

transmission, or reception of data or information. This includes both major applications and general support systems as defined by OMB Circular A-130. Examples of tasks that require security provisions include:

(1) Hosting of DOS e-Government sites or other IT operations;

(2) Acquisition, transmission or analysis of data owned by DOS with significant replacement cost should the Contractor's copy be corrupted; and

(3) Access to DOS general support systems/ major applications at a level beyond that granted the general public; e.g., bypassing a firewall.

(b) *IT Security Plan.* The Contractor shall develop, provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The plan shall describe those parts of the contract to which this clause applies. The Contractor's IT Security Plan shall comply with applicable Federal laws that include, but are not limited to, 40 U.S.C. 11331, the Federal Information Security Management Act (FISMA) of 2002, and the E-Government Act of 2002. The plan shall meet IT security requirements in accordance with Federal and DOS policies and procedures, as they may be amended from time to time during the term of this contract that include, but are not limited to:

(1) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources;

(2) National Institute of Standards and Technology (NIST) Guidelines (see NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Technology Systems (<http://src.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf>)); and

(3) Department of State information security sections of the Foreign Affairs Manual (FAM) and Foreign Affairs Handbook (FAH) (<http://foia.state.gov/Regs/Search.asp>), specifically:

(i) 12 FAM 230, Personnel Security;

(ii) 12 FAM 500, Information Security (sections 540, 570, and 590);

(iii) 12 FAM 600, Information Security Technology (section 620, and portions of 650);

(iv) 5 FAM 1060, Information Assurance Management; and

(v) 5 FAH 11, Information Assurance Handbook.

(c) *Submittal of IT Security Plan.* Within 30 days after contract award, the Contractor shall submit the IT Security Plan to the Contracting Officer and Contracting Officer's Representative (COR) for acceptance. This plan shall be consistent with and further detail the approach contained in the contractor's proposal or sealed bid that resulted in the award of this contract and in compliance with the requirements stated in this clause. The plan, as accepted by the Contracting Officer and COR, shall be incorporated into the contract as a compliance document. The Contractor shall comply with the accepted plan.

(d) *Accreditation.* Within six (6) months after contract award, the Contractor shall

submit written proof of IT security accreditation for acceptance by the Contracting Officer. Such written proof may be furnished either by the Contractor or by a third party. Accreditation must be in accordance with NIST Special Publication 800-37. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document, and shall include a final security plan, a risk assessment, security test and evaluation, and disaster recovery/continuity of operations plan. The Contractor shall comply with the accepted accreditation documentation.

(e) *Annual verification.* On an annual basis, the Contractor shall submit verification to the Contracting Officer that the IT Security Plan remains valid.

(f) *Warning notices.* The Contractor shall ensure that the following banners are displayed on all DOS systems (both public and private) operated by the Contractor prior to allowing anyone access to the system:

Government Warning

\*\*WARNING\*\*WARNING\*\*  
WARNING\*\*

Unauthorized access is a violation of U.S. law and Department of State policy, and may result in criminal or administrative penalties. Users shall not access other user's or system files without proper authority. Absence of access controls IS NOT authorization for access! DOS information systems and related equipment are intended for communication, transmission, processing and storage of U.S. Government information. These systems and equipment are subject to monitoring by law enforcement and authorized Department officials. Monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed or stored in this system by law enforcement and authorized Department officials. Use of this system constitutes consent to such monitoring.

\*\*WARNING\*\*WARNING\*\*  
WARNING\*\*

(g) *Privacy Act notification.* The Contractor shall ensure that the following banner is displayed on all DOS systems that contain Privacy Act information operated by the Contractor prior to allowing anyone access to the system:

This system contains information protected under the provisions of the Privacy Act of 1974 (Pub. L. 93-579). Any privacy information displayed on the screen or printed shall be protected from unauthorized disclosure. Employees who violate privacy safeguards may be subject to disciplinary actions, a fine of up to \$5,000, or both.

(h) *Privileged or limited privileged access.* Contractor personnel requiring privileged access or limited privileged access to systems operated by the Contractor for DOS or interconnected to a DOS network shall adhere to the specific contract security requirements contained within this contract and/or the Contract Security Classification Specification (DD Form 254).

(i) *Training.* The Contractor shall ensure that its employees performing under this contract receive annual IT security training in accordance with OMB circular A-130, FISMA, and NIST requirements, as they may be amended from time to time during the term of this contract, with a specific emphasis on rules of behavior.

(j) *Government access.* The Contractor shall afford the Government access to the Contractor's and subcontractor's facilities, installations, operations, documentation, databases and personnel used in performance of the contract. Access shall be provided to the extent required to carry out a program of IT inspection (to include vulnerability testing), investigation and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of DOS data or to the function of information technology systems operated on behalf of DOS, and to preserve evidence of computer crime.

(k) *Subcontracts.* The Contractor shall incorporate the substance of this clause in all subcontracts that meet the conditions in paragraph (a) of this clause.

(l) *Notification regarding employees.* The Contractor shall immediately notify the Contracting Officer when an employee either begins or terminates employment when that employee has access to DOS information systems or data.

(m) *Termination.* Failure on the part of the Contractor to comply with the terms of this clause may result in termination of this contract.

(End of clause)

Dated: August 28, 2007.

**Corey M. Rindner,**

*Procurement Executive, Bureau of Administration, Department of State.*

[FR Doc. E7-17752 Filed 9-7-07; 8:45 am]

**BILLING CODE 4710-24-P**

---

## DEPARTMENT OF COMMERCE

### National Oceanic and Atmospheric Administration

#### 50 CFR Part 679

[I.D. 041307D]

RIN 0648-AU68

#### Fisheries of the Exclusive Economic Zone Off Alaska; Allocating Bering Sea and Aleutian Islands Area Fishery Resources; Notice of Amendment 80 Public Workshop

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

**ACTION:** Notification of public workshop.

**SUMMARY:** NMFS will present a public workshop on the implementation of the Amendment 80 Program (Program) for potentially eligible participants and other interested parties. The Program

implements a limited access privilege program (LAPP) for specific groundfish fisheries in the Bering Sea and Aleutian Islands management area (BSAI). At the workshop, NMFS will provide an overview of the Program, discuss the key Program elements, describe the process for participating in the Program, and answer questions. NMFS is conducting this public workshop to provide assistance to fishery participants in understanding and reviewing this Program.

**DATES:** The workshop will be held on Monday, September 24, 2007, 1 p.m. to 4 p.m. Pacific standard time.

**ADDRESSES:** The workshop will be held at the Swedish Cultural Center, 1920 Dexter Avenue N., Seattle, WA 98109.

**FOR FURTHER INFORMATION CONTACT:** Glenn Merrill, 907-586-7228 or [glenn.merrill@noaa.gov](mailto:glenn.merrill@noaa.gov).

**SUPPLEMENTARY INFORMATION:** NMFS will publish a final rule that will implement a LAPP for Amendment 80 to the Fishery Management Plan for BSAI Groundfish (FMP) in mid-September, 2007. Among other things, Amendment 80 will allocate specific BSAI groundfish resources among a defined group of harvesters under a LAPP; limit the bycatch of halibut and crab resources; assign Amendment 80 quota share (QS) that can be used to yield an exclusive harvest privilege on an annual basis; allow Amendment 80 QS holders to form a cooperative with other Amendment 80 QS holders on an

annual basis to receive an exclusive harvest privilege; implement use caps to limit the amount of Amendment 80 QS a person can hold; limit the total amount of catch in other groundfish fisheries that could be taken by participants in the Program; ensure minimum retention of groundfish while fishing in the BSAI; and establish necessary monitoring and enforcement standards.

Amendment 80 was approved by the North Pacific Fishery Management Council (Council) on June 9, 2006. NMFS published a proposed rule to implement the Program on May 30, 2007 (72 FR 30052). The Secretary of Commerce approved Amendment 80 on July 26, 2007. The Program implements Amendment 80 and also meets the requirements of:

- Section 219 of the Consolidated Appropriations Act of 2005 (Public Law 108-447; December 8, 2004), which defined the Amendment 80 sector and implemented a capacity reduction program for several catcher/processor sectors;

- Section 416 of the Coast Guard and Maritime Transportation Act of 2006 (Public Law 109-241; July 11, 2006), which amended provisions of the Community Development Quota (CDQ) Program in the Magnuson-Stevens Fishery Conservation and Management Act; and

- The Magnuson-Stevens Fishery Conservation and Management Reauthorization Act (Public Law 109-

479, January 12, 2007), which modified provisions related to the CDQ Program and instituted other measures applicable to LAPPs.

NMFS is conducting a public workshop to provide assistance to fishery participants in reviewing the requirements of the Program. At the workshop, NMFS will provide an overview of the Program, and discuss the key Program elements, including quota share application; cooperative and limited access participation provisions; cooperative quota transfer provisions; the appeals process; monitoring and enforcement; and electronic reporting. Additionally, NMFS will answer questions from workshop participants. For further information on the Program, please visit the NMFS Alaska Region website at <http://www.fakr.noaa.gov>.

### Special Accommodations

This workshop is physically accessible to people with disabilities. Requests for special accommodations should be directed to Glenn Merrill (see **FOR FURTHER INFORMATION CONTACT**) at least 5 working days before the workshop date.

Dated: September 4, 2007.

### Emily H. Menashes

*Acting Director, Office of Sustainable Fisheries, National Marine Fisheries Service.*  
[FR Doc. E7-17772 Filed 9-7-07; 8:45 am]

**BILLING CODE 3510-22-S**