A. Background

The Computer Security Act of 1987 and Appendix III of the Office of Management and Budget (OMB) Circular No. A–130, Security of Federal Automated Information Resources, require that adequate security be provided for all Agency information collected, processed, transmitted, stored, or disseminated. NFS Part 1804 contains the requirement for all NASA contractors and subcontractors to comply with NASA policies in safeguarding unclassified NASA data held via information technology (IT). This interim rule clarifies NASA requirements by revising the clause at 1852.204–76, Security Requirements for Unclassified Information Technology Resources, and amending Section 1804.470 to clarify the applicability and requirements of the clause.

B. Regulatory Flexibility Act

NASA certifies that this interim rule will not have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*), because this interim rule only clarifies existing requirements and does not impose any new requirements.

C. Paperwork Reduction Act

This interim rule clarifies existing requirements that were previously approved by the Office of Management and Budget (OMB) under OMB Control No. 2700–0098.

D. Determination To Issue an Interim Rule

In accordance with 41 U.S.C. 418(d), NASA has determined that urgent and compelling reasons exist to promulgate this interim rule. The basis for this determination is that the clarifications contained in this interim rule are needed to ensure consistent implementation of NASA's acquisition-related aspects of Federal policies for assuring the security of unclassified automated information resources. Public comments received in response to this interim rule will be considered in the formation of the final rule.

List of Subjects in 48 CFR Parts 1804 and 1852

Government procurement.

Tom Luedtke,

Associate Administrator for Procurement.

Accordingly, 48 CFR Parts 1804 and 1852 are amended as follows:

1. The authority citation for 48 CFR Parts 1804 and 1852 continues to read as follows:

Authority: 42 U.S.C. 2473(c)(1).

PART 1804—ADMINISTRATIVE MATTERS

2. Revise sections 1804.470–1, 1804.470–2, 1804.470–3, and 1804.470–4 to read as follows:

1804.470–1 Scope.

This section implements NASA's acquisition-related aspects of Federal policies for assuring the security of unclassified automated information resources.

1804.470–2 Policy.

(a) NASA policies and procedures on security for automated information technology are prescribed in NPD 2810.1, Security of Information Technology, and in NPG 2810.1, Security of Information Technology. The provision of information technology (IT) security in accordance with these policies and procedures, is required in all contracts that include IT resources or services in which a contractor must have physical or electronic access to NASA's sensitive information contained in unclassified systems that directly support the mission of the Agency. This includes information technology, hardware, software, and the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. Examples of tasks that require security provisions include:

(1) Computer control of spacecraft, satellites, or aircraft or their payloads;

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

(3) Access to NASA networks or computers at a level beyond that granted the general public, e.g. bypassing a firewall.

(b) The contractor must not use or redistribute any NASA information processed, stored, or transmitted by the contractor except as specified in the contract.

1804.470–3 Security plan for unclassified Federal Information Technology systems.

(a) The requiring activity with the concurrence of the Center Chief Information Officer (CIO), and the Center Information Technology (IT) Security Manager, must determine whether an IT Security Plan for unclassified information is required.

(b) IT security plans must demonstrate a thorough understanding of NPG 2810.1 and NPD 2810.1 and must include, as a minimum, the security measures and program safeguards planned to ensure that the information technology resources acquired and used by contractor and subcontractor personnel—

(1) Are protected from unauthorized access, alteration, disclosure, or misuse of information processed, stored, or transmitted;

(2) Can maintain the continuity of automated information support for NASA missions, programs, and functions;

(3) Incorporate management, general, and application controls sufficient to provide cost-effective assurance of the systems' integrity and accuracy;

(4) Have appropriate technical, personnel, administrative, environmental, and access safeguards;

(5) Document and follow a virus protection program for all IT resources under its control; and

(6) Document and follow a network intrusion detection and prevention program for all IT resources under its control.

(c) The contractor must be required to develop and maintain an IT System Security Plan, in accordance with NPG 2810.1, for systems for which the contractor has primary operational responsibility on behalf of NASA.

(d) The contracting officer must obtain the concurrence of the Center Chief of Security before granting any contractor requests for waiver of the screening requirement contained in the clause at 1852.204–76.

1804.470–4 Contract clauses.

The contracting officer must insert a clause substantially the same as the clause at 1852.204–76, Security Requirements for Unclassified Information Technology Resources, in solicitations and contracts which require submission of an IT Security Plan.

PART 1852—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

3. Revise section 1852.204–76 to read as follows:

1852.204–76 Security Requirements for Unclassified Information Technology Resources.

As prescribed in 1804.470–4, insert a clause substantially as follows:

Security Requirements for Unclassified Information Technology Resources, July 2001

(a) The Contractor shall be responsible for Information Technology security for all systems connected to a NASA network or operated by the Contractor for NASA, regardless of location. This clause is applicable to all or any part of the contract that includes information technology

resources or services in which the Contractor must have physical or electronic access to NASA's sensitive information contained in unclassified systems that directly support the mission of the Agency. This includes information technology, hardware, software, and the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. Examples of tasks that require security provisions include:

(1) Computer control of spacecraft, satellites, or aircraft or their payloads;

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

(3) Access to NASA networks or computers at a level beyond that granted the general public, *e.g.* bypassing a firewall.

(b) The Contractor shall 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 be compliant with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 *et seq.*) and the Government Information Security Reform Act of 2000. The plan shall meet IT security requirements in accordance with Federal and NASA policies and procedures 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) NASA Procedures and Guidelines (NPG) 2810.1, Security of Information Technology; and

(3) Chapter 3 of NPG 1620.1, NASA Security Procedures and Guidelines.

(c) Within ____days after contract award, the contractor shall submit for NASA approval an IT Security Plan. This plan must be consistent with and further detail the approach contained in the offeror'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 approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(d)(1) Contractor personnel requiring privileged access or limited privileged access to systems operated by the Contractor for NASA or interconnected to a NASA network shall be screened at an appropriate level in accordance with NPG 2810.1, Section 4.5; NPG 1620.1, Chapter 3; and paragraph (d)(2) of this clause. Those Contractor personnel with non-privileged access do not require personnel screening. NASA shall provide screening using standard personnel screening National Agency Check (NAC) forms listed in paragraph (d)(3) of this clause, unless contractor screening in accordance with paragraph (d)(4) is approved. The Contractor shall submit the required forms to the NASA Center Chief of Security (CCS) within fourteen (14) days after contract award or assignment of an individual to a position requiring screening. The forms may be obtained from the CCS. At the option of the government, interim access may be granted pending completion of the NAC.

(2) Guidance for selecting the appropriate level of screening is based on the risk of adverse impact to NASA missions. NASA defines three levels of risk for which screening is required (IT–1 has the highest level of risk):

(i) IT–1—Individuals having privileged access or limited privileged access to systems whose misuse can cause very serious adverse impact to NASA missions. These systems include, for example, those that can transmit commands directly modifying the behavior of spacecraft, satellites or aircraft.

(ii) IT–2—Individuals having privileged access or limited privileged access to systems whose misuse can cause serious adverse impact to NASA missions. These systems include, for example, those that can transmit commands directly modifying the behavior of payloads on spacecraft, satellites or aircraft; and those that contain the primary copy of ''level 1'' data whose cost to replace exceeds one million dollars.

(iii) IT–3—Individuals having privileged access or limited privileged access to systems whose misuse can cause significant adverse impact to NASA missions. These systems include, for example, those that interconnect with a NASA network in a way that exceeds access by the general public, such as bypassing firewalls; and systems operated by the contractor for NASA whose function or data has substantial cost to replace, even if these systems are not interconnected with a NASA network.

(3) Screening for individuals shall employ forms appropriate for the level of risk as follows:

(i) IT–1: Fingerprint Card (FC) 258 and Standard Form (SF) 85P, Questionnaire for Public Trust Positions (Information regarding financial record, question 22, and the Authorization for Release of Medical Information are not applicable);

(ii) IT–2: FC 258 and SF 85, Questionnaire for Non-Sensitive Positions; and

(iii) IT–3: NASA Form 531, Name Check, and FC 258.

(4) The Contracting Officer may allow the Contractor to conduct its own screening of individuals requiring privileged access or limited privileged access provided the Contractor can demonstrate that the procedures used by the Contractor are equivalent to NASA's personnel screening procedures. As used here, equivalent includes a check for criminal history, as would be conducted by NASA, and completion of a questionnaire covering the same information as would be required by NASA.

(5) Screening of contractor personnel may be waived by the Contracting Officer for those individuals who have proof of—

(1) Current or recent national security clearances (within last three years);

(ii) Screening conducted by NASA within last three years; or

(iii) Screening conducted by the Contractor, within last three years, that is equivalent to the NASA personnel screening procedures as approved by the Contracting Officer under paragraph (d)(4) of this clause.

(e) The Contractor shall ensure that its employees, in performance of the contract, receive annual IT security training in NASA IT Security policies, procedures, computer ethics, and best practices in accordance with NPG 2810.1, Section 4.3 requirements. The contractor may use web-based training available from NASA to meet this requirement.

(f) The Contractor shall afford NASA, including the Office of Inspector General, access to the Contractor's and subcontractors' 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, investigation and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of NASA data or to the function of computer systems operated on behalf of NASA, and to preserve evidence of computer crime.

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

(End of clause)

[FR Doc. 01–17131 Filed 7–11–01; 8:45 am]

BILLING CODE 7510–01–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

50 CFR Part 679

[Docket No. 010122013–1013–01; I.D. 070901A]

Fisheries of the Exclusive Economic Zone Off Alaska; Pacific Ocean Perch in the West Yakutat District of the Gulf of Alaska

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

ACTION: Closure.

SUMMARY: MFS is prohibiting directed fishing for Pacific ocean perch in the West Yakutat District of the Gulf of Alaska (GOA). This is action is necessary to prevent exceeding the 2001 total allowable catch (TAC) of Pacific ocean perch in this area.

DATES: Effective 1200 hrs, Alaska local time (A.l.t.), July 9, 2001, through 2400 hrs, A.l.t., December 31, 2001.

FOR FURTHER INFORMATION CONTACT: Mary Furuness, 907–586–7228.

SUPPLEMENTARY INFORMATION: NMFS manages the groundfish fishery in the GOA exclusive economic zone according to the Fishery Management Plan for the Groundfish Fishery of the