NIST) launched a public competition in November 2007 to develop a new cryptographic hash algorithm for standardization to augment the Government standard hash algorithms specified in Federal Information Processing Standard (FIPS) 180, *Secure Hash Standard*. NIST announced the selection of KECCAK as the winning algorithm in a press release issued on October 2, 2012, which is available at http://www.nist.gov/itl/csd/sha-100212.cfm. Draft FIPS 202

specifies the new “Secure Hash Algorithm-3” (SHA-3) family of permutation-based functions based on KECCAK.

Four fixed-length cryptographic hash algorithms (SHA3-224, SHA3-256, SHA3-384, and SHA3-512) and two closely related, “extendable-output” functions (SHAKE128 and SHAKE256) are specified in Draft FIPS 202; all six algorithms are permutation-based “sponge” functions. The four SHA-3 hash functions provide alternatives to the SHA-2 family of hash functions. The extendable-output functions (XOFs) can be specialized to hash functions, subject to additional security considerations, or used in a variety of other applications. Hash algorithms are used in many information security applications, including 1) the generation and verification of digital signatures, 2) key-derivation functions, and 3) random bit generation.

Both FIPS 180-4 and Draft FIPS 202 specify cryptographic hash algorithms. FIPS 180-4 specifies SHA-1 and the SHA-2 family of hash functions, and mandates the use of one of these functions for Federal applications that require a cryptographic hash function. Draft FIPS 202 specifies the new SHA-3 family of hash and extendable-output functions. To allow the use of the functions specified in either FIPS 180-4 or Draft FIPS 202 for Federal applications that require a cryptographic hash function, NIST proposes revising the Applicability Clause (#6) of the Announcement Section of FIPS 180-4; the other sections of FIPS 180-4 remain unchanged. The *NIST Policy on Hash Functions*, available at http://csrc.nist.gov/groups/ST/hash/policy.html, provides guidance on the choice of hash functions for specific applications.

NIST invites public comments on Draft FIPS 202, which is available at http://csrc.nist.gov/publications/PubsDrafts.html, and on the proposed revision of the Applicability Clause of the Announcement Section of FIPS 180-4, available at http://csrc.nist.gov/publications/PubsFIPS.html. After the comment period closes, NIST will analyze the comments, make changes to the respective documents, as appropriate, and then propose Draft FIPS 202 and the revised FIPS 180-4 to the Secretary of Commerce for approval.

DATES: Comments on Draft FIPS 202 and the revised Applicability Clause of FIPS 180-4 must be received on or before [INSERT DATE 90 DAYS AFTER PUBLICATION OF THIS NOTICE IN THE FEDERAL REGISTER].

ADDRESSES: Comments on Draft FIPS 202 and the revised Applicability Clause of FIPS 180-4 may be sent electronically to *SHA3comments@nist.gov* with the relevant Subject line: "Comment on Draft FIPS 202," or "Comment on draft revision to the Applicability Clause of FIPS 180." Comments may also be sent by mail to: Chief, Computer Security Division, Information Technology Laboratory, ATTN: Comments on Draft FIPS 202 for SHA-3, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899–8930.

FOR FURTHER INFORMATION CONTACT: Ms. Shu-jen Chang (301) 975–2940, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899–8930, email: Shu-jen.Chang@nist.gov.

SUPPLEMENTARY INFORMATION: On November 2, 2007, NIST announced a Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA-3) Family in the Federal Register (72 FR 62212), which is available at https://federalregister.gov/a/E7-21581. The notice requested the submission of candidate hash algorithms for consideration in a public competition to select a new hash algorithm that would augment the Government standard hash algorithms specified in Federal Information Processing Standard (FIPS) 180, *Secure Hash Standard*. The competition was referred to as the SHA-3 Cryptographic Hash Algorithm Competition, or the SHA-3 Competition.

By October 31, 2008, NIST received sixty-four entries from cryptographers around the world. From these entries, NIST selected fifty-one first-round candidates in December 2008, fourteen second-round candidates in July 2009, and five finalists in December 2010. NIST summarized its decision in a report at the end of each round; NISTIR 7620 for the first round and NISTIR 7764 for the second round are available at http://csrc.nist.gov/publications/PubsNISTIRs.html.

Eighteen months were provided for the public review of the SHA-3 finalists.

The worldwide cryptographic community provided an enormous amount of analysis and public feedback on the candidates throughout the competition. NIST also hosted a SHA-3 candidate conference during each round of the competition to obtain public feedback.

After much careful study and consideration of the finalists and public comments, NIST announced the selection of KECCAK as the winner of the SHA-3 Cryptographic Hash Algorithm Competition in a press release on October 2, 2012. KECCAK is a family of permutation-based sponge functions that cryptographic hash functions and other applications can be built from. The press release is available at http://www.nist.gov/itl/csd/sha-100212.cfm, and a report explaining this selection (NISTIR 7896) is available at http://dx.doi.org/10.6028/NIST.IR.7896.

Request for Comments

NIST publishes this notice to solicit public comments on Draft FIPS 202. Draft FIPS 202 specifies the new SHA-3 family of permutation-based hash and extendable-output functions based on KECCAK. This algorithm is the core of the proposed SHA-3 Standard, but the standard does not standardize nor approve every variant that the KECCAK family of functions can support.

NIST strongly encourages the public to continue analyzing the security of the KECCAK family of permutation-based sponge functions in general, and the six algorithms specified in Draft FIPS 202 in particular, and to submit those analyses as official comments in response to this request. NIST invites public comments on Draft FIPS 202, which is available at http://csrc.nist.gov/publications/PubsDrafts.html. Such analyses and other comments received will be considered by NIST in preparing the final version of FIPS 202.

NIST also invites public comments on the revised Applicability Clause in the Announcement Section of FIPS 180-4; the revision would permit compliance with FIPS 202 in lieu of FIPS 180-4 for Federal applications when a cryptographic hash function is called for. Public comments received in response to this request will be posted regularly at http://csrc.nist.gov/groups/ST/hash/sha-3/sha-3_standardization.html.

NIST reminds all interested parties that the SHA-3 development effort was conducted as an open standards-setting activity. NIST requests that all interested parties inform NIST of any patents or inventions that may be required for the use of Draft FIPS 202 algorithms. This includes comments from all parties regarding specific claims that the use of Draft FIPS 202 algorithms infringes on their patent(s). Claims regarding the infringement of copyrighted software are also solicited. NIST views this input as a critical factor in the eventual widespread adoption and implementation of Draft FIPS 202. All comments received by the deadline will be made publicly available at http://csrc.nist.gov/groups/ST/hash/sha-3/sha-3_standardization.html without change or redaction. Therefore, comments should not include proprietary or confidential information.

To encourage on-going discussions related to the SHA-3 standardization effort, NIST will continue to maintain its SHA-3 electronic discussion forum at *hash-forum@nist.gov.* Please note that comments sent to this list will NOT be considered ‘‘official’’ comments; to be considered “official,” a comment must be submitted as described above in the ADDRESSES section of this Notice.

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.

E.O. 12866: This notice has been determined not to be significant for the purposes of E.O. 12866.

Dated: May 21, 2014.

Willie E. May
Associate Director for Laboratory Programs

[FR Doc. 2014-12336 Filed 05/27/2014 at 8:45 am; Publication Date: 05/28/2014]