NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

48 CFR Parts 1804 and 1852

RIN: 2700–AD26

Security Requirements for Unclassified Information Technology (IT) Resources

AGENCY: National Aeronautics and Space Administration.

ACTION: Proposed rule.

SUMMARY: NASA is proposing to amend the clause at NASA FAR Supplement (NFS) 1852.204–76, Security Requirements for Unclassified Information Technology Resources, to reflect the updated requirements of NASA Procedural Requirements (NPR) 2810, ''Security of Information Technology''. The NPR was recently revised to address increasing cyber threats and to ensure consistency with the Federal Information Security Management Act (FISMA), which requires agencies to protect information and information systems in a manner that is commensurate with the sensitivity of the information processed, transmitted, or stored.

DATES: Comments should be submitted on or before October 2, 2006.

ADDRESSES: Interested parties may submit comments, identified by RIN number 2700–AD26, via the Federal eRulemaking Portal: *http://www.regulations.gov.* Follow the instructions for submitting comments. Comments may also be submitted to Ken Stepka, NASA Headquarters, Office of Procurement, Analysis Division, Washington, DC 20546. Comments may also be submitted by e-mail to *Ken.stepka@nasa.gov.*

FOR FURTHER INFORMATION CONTACT: Ken Stepka, Office of Procurement, Analysis Division, (202) 358–0492, e-mail: *ken.stepka@nasa.gov.*

SUPPLEMENTARY INFORMATION:

A. Background

NASA's current contract requirements for IT Security are defined in the clause at NFS 1852.204–76, Security Requirements for Unclassified Information Technology Resources. In order to comply with the Government-wide requirements of FISMA, the proposed revision to 1852.204–76 incorporates several new requirements, including—

- Expanded requirements for IT Security Plans to include a Risk Assessment and a FIPS 199 Assessment;
- Added requirements for a Contingency Plan; and
- Change of the physical security requirement from a National Agency Check to a National Agency Check with Inquiries.

The revised clause is applicable to all NASA contracts that require contractors to: (1) Have physical or electronic access to NASA's computer systems, networks, or IT infrastructure; or (2) use information systems to generate, store, or exchange data with NASA or on behalf of NASA, regardless of whether the data resides on a NASA or a contractor's information system.

The text at NFS 1804.470 is also proposed to be revised consistent with the revised clause.

This is not a significant regulatory action and, therefore, was not subject to review under Section 6(b) of Executive Order 12866, Regulatory Planning and Review, dated September 30, 1993. This rule is not a major rule under 5 U.S.C. 804.

B. Regulatory Flexibility Act

This proposed rule is not expected to have a significant economic impact on a substantial number of small entities with the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601 et seq., because the proposed rule summarizes the existing Government-wide IT security requirements mandated by, and related to, FISMA.

C. Paperwork Reduction Act

The Paperwork Reduction Act (Pub. L. 96–511) does not apply because the Office of Management and Budget (OMB) has determined that the proposed changes to the NFS do not impose information collection requirements that require the approval of OMB under 44 U.S.C. 3501, et seq.

List of Subjects in 48 CFR Parts 1804 and 1852

Government procurement.

Tom Luedtke,

Assistant Administrator for Procurement.

Accordingly, 48 CFR parts 1804 and 1852 are proposed to be 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, 1804.470–1, 1804.470–2, 1804.470–3, and 1804.470–4 to read as follows:

§ 1804.470 Security requirements for unclassified information technology (IT) resources.

§ 1804.470–1 Scope.

This section implements NASA's acquisition requirements pertaining to Federal policies for the security of unclassified information and information systems. Federal policies include the Federal Information System Management Act (FISMA) of 2002, Homeland Security Presidential Directive (HSPD) 12, Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.), Public Law 106–398, section 1061, Government Information Security Reform, OMB Circular A–130, Management of Federal Information Resources, and the National Institute of Standards and Technology (NIST) security requirements and standards. These requirements safeguard IT services provided to NASA such as the management, operation, maintenance, development, and administration of hardware, software, firmware, computer systems, networks, and telecommunications systems.

§ 1804.470–2 Policy.

NASA IT security policies and procedures for unclassified information and IT are prescribed in NASA Policy Directive (NPD) 2810, Security of Information Technology; NASA Procedural Requirements (NPR) 2810, Security of Information Technology; and interim policy updates in the form of NASA Information Technology Requirements (NITR). IT services must be performed in accordance with these policies and procedures.

§ 1804.470–3 IT Security Requirements.

These IT security requirements cover all NASA contracts in which IT plays a role in the provisioning of services or products (e.g., research and development, engineering, manufacturing, IT outsourcing, human resources, and finance) that support NASA in meeting its institutional and mission objectives. These requirements are applicable where a contractor or subcontractor must obtain physical or electronic (i.e., authentication level 2 and above as defined in NIST Special Publication 800–63, Electronic Authentication Guideline) access to NASA's computer systems, networks, or IT infrastructure. These requirements are also applicable in cases where information categorized as low, moderate, or high by the Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, is stored, generated, or exchanged by NASA or on behalf of NASA by a contractor or

subcontractor, regardless of whether the information resides on a NASA or a contractor/subcontractor's information system.

§ 1804.470–4 Contract clause.

(a) Insert the clause at 1852.204–76, Security Requirements for Unclassified Information Technology Resources, in all solicitations and contracts when contract performance requires contractors to:

(1) Have physical or electronic access to NASA's computer systems, networks, or IT infrastructure; or

(2) Use information systems to generate, store, or exchange data with NASA or on behalf of NASA, regardless of whether the data resides on a NASA or a contractor's information system.

(b) Paragraph (d) of the clause allows contracting officers to waive the requirements of paragraphs (b) and (c)(1) through (3) of the clause. Contracting officers must obtain the approval of the:

(1) Center IT Security Manager before granting any waivers to paragraph (b) of the clause; and

(2) The Center Chief of Security before granting any waivers to paragraphs (c)(1) through (3) of the clause.

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(a), insert the following clause:

Security Requirements for Unclassified Information

Technology Resources

(XX/XX)

(a) The Contractor shall be responsible for information and information technology (IT) security when the Contractor or its subcontractors must obtain physical or electronic (i.e., authentication level 2 and above as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800–63, Electronic Authentication Guideline) access to NASA's computer systems, networks, or IT infrastructure, or where information categorized as low, moderate, or high by the Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, is stored, generated, or exchanged by NASA or on behalf of NASA by a contractor or subcontractor, regardless of whether the information resides on a NASA or a contractor/subcontractor's information system.

(b) IT Security Requirements.

(1) Within 30 days after contract award, a Contractor shall submit to the Contracting Officer for NASA approval an IT Security Plan, Risk Assessment, and FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, Assessment. These plans and assessments, including annual updates shall be incorporated into the contract as compliance documents.

(i) The IT system security plan shall be prepared consistent, in form and content, with NIST SP 800–18, Guide for Developing Security Plans for Federal Information Systems, and any additions/augmentations described in NASA Procedural Requirements (NPR) 2810, Security of Information Technology. The security plan shall identify and document appropriate IT security controls consistent with the sensitivity of the information and the requirements of Federal Information Processing Standards (FIPS) 200, Recommended Security Controls for Federal Information Systems. The plan shall be reviewed and updated in accordance with NIST SP 800–26, Security Self-Assessment Guide for Information Technology Systems, and FIPS 200, on a yearly basis.

(ii) The risk assessment shall be prepared consistent, in form and content, with NIST SP 800–30, Risk Management Guide for Information Technology Systems, and any additions/augmentations described in NPR 2810. The risk assessment shall be updated on a yearly basis.

(iii) The FIPS 199 assessment shall identify all information types as well as the ''high water mark,'' as defined in FIPS 199, of the processed, stored, or transmitted information necessary to fulfill the contractual requirements.

(2) The Contractor shall produce contingency plans consistent, in form and content, with NIST SP 800–34, Contingency Planning Guide for Information Technology Systems, and any additions/augmentations described in NPR 2810. The Contractor shall perform yearly ''Classroom Exercises.'' ''Functional Exercises,'' shall be coordinated with the Center CIOs and be conducted once every three years, with the first conducted within the first two years of contract award. These exercises are defined and described in NIST SP 800–34.

(3) The Contractor shall ensure coordination of its incident response team with the NASA Incident Response Center and the NASA Security Operations Center.

(4) 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 NPR 2810 requirements. The Contractor may use web-based training available from NASA to meet this requirement.

(5) The Contractor shall provide NASA, including the NASA 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 IT security inspection, investigation, and/or audits to safeguard against threats and hazards to the integrity, availability, and confidentiality of NASA information or to the function of computer systems operated on behalf of NASA, and to preserve evidence of computer crime. To facilitate mandatory reviews, the Contractor shall ensure appropriate compartmentalization of NASA information, stored and/or processed, either by information systems in direct support of the contract or that are incidental to the contract.

(6) The Contractor shall ensure that all individuals who perform tasks as a system administrator, or have authority to perform tasks normally performed by a system administrator, demonstrate knowledge appropriate to those tasks. Knowledge is demonstrated through the NASA System Administrator Security Certification Program. A system administrator is one who provides IT services, network services, files storage, and/or web services, to someone else other than themselves and takes or assumes the responsibility for the security and administrative controls of that service. Within 30 days after contract award, the Contractor shall provide to the Contracting Officer a list of all system administrator positions and personnel filling those positions, along with a schedule that ensures certification of all personnel within 90 days after contract award. Additionally, the Contractor should report all personnel changes which impact system administrator positions within 5 days of the personnel change and ensure these individuals obtain System Administrator certification within 90 days after the change.

(7) When the Contractor is located at a NASA Center or installation or is using NASA IP address space, the Contractor shall—

(i) Submit requests for non-NASA provided external Internet connections to the Contracting Officer for approval by the Network Security Configuration Control Board (NSCCB);

(ii) Comply with the NASA CIO metrics including patch management, operating systems and application configuration guidelines, vulnerability scanning, incident reporting, system administrator certification, and security training; and

(iii) Utilize the NASA Public Key Infrastructure (PKI) for all encrypted communication or non-repudiation requirements within NASA when secure e-mail capability is required.

(c) Physical and Logical Access Requirements.

(1) Contractor personnel requiring access to IT systems operated by the Contractor for NASA or interconnected to a NASA network shall be screened at an appropriate level in accordance with NPR 2810 and Chapter 4, NPR 1600.1, NASA Security Program Procedural Requirements. NASA shall provide screening, appropriate to the highest risk level, of the IT systems and information accessed, using, as a minimum, National Agency Check with Inquiries (NACI). 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 NASA, interim access may be granted pending completion of the required investigation and final access determination. For Contractors who will reside on a NASA Center or installation, the security screening required for all required access (*e.g.*, installation, facility, IT, information, etc.) is consolidated to ensure only one investigation is conducted based on the highest risk level. Contractors not residing on a NASA installation will be screened based on their IT access risk level determination only. See NPR 1600.1, Chapter 4.

(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'' information 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 information 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 established in Chapter 4, NPR 1600.1.

(4) The Contractor may conduct its own screening of individuals requiring privileged access or limited privileged access provided the Contractor can demonstrate to the Contracting Officer that the procedures used by the Contractor are equivalent to NASA's personnel screening procedures for the risk level assigned for the IT position.

(5) Subject to approval of the Contracting Officer, the Contractor may forgo screening of Contractor personnel for those individuals who have proof of a—

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

(ii) Screening conducted by NASA within the last three years that meets or exceeds the screening requirements of the IT position; or

(iii) Screening conducted by the Contractor, within the last three years, that is equivalent to the NASA personnel screening procedures as approved by the Contracting Officer and concurred on by the CCS.

(d) The Contracting Officer may waive the requirements of paragraphs (b) and (c)(1) through (c)(3) upon request of the Contractor. The Contractor shall provide all relevant information requested by the Contracting Officer to support the waiver request.

(e) The Contractor shall contact the Contracting Officer for any documents, information, or forms necessary to comply with the requirements of this clause.

(f) The Contractor shall insert this clause, including this paragraph (f), in all subcontracts when the subcontractor is required to:

(1) Have physical or electronic access to NASA's computer systems, networks, or IT infrastructure; or

(2) Use information systems to generate, store, or exchange data with NASA or on behalf of NASA, regardless of whether the data resides on a NASA or a contractor's information system.

[FR Doc. E6–12351 Filed 7–31–06; 8:45 am]

BILLING CODE 7510–01–P

DEPARTMENT OF THE INTERIOR

Fish and Wildlife Service

50 CFR Part 17

Endangered and Threatened Wildlife and Plants; 12-Month Finding on a Petition To Establish the Northern Rocky Mountain Gray Wolf Population (*Canis lupus*) as a Distinct Population Segment To Remove the Northern Rocky Mountain Gray Wolf Distinct Population Segment From the List of Endangered and Threatened Species

AGENCY: Fish and Wildlife Service, Interior.

ACTION: Notice of 12-month petition finding.

SUMMARY: We, the U.S. Fish and Wildlife Service (Service), announce a 12-month finding on a petition to establish the northern Rocky Mountain (NRM) gray wolf (*Canis lupus*) population as a Distinct Population Segment (DPS) and to remove the NRM gray wolf DPS from the Federal List of Endangered and Threatened Wildlife, under the Endangered Species Act of 1973, as amended (ESA). After review of all available scientific and commercial information, we find that the petitioned action is not warranted. We have determined that Wyoming State law and its wolf management plan do not provide the necessary regulatory mechanisms to assure that Wyoming's numerical and distributional share of a recovered NRM wolf population would be conserved if the protections of the ESA were removed.

DATES: The finding announced in this document was made on August 1, 2006.

ADDRESSES: Comments and materials received, as well as supporting documentation used in the preparation of this 12-month finding, will be available for public inspection, by appointment, during normal business hours at U.S. Fish and Wildlife Service,