DEPARTMENT OF COMMERCE

National Institutes of Standards and Technology

[Docket No. 001214352–0352–01]

RIN 0693–AB34

Announcing Draft Federal Information Processing Standards (FIPS) 180–2, Secure Hash Standard, and Request for Comments

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

ACTION: Notice, request for comments.

SUMMARY: This notice announces Draft Federal Information Processing Standard (FIPS) 180–2, Secure Hash Standard (SHS), for public review and comment. The draft standard, designated ''Draft FIPS 180–2,'' is proposed to supersede FIPS 180–1.

Published in 1992, FIPS 180–1 specified that the standard be reviewed within five years. The standard specifies a secure hash algorithm, designated SHA–1, which produces a 160-bit output called a message digest. To provide for comparability with the anticipated increase in security to be afforded by the use of the Advanced Encryption Standard (currently under development), NIST is proposing the expansion of the hash standard to include additional algorithms that produce a 256-bit, 384-bit, and 512-bit message digest. The proposed standard is available at http://www.nist.gov/sha.

Prior to the submission of this proposed standard to the Secretary of Commerce for review and approval, it is essential that consideration is given to the needs and views of the public, users, the information technology industry, and Federal, State, and local government organizations. The purpose of this notice is to solicit such views.

DATES: Comments must be received on or before August 28, 20001.

ADDRESSES: Written comments may be sent to: Chief, Computer Security Division, Information Technology Laboratory, Attention: Comments on Draft FIPS 180–2, 100 Bureau Drive, Stop 8930, National Institute of Standards and Technology, Gaithersburg, MD 20899–8930.

Electronic Comments may be sent to: Proposed 180–2@nist.gov.

The current FIPS 180–1 and its proposed replacement, Draft FIPS 180–2, are available electronically at http://www.nist.gov/sha.

Comments received in response to this notice will be published electronically at http://www.nist.gov/sha.

FOR FURTHER INFORMATION CONTACT: Elaine Barker, Computer Security Division, National Institutes of Standards and Technology, Gaithersburg, MD 20899–8930, telephone (301) 975–2911, e-mail: elaine.barker@nist.gov.

SUPPLEMENTARY INFORMATION: FIPS 180–1, Secure Hash Standard, issued in 1995, specifies a secure has algorithm, designated SHA–1, for computing a condensed representation of a message or a data file. When a data is input, the SHA–1 produces a 160-bit output called a message digest. The message digest can then be used as input to a digital signature algorithm that generates or verifies the digital signature for a message. Other uses of a message digest include the generation of random numbers and keyed hash message authentication codes.

As technology advances, the input parameters used by signature algorithms must be increased to provide adequate security. One of these inputs is the message digest. Therefore, as part of the five-year review of the hash standard, Draft FIPS 180–2 proposed additional has algorithms with outputs of 256-bit, 384-bit and 512-bits. The additional algorithms will produce outputs that will provide security comparable to that projected for the Advanced Encryption Standard.

Authority: NIST's activities to develop computer security standards to protect Federal sensitive (unclassified) systems are undertaken pursuant to specific responsibilities assigned to NIST in Section 5131 of the Information Technology Management Reform Act of 1996 (P.L. 104–106), the Computer Security Act of 1987 (P.L. 100–235), and Appendix III to Office of Management and Budget Circular A–130.

Executive Order 12866: This notice has been determined to be non-significant for the purposes of Executive Order 12866.

Dated: May 21, 2001.

Karen H. Brown,

Acting Director, NIST.

[FR Doc. 01–13522 Filed 5–29–01; 8:45 am]

BILLING CODE 3510–CN–M

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[I.D. 050701A]

Small Takes of Marine Mammals Incidental to Specified Activities; Shallow-Water Hazard Activities in the Beaufort Sea

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice of receipt of application and proposed authorization for a small take exemption; request for comments.

SUMMARY: NMFS has received a request from BP Exploration (Alaska), Inc; ExxonMobil Production Co, a division of Exxon Mobil Corporation; and Phillips Alaska, Inc. (BP/EM/PAI), working as members of a study team referred to in their application as the North American Natural Gas Pipeline Group (NANGPG), for an authorization to take small numbers of marine mammals by harassment incidental to conducting shallow hazard surveys in the central and eastern Alaskan Beaufort Sea. Under the Marine Mammal Protection Act (MMPA), NMFS is requesting comments on its proposal to authorize BP/EM/PAI to incidentally take, by harassment, small numbers of bowhead whales and other marine mammals in the U.S. Beaufort Sea during the open water period of 2001.

DATES: Comments and information must be received no later than June 29, 2001.

ADDRESSES: Comments on the application should be addressed to Donna Wieting, Chief, Marine Mammal Conservation Division, Office of Protected Resources, NMFS, 1315 East-West Highway, Silver Spring, MD 20910–3225. A copy of the application, and a list of references used in this document may be obtained by writing to this address or by telephoning one of the contacts listed here.

FOR FURTHER INFORMATION CONTACT: Kenneth R. Hollingshead, (301) 713–2055, ext 128; Brad Smith, (907) 271–5006.

SUPPLEMENTARY INFORMATION:

Background

Sections 101(a)(5)(A) and (D) of the MMPA (16 U.S.C. 1361 et seq.) direct the Secretary of Commerce to allow, upon request, the incidental, but not intentional taking of small numbers of marine mammals by U.S. citizens who engage in a specified activity (other than commercial fishing) within a specified