

specifying an additional voluntary industry standard for generating and verifying digital signatures. This action will enable Federal agencies to use the Digital Signature Algorithm (DSA), which was originally the single approved technique for digital signatures, as well as two new ANSI standards that were developed for the financial community. These new standards are ANSI X9.31, Digital Signature Using Reversible Public Key Cryptography, and ANSI X9.62, Elliptic Curve Digital Signature Algorithm (ECDSA).

EFFECTIVE DATE: This standard is effective June 27, 2000.

FOR FURTHER INFORMATION CONTACT: Ms. Elaine Barker (301) 975-2911, National Institute of Standards and Technology, 100 Bureau Drive, STOP 8930, Gaithersburg, MD 20899-8930.

Specifications for FIPS 186-2 are available on NIST Web page: <<http://csrc.nist.gov/encryption>>.

Copies of ANSI X9.31, Digital Signatures Using Reversible Public Key Cryptography, and ANSI X9.62, Elliptic Curve Digital Signature Algorithm (ECDSA) are available from the American Bankers Assoc./DC, X9 Customer Service Dept. P.O. Box 79064, Baltimore, MD 21279-0064; telephone 1-800-338-0626.

SUPPLEMENTARY INFORMATION: Under Section 5131 of the Information Technology Management Reform Act of 1996 and the Computer Security Act of 1987, the Secretary of Commerce is authorized to approve standards and guidelines for the cost effective security and privacy of sensitive information processed by federal computer systems. In May 1994, the Secretary of Commerce approved FIPS 186, Digital Signature Standard (DSS), which specified the Digital Signature Algorithm (DSA) as the single technique for the generation and verification of digital signatures. In 1997 NIST solicited comments on augmenting FIPS 186 with other digital signature techniques including the Rivest-Shamir-Adleman (RSA) and the elliptic curve technique. The comments received by NIST supported adding both techniques to FIPS 186. Both techniques were being considered by the financial services industry as voluntary industry standards.

On December 15, 1998, (FR Vol. 63, No. 240, pp 69049-51) NIST announced that the Secretary of Commerce had approved FIPS 186-1, Digital Signature Standard (DSS) as an interim final standard. FIPS 186-1 added the RSA digital signature technique, which had been approved as an industry standard (X9.31-1998, Digital Signatures Using

Reversible Public Key Cryptography for the Financial Services Industry). The elliptic curve technique was not included in the interim final standard since it had not yet been approved by the American National Standards Institute (ANSI) as a voluntary industry standard.

The December 1998 Notice from NIST invited comments from public, academic and research communities, manufacturers, voluntary standards organizations, and Federal, state, and local government organizations concerning the specification of two techniques (DSA and ANSI X9.31-1998) for the generation and verification of digital signatures. That Notice also referred to the elliptic curve technique, which NIST had expected to be approved by ANSI as a voluntary industry standard. In addition to being published in the **Federal Register**, the Notice was posted on the NIST Web pages; information was provided for submission of electronic comments. NIST received comments from 15 private sector organizations and individuals, and from two federal government organizations. The comments supported the addition of the ANSI X9.31 standard, as well as the addition of the elliptic curve technique to the Digital Signature Standard (DSS). NIST recommended that the Secretary of Commerce approve FIPS 186-2, which includes the DSA, ANSI X9.31, and the elliptic curve technique, which has now been approved as ECDSA, under ANSI X9.62, Elliptic Curve Digital Signature Algorithm. Other comments supported the continued use of another RSA signature algorithm that is specified by PKCS#1. The algorithm specified in PKCS#1 does not interoperate with the algorithm specified in ANSI X9.31. FIPS 186-2 allows for the continued acquisition of implementations of PKCS#1 for a transition period of eighteen months from the date of approval of this standard, which will enable federal agencies to plan for the acquisition of implementations of the algorithms promulgated by FIPS 186-2.

Dated: February 8, 2000.

Karen H. Brown,

Deputy Director, NIST.

[FR Doc. 00-3450 Filed 2-14-00; 8:45 am]

BILLING CODE 3510-CN-M

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[Docket No. 000204026-0026-01; I.D. 121799A]

RIN 0648-AN48

Tautog; Interstate Fishery Management Plans

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

ACTION: Notice of determination of noncompliance; notice of declaration of a moratorium.

SUMMARY: In accordance with the Atlantic Coastal Fisheries Cooperative Management Act of 1993 (Act), 16 U.S.C. 5101 *et seq.*, the Secretary of Commerce (Secretary) has determined that the State of Rhode Island is not in compliance with the Atlantic States Marine Fisheries Commission's (Commission) Interstate Fishery Management Plan (ISFMP) for tautog and has failed to implement measures necessary for the conservation of the fishery in question. Pursuant to the Act, a Federal moratorium on fishing for tautog within Rhode Island state waters to be effective on June 15, 2000, if Rhode Island does not come into compliance with the ISFMP for tautog by June 1, 2000, is hereby declared. The purpose of this action is to support and encourage the development, implementation, and enforcement of the Commission's ISFMPs to conserve and manage Atlantic coastal fishery resources.

DATES: The moratorium will become effective on June 15, 2000, through a separate rule unless, by June 1, 2000, the State of Rhode Island adopts and implements measures to return to compliance with the Commission's ISFMP for tautog. If the State of Rhode Island adopts and implements the measures required by the ISFMP for tautog, the Secretary will publish an appropriate announcement in the **Federal Register** rescinding the moratorium with respect to the State.

FOR FURTHER INFORMATION CONTACT: Richard H. Schaefer, Chief, Staff Office for Intergovernmental and Recreational Fisheries, NMFS, 301-427-2014.

SUPPLEMENTARY INFORMATION:

Background

The Act was enacted to support and encourage the development, implementation, and enforcement of the Commission's ISFMPs to conserve and

manage Atlantic coastal fishery resources. Section 807 of the Act specifies that, after notification by the Commission that an Atlantic coastal state is not in compliance with an ISFMP of the Commission, the Secretary shall make a finding, no later than 30 days after receipt of the Commission's notification, on: (1) Whether the state has failed to carry out its responsibilities to implement and enforce the Commission's ISFMP; and (2) whether the measures that the state has failed to implement and enforce are necessary for the conservation of the fishery in question. In making such a finding, the Act requires the Secretary to give careful consideration to the comments of the Commission, the Atlantic coastal state found out of compliance by the Commission, and the appropriate Regional Fishery Management Councils. If the Secretary finds that the state is not in compliance with the Commission's ISFMP, and if the measures the state has failed to implement are necessary for the conservation of the fishery, the Act requires the Secretary to declare a moratorium on fishing in that fishery within the waters of the noncomplying state. The Secretary shall specify the moratorium's effective date, which must be any date within 6 months after the declaration of the moratorium.

Activities Pursuant to the Act

On November 19, 1999, the Secretary received a letter from the Commission prepared pursuant to section 806(b) of the Act. The Commission's letter stated that the State of Rhode Island's tautog regulations did not meet the provisions of the Commission's ISFMP, and, therefore, the Commission found the State of Rhode Island out of compliance with the ISFMP as described here:

Commission Findings on Tautog

The Commission found that the State of Rhode Island has not implemented and is not enforcing the Commission's ISFMP for tautog because it has failed to adopt recreational bag limits for tautog that can be effectively evaluated by the Commission as meeting the mortality reduction requirements of the ISFMP.

Under the ISFMP, states are required to implement and enforce management measures that will achieve an interim fishing mortality target of $F=0.24$, with an ultimate target of $F=0.15$.

To meet these targets, the ISFMP recommends that possession and seasonal limits be imposed which are consistent for all recreational fishing modes. Rhode Island's recreational bag limits for tautog differ between fishing modes. Upon review of Rhode Island's

analysis of its management plan, the Commission's Tautog Technical Committee determined that there was insufficient quantitative data available to effectively determine whether the State's management plan met the overall mortality targets of the Commission's ISFMP. Since the mortality targets of the ISFMP are essential to the conservation of the tautog resource, and it could not be determined whether these targets would be achieved under Rhode Island's current management scheme, the Commission found that the State is not in compliance with the ISFMP.

The Commission's letter also suggested that the Secretary use his discretionary authority under the Act to delay the date of the moratorium for up to 6 months, because the State of Rhode Island is making an effort to come into compliance. The letter stated that Rhode Island is taking action to be in compliance with the Commission ISFMP for tautog by the start of the 2000 tautog season (May 2000).

Determination Regarding Compliance by the State of Rhode Island

Based on a careful analysis of all relevant information, and taking into account comments presented by the State of Rhode Island and the New England Fishery Management Council, the Secretary has determined that the State of Rhode Island is not in compliance with the Commission's ISFMP for tautog. This determination is based on Rhode Island's failure to adopt recreational bag limits for tautog that can be effectively evaluated by the Commission as meeting the mortality reduction requirements of the ISFMP. Therefore, Rhode Island must implement and enforce a recreational bag limit consistent with the ISFMP in order to come back into compliance. Further, the Secretary has determined that implementation and enforcement of a recreational bag limit that can be shown to meet the fishing mortality targets is necessary for the conservation of the resource. Although the State of Rhode Island is not in compliance with the Commission's ISFMP for tautog, because Rhode Island is making expeditious efforts to promulgate regulations that would bring the state into compliance by the start of the 2000 tautog season (May 2000), the Secretary is delaying implementation of the moratorium until June 15, 2000. If the State of Rhode Island adopts and implements measures bringing the state into compliance, the Secretary will publish an appropriate announcement in the **Federal Register** rescinding the moratorium with respect to the State of Rhode Island. If the State of Rhode

Island has not promulgated appropriate regulations by June 1, 2000, NMFS will issue a rule implementing the moratorium effective June 15, 2000. Delaying the effective date of the moratorium until June 15, 2000, will not significantly diminish tautog conservation efforts because the recreational bag limit at issue in this action would not go into effect until October 2000, and the State currently has in place bag limits that meet the conservation goals of the ISFMP.

NMFS will notify the Governor of Rhode Island of this action. *If the moratorium goes into effect, the Secretary will terminate it immediately upon receipt of notification from the Commission that the State has taken appropriate remedial actions to bring it into compliance with the ISFMP, and if the Secretary concurs with the Commission.*

Dated: February 9, 2000.

Andrew A. Rosenberg,

Deputy Assistant Administrator for Fisheries,
National Marine Fisheries Service.

[FR Doc. 00-3552 Filed 2-14-00; 8:45 am]

BILLING CODE 3510-22-F

DEPARTMENT OF DEFENSE

Test Program for Negotiation of Comprehensive Small Business Subcontracting Plans

AGENCY: Department of Defense (DoD).

ACTION: Notice of test program.

SUMMARY: The Department of Defense is amending its Test Program for Negotiation of Comprehensive Small Business Subcontracting Plans to update the regulatory cite reflected in the test program under "III. Program Requirements" for Defense Federal Acquisition Regulation Supplement (DFARS) coverage of source selection. DFARS coverage of source selection is found at Subpart 215.3.

EFFECTIVE DATE: February 15, 2000.

FOR FURTHER INFORMATION CONTACT: Mr. Ivory Fisher, Office of Small and Disadvantaged Business Utilization (OSADBU), Office of the Under Secretary of Defense (Acquisition, Technology & Logistics), 1777 North Kent Street, Suite 9100, Arlington, VA 22209, telephone (703) 588-8616, telefax (703) 588-7561.

SUPPLEMENTARY INFORMATION:

A. Background

In accordance with Section 834 of Public Law 101-189, as amended, the Department of Defense (DoD) established a Test Program for