direct final action, of the same title, which is located in the Rules section of this **Federal Register**. EPA is approving the State's SIP revision as a direct final rule without prior proposal because EPA views this as a noncontroversial SIP revision and anticipates no adverse comments. A detailed rationale for the approval is set forth in the preamble to the direct final rule. If EPA receives no adverse comments, EPA will not take further action on this proposed rule.

If EPA receives adverse comments, EPA will withdraw the direct final rule and it will not take effect. EPA will address all public comments in a subsequent final rule based on this proposed rule. EPA will not institute a second comment period on this action. Any parties interested in commenting on this action should do so at this time. Please note that if we receive adverse comment on an amendment, paragraph, or section of this rule and if that provision may be severed from the remainder of the rule, EPA may adopt as final those provisions of the rule that are not the subject of an adverse comment.

Dated: June 14, 2007.

Michael F. Gearheard,

Acting Regional Administrator, Region 10.

[FR Doc. E7–12235 Filed 6–25–07; 8:45 am]

BILLING CODE 6560–50–P

DEPARTMENT OF STATE

48 CFR Parts 639 and 652

[Public Notice 5836]

RIN 1400–AC31

Department of State Acquisition Regulation

AGENCY: State Department.

ACTION: Proposed rule.

SUMMARY: This proposed rule will add a new solicitation provision and contract clause to implement Department of State requirements regarding security issues for information technology systems, as required by the Federal Information Security Management Act of 2002 (FISMA).

DATES: The Department will accept comments from the public up to 60 days from June 26, 2007.

ADDRESSES: You may submit comments, identified by any of the following methods:

- *E-mail: ginesgg@state.gov*. You must include the RIN in the subject line of your message.
- *Mail (paper, disk, or CD–ROM submissions):* Gladys Gines, Procurement Analyst, Department of State, Office of the Procurement Executive, 2201 C Street, NW., Suite 603, State Annex Number 6, Washington, DC 20522–0602.
- *Fax:* 703–875–6155.

Persons with access to the Internet may also view this notice and provide comments by going to the regulations.gov Web site at *http://www.regulations.gov/index.cfm.*

FOR FURTHER INFORMATION CONTACT: Gladys Gines, Procurement Analyst, Department of State, Office of the Procurement Executive, 2201 C Street, NW., Suite 603, State Annex Number 6, Washington, DC 20522–0602; e-mail address: *ginesgg@state.gov.*

SUPPLEMENTARY INFORMATION: On September 30, 2005, the Federal Acquisition Regulation (FAR) was revised to implement the Information Technology (IT) Security provisions of the Federal Information Security Management Act of 2002 (FISMA) (Title III of the E-Government Act of 2002 (E-Gov Act)). (See 70 FR 57447, September 30, 2005). While the FAR provided some guidance to Government contracting officials and other members of the acquisition team, it recognized that Federal agencies would need to customize IT security policies and implementations to meet mission needs. Therefore, the FAR did not provide specific contract language for inclusion in affected contracts, but required that agencies ''include the appropriate information technology security policies and requirements'' when acquiring information technology.

This proposed rule will add a new solicitation provision and contract clause to the Department of State Acquisition Regulation (DOSAR) to implement the Department's requirements regarding security issues for information technology systems. The clause and provision will apply to contracts that include information technology resources to services in which the contractor has physical or electronic access to Department information that directly supports the mission of the Department of State. This will include contracts to acquire personal services from organizations. It does not include personal services contracts that the Department executes directly with specific individuals. Such individuals are considered to be employees of the Department and as such are under its direct supervision and control for purposes of ensuring compliance with applicable information security laws and regulations.

The clause requires that the contractor be responsible for IT security, based on agency risk assessments, for all systems connected to a Department of State (DOS) network or operated by a contractor for DOS. It requires the development of an IT security plan and IT security certification and accreditation in accordance with NIST Special Publication 800–37, Guide for the Security Certification and Accreditation of Federal Information Technology Systems, as well as all related policies and guidance promulgated by the Office of Management and Budget under FISMA and the Privacy Act. This would include related testing and continuous monitoring, incident reporting, and DOS oversight activities. The solicitation provision requires that, as part of their bid/offer, vendors address the approach for completing the security plan, testing, reporting, and certification and accreditation requirements.

Regulatory Findings

Administrative Procedure Act

In accordance with provisions of the Administrative Procedure Act governing rules promulgated by federal agencies that affect the public (5 U.S.C. 552), the Department is publishing this proposed rule and inviting public comment.

Regulatory Flexibility Act

The Department of State, in accordance with the Regulatory Flexibility Act (5 U.S.C. 605(b)), has reviewed this regulation and, by approving it, certifies that this rule will not have a significant economic impact on a substantial number of small entities.

Unfunded Mandates Act of 1995

This rule will not result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of $100 million or more in any year and it will not significantly or uniquely affect small governments. Therefore, no actions were deemed necessary under the provisions of the Unfunded Mandates Act of 1995.

Small Business Regulatory Enforcement Fairness Act of 1996

This rule is not a major rule as defined by section 804 of the Small Business Regulatory Enforcement Act of 1996. This rule will not result in an annual effect on the economy of $100 million or more; a major increase in costs or prices; or significant adverse effects on competition, employment, investment, productivity, innovation, or on the ability of United States-based companies to compete with foreign based companies in domestic and import markets.

Executive Order 13132

This rule will not have substantial direct effects on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government. Therefore, in accordance with section 6 of the Executive Order 13132, it is determined that this rule does not have sufficient federalism implications to require consultations or warrant the preparation of a federalism summary impact statement.

Paperwork Reduction Act

Information collection requirements have been approved under the Paperwork Reduction Act of 1980 by OMB, and have been assigned OMB control number 1405–0050.

List of Subjects in 48 CFR Parts 639 and 652

Government procurement.

Accordingly, for reasons set forth in the preamble, title 48, chapter 6 of the Code of Federal Regulations is proposed to be amended as follows:

Subchapter F—Special Categories of Contracting

1. The authority citation for 48 CFR parts 639 and 652 continues to read as follows:

Authority: 40 U.S.C. 486(c); 22 U.S.C. 2658.

PART 639—ACQUISITION OF INFORMATION TECHNOLOGY

2. A new Part 639, consisting of subpart 639.1, sections 639.107 and 639.107–70, is added to subchapter F as follows:

PART 639—ACQUISITION OF INFORMATION TECHNOLOGY

Subpart 639.1—General

639.107 Contract clause.

639.107–70 DOSAR solicitation provision and contract clause.

(a) The contracting officer shall insert the provision at 652.239–70, Information Technology Security Plan and Accreditation, in solicitations that include information technology resources or services in which the contractor will have physical or electronic access to Department information that directly supports the mission of the Department.

(b) The contracting officer shall insert the clause at 652.239–71, Security Requirements for Unclassified Information Technology Resources, in solicitations and contracts containing the provision at 652.239–70. The provision and clause shall not be inserted in solicitations and contracts for personal services with individuals.

Subchapter H—Clauses and Forms

PART 652—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

3. Section 652.239–70 is added to read as follows:

652.239–70 Information Technology Security Plan and Accreditation.

As prescribed in 639.107–70(a), insert the following provision:

Information Technology Security Plan and Accreditation (DATE)

All offers/bids submitted in response to this solicitation must address the approach for completing the security plan and certification and accreditation requirements as required by the clause at 652.239–71, Security Requirements for Unclassified Information Technology Resources.

(End of provision)

4. Section 652.239–71 is added to read as follows:

652.239–71 Security Requirements for Unclassified Information Technology Resources.

As prescribed in 639.107–70(b), insert the following clause:

Security Requirements for Unclassified Information Technology Resources (DATE)

(a) *General.* The Contractor shall be responsible for information technology (IT) security, based on Department of State (DOS) risk assessments, for all systems connected to a Department of State (DOS) network or operated by the Contractor for DOS, 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 has physical or electronic access to DOS's information that directly supports the mission of DOS. The term ''information technology'', as used in this clause, means any equipment, including telecommunications equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, 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 System *(http://csrc.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

WARNINGWARNING**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.

WARNINGWARNING**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: June 13, 2007.

Corey M. Rindner,

Procurement Executive, Department of State.

[FR Doc. 07–3116 Filed 6–25–07; 8:45 am]

BILLING CODE 4710–24–M

DEPARTMENT OF THE INTERIOR

Fish and Wildlife Service

50 CFR Part 17

RIN 1018–AU91

Endangered and Threatened Wildlife and Plants; Designation of Critical Habitat for the Marbled Murrelet (Brachyramphus marmoratus)

AGENCY: Fish and Wildlife Service, Interior.

ACTION: Proposed rule; reopening of comment period, notice of availability of draft economic analysis, and amended required determinations.

SUMMARY: We, the U.S. Fish and Wildlife Service (Service), announce the reopening of the comment period on the proposed designation of critical habitat for the marbled murrelet (*Brachyramphus marmoratus*) under the Endangered Species Act of 1973, as amended (Act). We also announce the availability of the draft economic analysis for the proposed critical habitat designation and amended required determinations for the proposal. The draft economic analysis estimates the post-designation impacts associated with marbled murrelet conservation efforts in areas proposed for final critical habitat designation to range from $69.4 million to $1.42 billion at present value over a 20-year period in undiscounted dollars, $38.1 million to $535 million ($2.22 million to $16.8 million annualized) assuming a 3 percent discount rate, or $24.2 million to $251 million ($2.18 million to $12 million annualized) assuming a 7 percent discount rate. We are reopening the comment period to allow all interested parties the opportunity to comment simultaneously on the proposed rule and the associated draft economic analysis. Comments previously submitted on the proposed rule need not be resubmitted as they are already part of the public record and will be fully considered in preparation of the final rule.

DATES: We will accept public comments until July 26, 2007.

ADDRESSES: If you wish to comment, you may submit your comments and materials by any one of several methods:

1. Submit written comments and information by mail or hand deliver to Ken Berg, Field Supervisor, U.S. Fish and Wildlife Service, Western Washington Fish and Wildlife Office, 510 Desmond Drive, SE., Suite 101, Lacey, WA 98503–1273.

2. Send comments by electronic mail (e-mail) to *MurreletCH@fws.gov.* Please see the Public Comments Solicited section below for information about electronic filing.

3. Fax your comments to 360–753–9405.

4. Go to the Federal eRulemaking Portal: *http://www.regulations.gov.* Follow the instructions for submitting comments.

FOR FURTHER INFORMATION CONTACT: Ken Berg, Field Supervisor, Western Washington Fish and Wildlife Office, at the address listed in the **ADDRESSES** section (telephone 360–753–9440; facsimile 360–753–9405).

SUPPLEMENTARY INFORMATION:

Public Comments Solicited

We will accept written comments and information during this reopened comment period. We solicit comments on the original proposed critical habitat designation published in the **Federal Register** on September 12, 2006 (71 FR 53838), and on our draft economic analysis of the proposed designation. We will consider information and recommendations from all interested parties. We are particularly interested in comments concerning:

(1) The reasons why habitat should or should not be designated as critical habitat under section 4 of the Act (16 U.S.C. 1531 *et seq.*), including whether the benefit of designation would outweigh threats to the species caused by designation such that the designation of critical habitat is prudent;

(2) Specific information on the amount and distribution of marbled murrelet habitat, what areas should be