7. Miscellaneous

This section is intended to address some of the questions/comments raised in the review of the draft evaluation criteria.

When evaluating algorithms, NIST will make every effort to obtain public input and will encourage review of the candidate algorithms by outside organizations; however, the final decision as to which algorithms(s) will be proposed to the Secretary of Commerce for inclusion in the AES is the responsibility of NIST.

NIST intends to develop a validation program for AES conformance testing, with the goal of having it operational concurrently with the effective date of the AES.

NIST does NOT have a fixed timeable for completion of the AES.

NIST is not specifically seeking a stream cipher algorithm, since any block cipher algorithm can be operated in a stream cipher mode.

NIST does not intend to select a wholly distinct algorithm for each of the minimum required key-block combinations. It is strongly recommended that no submission be so constructed.

NIST does not wish to target a specific application or platform for implementing the AES, as the evaluation of candidate algorithms takes place. However, one factor that is being taken into consideration for each candidate algorithm is its flexibility—the ability to implement the algorithm securely and efficiently in a wide variety of platforms and applications (see ''Algorithm and Implementation Characteristics'' under ''Evaluation Criteria'' section).

NIST does not intend to select a ''backup'' AES algorithm. Rather, should the circumstances arise (e.g., discovery of a significant security flaw) which could not be satisfactorily addressed by modifying the AES, NIST would likely look to the other AES candidate finalists. Additionally, if a significant period of time has elapsed since the AES selection, it would also make sense to examine other algorithms which may have been developed in the intervening period.

Exportability decisions regarding submissions and, eventually, products implementing AES will be made by the appropriate government regulatory authorities. NIST is a non-regulatory agency of the U.S. Department of Commerce.

NIST does not intend to offer financial incentives (e.g., contests) for cryptanalysis of AES candidates.

Should no appropriate algorithms be submitted in response to this call, NIST expressly reserves the right to cease this process and examine other possible courses of action.

Submitters are strongly encouraged to submit only one algorithm each (presumably the one in which the submitter has the greatest confidence). Submission of similar, yet distinct, algorithms may delay the public evaluation process and may well raise public questions as to the submitter's level of confidence in his/her candidates.

For conference and resource allocation planning purposes, it would be appreciated if those planning to submit candidates could notify the individuals listed in the ''For Further Information'' section as soon as possible.

Appreciation

NIST extends its appreciation to all submitters and those providing public comments during the AES development process.

Dated: September 8, 1997.

Elaine Bunten-Mines,

Director, Program Office.

[FR Doc. 97–24214 Filed 9–11–97; 8:45 am]

BILLING CODE 3510–CN–M

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[I.D. 080697D]

Request for Nomination of Individuals for the Federal Investment Task Force (Deadline Extension)

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

ACTION: Notice of request for nominations deadline extension.

SUMMARY: The Sustainable Fisheries Act (SFA) requires the Secretary of Commerce (Secretary) to establish a task force to study the role of the Federal Government in subsidizing fleet capacity and influencing capital investment in fisheries. NMFS is extending the deadline for nominations of qualified individuals to serve on the task force.

DATES: Nominations will now be accepted through October 1, 1997.

ADDRESSES: Nominations should be sent to Atlantic States Marine Fisheries Commission, 1444 Eye Street, NW, 6th Floor, Washington, DC 20005, ATTN: Federal Investment Task Force. Nominations may be submitted by fax, (202) 289–6051

FOR FURTHER INFORMATION CONTACT: Robert Beal, Atlantic States Marine Fisheries Commission, (202) 289–6400.

SUPPLEMENTARY INFORMATION: The Secretary is establishing a task force of interested parties to study the role of the Federal Government in (1) subsidizing the expansion and contraction of fishing capacity in fishing fleets the Magnuson-Stevens Fishery Conservation and Management Act, and (2) otherwise influencing the aggregate capital investment in fisheries. The original request for nominations was published in the **Federal Register** at Vol. 62, No. 167/Thursday August 28, 1997, page 45628. However, in order to allow sufficient time for all interested parties to submit nominations, the deadline for submission has been extended through October 1, 1997. The procedures and guidelines for submitting nominations can be found in the original **Federal Register** notice.

Please note: The task force is now tentatively scheduled to meet five times between November 1997 and June 1997.

Dated: September 8, 1997.

David L. Evans,

Deputy Assistant Administrator for Fisheries, National Marine Fisheries Service.

[FR Doc. 97–24263 Filed 9–9–97; 3:19 pm]

BILLING CODE 3510–22–F

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[I.D. 090497A]

Spiny Dogfish in U.S. Waters in the Western Atlantic Ocean; Scoping Process

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

ACTION: Notice of intent to prepare an environmental impact statement (EIS) and request for scoping comments.

SUMMARY: The Mid-Atlantic and New England Fishery Management Councils (Councils) announce their intention to jointly prepare, in cooperation with NMFS, an EIS to assess potential effects on the human environment of a management regime for spiny dogfish (*Squalus acanthias*) pursuant to the Magnuson-Stevens Fishery Conservation and Management Act of 1976, as amended (Magnuson-Stevens Act). This would be accomplished through the development of a Spiny Dogfish Fishery Management Plan (FMP). If such an FMP is approved by the Secretary of Commerce (Secretary),