DES encrypted ciphertext by trying all possible keys) has become increasingly more feasible with technology advances. Following a recent hardware based DES key exhaustion attack, NIST can no longer support the use of single DES for many applications. Therefore, Government agencies with legacy single DES systems are encouraged to transition to Triple DES. Agencies are advised to implement Triple DES when building new systems.

16. Comments. Comments and suggestions regarding this standard and its use are welcomed and should be addressed to the National Institute of Standards and Technology, Attn: Director, Information Technology Laboratory, Gaithersburg, MD 20899.

17. Waiver Procedure. Under certain exceptional circumstances, the heads of Federal departments and agencies may approve waivers to Federal Information Processing Standards (FIPS). The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of Title 44, United States Code. Waiver shall be granted only when:

a. Compliance with standard would adversely affect the accomplishment of the mission of an operator of a Federal computer system; or

b. Compliance with a standard would cause a major adverse financial impact on the operator which is not offset by Government-wide savings.

Agency heads may act upon a written waiver request containing the information detailed above. Agency heads may also act without a written waiver request when they determine that conditions for meeting the standard cannot be met. Agency heads may approve waivers only by a written decision which explains the basis on which the agency head made the required finding(s). A copy of each decision, with procurement sensitive or classified portions clearly identified, shall be sent to: National Institute of Standards and Technology; ATTN: FIPS Waiver Decisions 100 Bureau Drive, Stop 8970, Gaithersburg, MD 20899–8970.

In addition, notice of each waiver granted and each delegation of authority to approve waivers shall be sent promptly to the Committee on Government Operations of the House of Representatives and the Committee on Government Affairs of the Senate and shall be published promptly in the **Federal Register.**

When the determination on a waiver applies to the procurement of equipment and/or services, a notice of the waiver determination must be published in the Commerce Business Daily as a part of the notice of solicitation for offers of an acquisition or, if the waiver determination is made after that notice is published, by amendment to such notice.

A copy of the waiver, any supporting documents, the document approving the waiver an any accompanying documents, with such deletions as the agency is authorized and decides to make under 5 United States Code Section 552(b), shall be part of the procurement documentation and retained by the agency.

18. Special Information. In accordance with the Qualifications Section of this standard, review of this standard have been conducted every 5 years since its adoption in 1977. The standard was reaffirmed during each of those reviews. This revision to the text of the standard contains changes which allow software implementations of the algorithm, permit the use of other FIPS approved cryptographic algorithms, and designate Triple DES (i.e., TDEA) as a FIPS approved cryptographic algorithm.

19. Where to Obtain Copies of the Standard. Copies of this publication are for sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. When ordering, refer to Federal Information Processing Standards Publication 46–3 (FIPSPUB46–3), and identify the title. When microfiche is desired, this should be specified. Prices are published by NTIS in current catalogs and other issuances. Payment may be made by check, money order, deposit account or charged to a credit card accepted by NTIS.

(Note that the technical specifications of the DES encryption algorithm are not reproduced in this **Federal Register** Notice. They are available in FIPS 46–2 and the draft of FIPS 46–3. No technical changes are being proposed in the DES algorithm itself from the specifications in FIPS 46–2.)

Triple Data Encryption Algorithm

Let $E_K(I)$ and $D_K(I)$ represent the DEA encryption and decryption of I using DEA key K respectively. Each TDEA encryption/decryption operation (as specified in ANSI X9.52) is a compound operation of DEA encryption and decryption operations. The following operations are used:

1. TDEA encryption operation: the transformation of a 64-bit block I into a 64-bit block) that is defined as follows: $O=E_{K3}(D_{K2}(E_{K1}(I)))$

2. TDEA decryption operation: the transformation of a 64-bit block I into a 64-bit block O that is defined as follows: $O = D_{K1}(E_{K2}(D_{K3}(I)))$

The standard species the following keying options for bundle (K_1, K_2, K_3)

1. Keying Option 1: K_1, K_2 and K_3 are independent keys;

2. Keying option 2: K_1 and K_2 and independent keys and $K_3 = K_1$;

3. Keying Option 3: $K_1 = K_2 = K_3$.

A TDEA mode of operation is backward compatible with its single DEA counterpart if, with compatible keying options for TDEA operation,

1. An encrypted plaintext computed using a single DEA mode of operation can be decrypted correctly by a corresponding TDEA mode of operation; and

2. An encrypted plaintext computed using a TDEA mode of operation can be decrypted correctly by a corresponding single DEA mode of operation.

When using keying Option 3 ($K_1 = K_2 = K_3$), TECB, TCBC, TCFB, amd TOFB modes are backward compatible with single DEA modes of operation ECB, CBC, CFB, OFB respectively.

The diagram in Appendix 2 illustrates TDEA encryption an TDEA decrytion.

(Note that the two appendices to FIPS 46–3 are not reproduced in this **Federal Register** notice. They are available in the complete draft of FIPS 46–3.)

Dated: January 8, 1999.

Robert E. Hebner,

Acting Deputy Director.

[FR Doc. 99–898 Filed 1–14–99; 8:45 am]

BILLING CODE 3510–CN–M

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Announcement of Meeting of National Conference on Weights and Measures

AGENCY: National Institute of Standards and Technology.

ACTION: Notice of meeting.

SUMMARY: Notice is hereby given that the Interim Meeting of the National Conference on Weights and Measures will be held January 31 through February 4, 1999, at the Sheraton Old Town Hotel, Albuquerque, New Mexico. The meeting is open to the public.

The National Conference on Weights and Measures is an organization of weights and measures enforcement officials of the States, counties, and cities of the United States, and private sector representatives. The interim meeting of the conference, as well as the annual meeting to be held next July (a notice will be published in the **Federal Register** prior to such meeting), brings together enforcement officials, other government officials, and representatives of business, industry, trade associations, and consumer

organizations to discuss subjects that relate to the field of weights and measures technology and administration.

Pursuant to 15 U.S.C. 272 B, the National Institute of Standards and Technology acts as a sponsor of the National Conference on Weights and Measures in order to promote uniformity among the States in the complex of laws, regulations, methods, and testing equipment that comprises regulatory control by the States of commercial weighing and measuring.

DATES: The meeting will be held January 31–February 4, 1999, 8:00 a.m.–5:00 p.m.

LOCATION OF MEETING: Sheraton Old Town Hotel, 800 Rio Grande Boulevard, N.W., Albuquerque, New Mexico 878104.

FOR FURTHER INFORMATION CONTACT: Dr. Gilbert Ugiansky, Chief, NIST, Office of Weights and Measures, 100 Bureau Drive Stop 2350 Gaithersburg, Maryland 20899–2350. Telephone: (301) 975–4004, or E-mail: owm@nist.gov.

Dated: January 8, 1999.

Robert E. Hebner,

Acting Deputy Director.

[FR Doc. 99–899 Filed 1–14–99; 8:45 am]

BILLING CODE 3510–13–M

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[I.D. 011199C]

Endangered and Threatened Species; Request for Information on Candidate Species List Under the Endangered Species Act

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

ACTION: Request for information for revision of candidate species list.

SUMMARY: NMFS solicits information on marine and anadromous species that may qualify as candidates for possible addition to the List of Endangered and Threatened Species, including information on the status of species currently classified as candidate species. This notice is not a proposal for listing; candidate species do not receive substantive or procedural protection under the Endangered Species Act of 1973 (ESA). The goal of the candidate species program is to identify marine and anadromous species as candidates for possible addition to the List of Endangered and Threatened Species and encourage voluntary efforts to help prevent listings.

DATES: Comments will be accepted until April 15, 1999.

ADDRESSES: Comments and documentation for these and any recommended additions or deletions to the candidate species list should be sent to Chief, Endangered Species Division, Office of Protected Resources, NMFS, 1315 East-West Highway, Silver Spring, MD 20910.

FOR FURTHER INFORMATION CONTACT: Marta Nammack or Terri Jordan at (301)713–1401.

SUPPLEMENTARY INFORMATION: The ESA requires determinations of whether species of wildlife and plants are endangered or threatened, based on the best available scientific and commercial data. ''Species'' includes any species or subspecies of fish, wildlife, or plant, and any distinct population segment of any vertebrate species that interbreeds when mature (vertebrate population). NMFS and the U.S. Fish and Wildlife Service share responsibilities under the ESA. With some exceptions, NMFS is responsible for species that reside all or the major portion of their lifetime in marine or estuarine waters. The regulations implementing Section 4 of the ESA (49 FR 38900, October 1, 1984) define ''candidate'' as ''any species being considered by the Secretary for listing as an endangered or a threatened species, but not yet the subject of a proposed rule.''

The four main purposes of the candidate species list are to (1) Increase public awareness about these species; (2) identify those species that may be in need of protective measures under the ESA, and if possible, recover them before listing under the ESA becomes necessary; (3) stimulate voluntary conservation efforts by Federal agencies and other appropriate parties with regard to these species; and (4) identify uncertainties associated with the status of the species. As resources permit, NMFS conducts a review of the status of each candidate species to determine if it warrants listing as endangered or threatened under the ESA. Sometimes, even though NMFS may determine after conducting a status review that a species does not warrant listing under the ESA, NMFS may retain the species on the candidate species list due to remaining concerns or uncertainties. NMFS believes it is important to highlight species for which listing may be warranted so that Federal and state agencies, Native American tribes, and the private sector are aware of which species could benefit from proactive conservation efforts. Agencies and other appropriate parties can take candidate species into account in project planning, which may lower the likelihood of an ESA listing.

NMFS has developed specific criteria for determining which species/vertebrate populations should be included on the NMFS candidate species list. These criteria are based on the requirement for reliable information on the biological status of a species or vertebrate population.

Biological status is determined by both demography and genetic composition of the species/vertebrate population. If there is evidence of demographic or genetic concerns that would indicate that listing may be warranted, the species/vertebrate population should be added to the candidate species list. Demographic concerns would occur when there is a significant decline in abundance or range from historical levels that would indicate that listing may be warranted. This could result from activities such as over-harvest, habitat degradation, disease outbreaks, predation, natural climatic conditions, and hatchery operations that negatively impact natural stocks. Genetic concerns that would indicate that listing may be warranted include outbreeding and inbreeding depression resulting from poor hatchery practices or substantially reduced numbers of natural individuals.

If you wish to propose that a species/vertebrate population be designated as a candidate species, please submit available information, including: (1) Taxonomic validity of the species, subspecies or vertebrate population; (2) life history; (3) historic and current population size and distribution; (4) assessment of confirmed and likely threats and declines; (5) existing laws, regulations, agreements and other protective mechanisms; and (6) documentation of information used to justify their proposal.

The previous list was published on July 14, 1997, (62 FR 37560). NMFS intends to consider the results of ongoing status reviews and all data received in response to this notice to make appropriate amendments to the list. Some of the species NMFS is considering adding to the candidate species list are the largetooth sawfish (*Pristis pristis*), smalltooth sawfish (*Pristis pectinata*), barndoor skate (*Raja laevis*), elkhorn coral (*Acropora palmata*), staghorn coral (*Acropora cervicornis*), and four gastropods that are possibly extinct: ''*Collisella*'' *edmitchelli*, *Lottia alveus alveus*, *Cerithidea fuscata*, and *Phyllaplysia smaragda*.

It is important to note that the candidate species list is limited by the information available. Therefore, it does