ode: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Proposed Withdrawal of Federal Information Processing Standards (FIPS) 198-1, The Keyed-Hash Message Authentication Code (HMAC)

AGENCY: National Institute of Standards and Technology, Department of Commerce.

ACTION: Notice; request for comments.

SUMMARY: The National Institute of Standards and Technology (NIST) proposes to withdraw FIPS 198-1, the Keyed-Hash Message Authentication Code (HMAC), from the FIPS series. Prior to the submission of this proposed withdrawal of FIPS 198-1 to the Secretary of Commerce for review and approval, NIST invites comments from the public, users, the information technology industry, and Federal, State, and local governments, and government organizations concerning the withdrawal of this FIPS.

DATES: Comments on the proposed withdrawal of this FIPS must be received no later than 11:59 pm EDT on **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].**

ADDRESSES: Written comments concerning the withdrawal of FIPS 198-1 should be sent to: Crypto Publication Review Board, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899-8930, ATTN: FIPS 198-1 Comments.

Electronic comments should be sent to: cryptopubreviewboard@nist.gov.

Information about the FIPS is available on the NIST web page https://csrc.nist.gov/pubs/fips/198-1/final.

Comments received in response to this notice will be published electronically on that page without change or redaction, so commenters should not include information they do not wish to be posted (e.g. personal or confidential business information).

FOR FURTHER INFORMATION CONTACT: Morris Dworkin, NIST, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899-8930, cryptopubreviewboard@nist.gov, (301) 975-2354.

SUPPLEMENTARY INFORMATION:

FIPS 198-1 is being proposed for withdrawal from the FIPS series because the content is more suitable in a NIST Special Publication (SP) and outdated. Specifically, a) it describes a cryptographic scheme, instead of a fundamental cryptographic primitive, and b) the HMAC specification needs to be updated to include block sizes to support the SHA-3 family of hash functions defined in FIPS 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions.

Subsequent to the issuance of FIPS 198-1 in 2008, NIST developed NIST Internal Report (IR) 7977, NIST Cryptographic Standards and Guidelines Development Process (March 2016), available at https://csrc.nist.gov/pubs/ir/7977/final. Under NIST IR 7977, NIST typically specifies fundamental cryptographic primitives—block ciphers, digital signature algorithms, and hash functions—as FIPS publications, whereas other cryptographic schemes—modes of operation, key management, message authentication codes, etc.—are published as a part of the NIST SP 800 "Computer Security" series. For more information, see Section 3 of NIST IR 7977. As FIPS 198-1 describes HMAC, a message authentication code, NIST proposes to move this specification to an SP 800 publication and withdraw FIPS 198-1 to be consistent with the approach in NIST IR 7977.

Additionally, the HMAC specification needs updating to include larger block sizes to support the SHA-3 family of hash functions specified in FIPS 202. A discussion of truncation, an editorial

refresh, and updated references are also needed and have been implemented in NIST SP 800-224, as further described below.

In August 2021, NIST's Crypto Publication Review Board (CPRB) initiated a review process for FIPS 198-1 (published in 2008) and received public comments. In September 2022, CPRB proposed converting FIPS 198-1 to a NIST SP and received additional comments on that proposed decision. The public comments received during these comment periods are available at https://csrc.nist.gov/projects/crypto-publication-review-project/completed-reviews#fips198-1. In November 2022, NIST announced its intention to develop NIST SP 800-224, with a proposed plan to withdraw FIPS 198-1 after the new SP is published.

A draft of NIST SP 800-224, Keyed-Hash Message Authentication Code (HMAC): Specification of HMAC and Recommendation for Message Authentication, was released for public comment from June 28, 2024, to September 6, 2024. A copy of the draft and a compilation of comments received are posted at https://csrc.nist.gov/pubs/sp/800/224/ipd. NIST prepared a final version of SP 800-224, which was cleared for publication in March 2025, and this notice follows.

Should the Secretary of Commerce approve the withdrawal of this FIPS, NIST will keep references to the withdrawn FIPS on its FIPS web pages and will link to current versions of these standards and specifications where appropriate.

Withdrawal means that federal agencies will no longer be required to comply with this FIPS. NIST will continue to provide relevant information on standards and guidelines by means of electronic dissemination methods.

(Authority: 40 U.S.C. 11331(f), 15 U.S.C. 278g-3.)

Alicia Chambers,

NIST Executive Secretariat.

[FR Doc. 2025-11497 Filed: 6/20/2025 8:45 am; Publication Date: 6/23/2025]