All meetings are accessible to persons with disabilities. Sign language interpreters and an assistive listening system are available at all meetings.

David Capozzi,

Director, Office of Technical and Information Services.

[FR Doc. 96–33125 Filed 12–31–96; 8:45 am]

BILLING CODE 8150–01–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 960924272–6272–01]

RIN 0693–ZA13

Announcing Development of a Federal Information Processing Standard for Advanced Encryption Standard

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

ACTION: Notice; Request for comments.

SUMMARY: A process to develop a Federal Information Processing Standard (FIPS) for Advanced Encryption Standard (AES) incorporating an Advanced Encryption Algorithm (AEA) is being initiated by the National Institute of Standards and Technology (NIST). As the first step in this process, draft minimum acceptability requirements and draft criteria to evaluate candidate algorithms are being published for comment. Also announced for comment are draft submission requirements. An open, public workshop on the draft minimum acceptability requirements, evaluation criteria and submission requirements has also been scheduled. It is intended that the AES will specify an unclassified, publicly disclosed encryption algorithm capable of protecting sensitive government information well into the next century.

The purpose of this notice is to solicit views from the public, manufacturers, voluntary standards organizations, and Federal, state, and local government users so that their needs can be considered in the process of developing the AES.

DATES: Comments must be received on or before April 2, 1997.

The AES Evaluation Criteria/Submission Requirements Workshop will be held on April 15, 1997, from 9:00 a.m. to 4:00 p.m.

ADDRESSES: Written comments should be sent to Director, Computer Systems Laboratory, Attn: FIPS for AES Comments, Technology Building, Room A231, National Institute of Standards and Technology, Gaithersburg, MD 20899.

Electronic comments may be sent to AES@nist.gov.

Comments received in response to this notice will be made part of the public record and will be made available for inspection and copying in the Central Records and Reference Inspection Facility, Room 6020, Herbert C. Hoover Building, 14th Street between Pennsylvania and Constitution Avenues, NW, Washington, DC, 20230.

The AES Criteria Workshop will be held at the Green Auditorium, Administration Building, National Institute of Standards and Technology, Gaithersburg, Maryland. Copies of the comments submitted will be available at the Workshop. For planning purposes, advance registration is encouraged. To register, please fax your name, address, telephone, fax and e-mail address to 301–948–1233 (Attn: AES Criteria Workshop) by April 10, 1997. Registration will also be available at the door. The workshop will be open to the public.

FOR FURTHER INFORMATION CONTACT: Edward Roback, National Institute of Standards and Technology, Building 820, Room 426, Gaithersburg, MD 20899; telephone 301–975–3696 or via fax at 301–948–1233. Technical inquiries regarding the proposed draft evaluation criteria and draft submission requirements should be addressed to Miles Smid, National Institute of Standards and Technology, Building 820, Room 426, Gaithersburg, MD 20899; telephone 301–975–2938 or via fax at 301–948–1233.

SUPPLEMENTARY INFORMATION: This work effort is being initiated pursuant to NIST's responsibilities under the Computer Security Act of 1987, the Information Technology Management Reform Act of 1996, Executive Order 13011, and OMB Circular A–130.

NIST recognizes that many institutions, both within and outside the Federal Government, have considerable investments in their current installed base of encryption equipment implementing the Data Encryption Algorithm, specified in the Data Encryption Standard (DES, Federal Information Processing Standard 46–2). DES was first approved in 1977 and was most recently reaffirmed by the Secretary in 1993, until December 1998. In 1993 the following statement was included in the standard:

''At the next review (1998), the algorithm specified in this standard will be over twenty years old. NIST will consider alternatives which offer a higher level of security. One of these alternatives may be proposed as a replacement standard at the 1998 review.''

It is NIST's review that a multi-year transition period will be necessary to move toward any new encryption standard and that DES will continue to be of sufficient strength for many applications. NIST will consult with all interested parties so that a smooth transition can be accomplished.

In order to provide a basis for the evaluation of encryption algorithms submitted to be considered as the AEA for incorporation into the FIPS for AES, evaluation criteria will be used to review submitted algorithms. Comments on the draft criteria (and, at the appropriate time, or candidate algorithms) from voluntary consensus standards organizations are particularly encouraged.

Proposed Draft Minimum Acceptability Requirements and Evaluation Criteria

The draft minimum acceptability requirements and evaluation criteria are:

A.1 AES shall be publicly defined.

A.2 AES shall be a symmetric block cipher.

A.3 AES shall be designed so that the key length may be increased as needed.

A.4 AES shall be implementable in both hardware and software.

A.5 AES shall either be (a) freely available or (b) available under terms consistent with the American National Standards Institute (ANSI) patent policy.

A.6 Algorithms which meet the above requirements will be judged based on the following factors:

(a) Security (i.e., the effort required to cryptanalyze),

(b) Computational efficiency,

(c) Memory requirements,

(d) Hardware and software suitability,

(e) Simplicity,

(f) Flexibility, and

(g) Licensing requirements.

Comments are being sought on these draft minimum acceptability criteria and evaluation criteria, suggestions for other criteria, and relative importance of each individual criterion in the evaluation process. Criteria will be finalized by NIST following the criteria workshop.

Proposed Draft Submission Requirements

In order to provide for an orderly, fair, and timely evaluation of candidate algorithm proposals, submission requirements will specify the procedures and supporting documentation necessary to submit a candidate algorithm.

B.1 A complete written specification of the algorithm including all necessary mathematical equations, tables, and parameters needed to implement the algorithm.

B.2 Software implementation and source code, in ANSI C code, which will compile on a personal computer. This code will be used to compare software performance and memory requirements with respect to other algorithms.

B.3 Statement of estimated computational efficiency in hardware and software.

B.4 Encryption example mapping a specified plaintext value into ciphertext.

B.5 Statement of licensing requirements and patents which may be infringed by implementations of this algorithm.

B.6 An analysis of the algorithm with respect to known attacks.

B.7 Statement of advantages and limitations of the submitted algorithm.

(end of draft submission requirements)

Since both the evaluation criteria and submission requirements have not yet been set, candidate algorithms should NOT be submitted at this time.

Dated: December 16, 1996.

Samuel Kramer,

Associate Director.

[FR Doc. 96–32494 Filed 12–31–96; 8:45 am]

BILLING CODE 3510–CN–M

National Oceanic and Atmospheric Administration

[Docket No. 960322092–6367–04; I.D. 122696A]

RIN 0648–ZA19

Gulf of Mexico Sustainable Fisheries Program

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

ACTION: Notice; request for comments.

SUMMARY: Pursuant to the Interjurisdictional Fisheries Act of 1986 (IFA), the Secretary of Commerce (Secretary) declared fishery resource disasters in the Northeast, Northwest, and the Gulf of Mexico (Gulf) on August 2, 1995. Emergency aid totaling $15 million was made available for the Gulf, $5 million of which has been committed for financial assistance to commercial fishermen who suffered uninsured fishing vessel or gear damage or loss caused by hurricanes, floods, or their aftereffects that occurred from August 22, 1992, through December 31, 1995. NMFS now proposes to allocate the remaining $10 million to the five Gulf states' fisheries resources agencies for projects or other measures designed to alleviate the long-term effects of the disasters on the Gulf's fishery resources and associated habitat. Pursuant to the IFA, NMFS must provide notice and an opportunity for public comment on any terms, limitations, and conditions that are established as prerequisites for receiving IFA Federal assistance funds. This notice describes those terms, limitations, and conditions, and requests public comment.

DATES: Comments must be submitted on or before January 30, 1997.

ADDRESSES: Comments regarding this proposed program should be sent to the National Marine Fisheries Service, Southeast Region, 9721 Executive Center Drive, St. Petersburg, FL 33702–2432.

FOR FURTHER INFORMATION CONTACT: Buck Sutter, (813) 570–5324.

SUPPLEMENTARY INFORMATION:

Background

On August 2, 1995, the Secretary declared fishery resource disasters in the Pacific Northwest, New England, and the Gulf. With respect to the Gulf, the Secretary's disaster declaration (Declaration) cited multiple impacts. Non-point source nutrients and debris entering the Gulf as a result of the Mississippi River floods in 1993 and 1994 caused severe hypoxia, a condition where the excess nutrients react to deplete the water of necessary oxygen, which spread to massive areas in the Gulf and threatened marine life and coastal resources. The flood debris created underwater hazards for commercial fishermen who suffered damaged or lost gear and vessels. In addition, the Secretary cited hurricanes that harmed fisheries habitat and engendered substantial economic damage and social disruption. Because of these impacts, the Secretary made $15 million available for the Gulf of Mexico for disaster relief.

On June 10, 1996, NMFS published a final notice describing the Gulf of Mexico Fisheries Disaster Program (FDP), which committed up to $5 million of the available $15 million for direct grants to commercial fishermen who suffered uninsured fishing vessel or gear damage or loss caused by the hurricanes, floods, or their aftereffects (61 FR 29350, June 10, 1996; 61 FR 55132, Oct. 24, 1996).

Section 308(d) of the IFA allows the Secretary to help persons engaged in commercial fisheries by providing assistance indirectly through state and local government agencies. Therefore, the Secretary proposes to use the remaining $10 million in Gulf disaster assistance for projects or other measures to alleviate the long-term impacts on Gulf fishery resources and associated habitat from conditions cited in the August 2, 1995, Declaration. Because the impacts varied from state to state, a determination has been made to provide this assistance through the five Gulf state fisheries resources agencies, as they are in the best position to determine how the funds can be used.

This notice proposes the criteria that will be used by NOAA to fund state disaster assistance proposals and provides opportunity for public comment. NMFS will publish a final notice that will address public comments submitted on this notice and establish the final criteria for the state grants. States will also be notified and required to comply with all existing Federal assistance requirements. Once NMFS determines that a state's proposal(s) complies with all applicable terms, limitations, and conditions, NMFS will enter into a financial assistance agreement with that state for the administration of each project.

After consultations with appropriate state officials and review of available information regarding the impacts of disasters that occurred from August 23, 1992, through December 31, 1995, NMFS has decided upon the following apportionment of funds: Alabama—$1 million; Florida—$2.25 million; Louisiana—$4.5 million; Mississippi—$1 million; and Texas—$1.25 million.

I. Criteria

In order to be considered for funding, a state proposal must adhere to the following criteria:

1. The proposed project(s) must be consistent with the original intent of the Secretary's disaster declaration and the IFA (i.e., each project must address conditions resulting from nutrients and debris entering the Gulf as a result of floods and/or hurricanes or hurricane-strength storms from August 23, 1992, through December 31, 1995).

2. Projects must address the long-term benefit of the fishery resource and associated habitat and must seek to create healthy, sustainable fisheries in the Gulf of Mexico.

3. Projects must not duplicate existing Federal, state, or local projects. However, they may augment or allow the maintenance of effort of existing projects, provided that those projects are consistent with all other criteria. In other words, separate funds may be used to maintain existing projects.

4. Projects that primarily involve new data collection must show a clear relationship between that project and