converter or subscription service, may be unprepared for the digital transition when it arrives, and may be unable to obtain critical information in emergencies after the transition. In such instances, consumers would be financially harmed and deprived of service at a critical time. We are concerned that delay in the effective date of the disclosure requirement will result in additional analog-only equipment being sold to uninformed consumers due to the absence of appropriate disclosure, thereby harming consumers and undermining the goal of the rule. Parties subject to the rule will have a reasonable opportunity to comply with it, particularly in light of the fact that it will not be effective until OMB approval. Because delay can result in such harms to consumers and because affected parties will be afforded a reasonable opportunity to comply with the rule, we find that there is good cause to expedite the effective date of this rule. We are also requesting emergency PRA approval from OMB.

38. *It is further ordered* that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, shall send a copy of this Second Report and Order, including the Final Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

39. *It is further ordered* that the Commission shall send a copy of this Second Report and Order in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act, see 5 U.S.C. 801(a)(1)(A).

List of Subjects in 47 CFR Part 15

Radio frequency devices.

Federal Communications Commission.

Marlene H. Dortch,

Secretary.

Rule Changes

■ For the reasons discussed in the preamble, the FCC amends 47 CFR part 15 as follows:

PART 15—RADIO FREQUENCY DEVICES

■ 1. The authority citation for part 15 continues to read as follows:

Authority: 47 U.S.C. 154, 302, 303, 304, 307, 336, and 544A.

■ 2. Section 15.117 is amended by adding paragraph (k) to read as follows:

§ 15.117 TV broadcast receivers.

* * * * *

(k) The following requirements apply to all responsible parties, as defined in § 2.909 of this chapter, and any person that displays or offers for sale or rent television receiving equipment that is not capable of receiving, decoding and tuning digital signals.

(1) Such parties and persons shall place conspicuously and in close proximity to such television broadcast receivers a sign containing, in clear and conspicuous print, the Consumer Alert disclosure text required by paragraph (k)(3) of this section. The text should be in a size of type large enough to be clear, conspicuous and readily legible, consistent with the dimensions of the equipment and the label. The information may be printed on a transparent material and affixed to the screen, if the receiver includes a display, in a manner that is removable by the consumer and does not obscure the picture, or, if the receiver does not include a display, in a prominent location on the device, such as on the top or front of the device, when displayed for sale, or the information in this format may be displayed separately immediately adjacent to each television broadcast receiver offered for sale and clearly associated with the analog-only model to which it pertains.

(2) If such parties and persons display or offer for sale or rent such television broadcast receivers via direct mail, catalog, or electronic means, they shall prominently display in close proximity to the images or descriptions of such television broadcast receivers, in clear and conspicuous print, the Consumer Alert disclosure text required by paragraph (k)(3) of this section. The text should be in a size large enough to be clear, conspicuous, and readily legible, consistent with the dimensions of the advertisement or description.

(3) *Consumer alert.* This television receiver has only an analog broadcast tuner and will require a converter box after February 17, 2009, to receive over-the-air broadcasts with an antenna because of the Nation's transition to digital broadcasting. Analog-only TVs should continue to work as before with cable and satellite TV services, gaming consoles, VCRs, DVD players, and similar products. For more information, call the Federal Communications Commission at 1–888–225–5322 (TTY: 1–888–835–5322) or visit the Commission's digital television Web site at: *http://www.dtv.gov.*

[FR Doc. 07–2318 Filed 5–9–07; 8:45 am]

BILLING CODE 6712–01–P

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: Final rule.

SUMMARY: NASA is amending 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.

EFFECTIVE DATE: This final rule is effective May 10, 2007.

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 published a proposed rule in the **Federal Register** (71 FR 43408–43410) on August 1, 2006. The sixty day comment period expired October 2, 2006. Four comments were received from two respondents. A summary of the comments and NASA responses follows.

Comment: The clause is ''* * * not appropriate in situations where university contractors develop data and software to which NASA has access and the right to use, but is owned by the university under normal FAR and NFS provisions for university research contracts'' and should not ''* * * be included when the contractor will simply be delivering software or data in electronic format to the government, unless the government will be the sole and exclusive owner of such delivered software or data * * *.''

NASA Response: FISMA requires agencies to protect their information and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. This is a data protection, and not an ownership, issue.

Accordingly, the NASA clause which implements the FISMA requirements applies to contracts that require the contractor to process, store, or transmit NASA data, regardless of whether the contractors owns the underlying systems or software. Ownership of systems or software is not a determining factor for clause applicability. We note that the NASA clause is only inserted in contracts when the conditions specified in 1804.470–4 apply. The clause is not used in contracts that merely require the delivery of contractor-owned software.

Comment: The industry screening standard requirement for university personnel is the NACLC (National Agency Check + Local Agency Check) which does not satisfy the new requirement in the clause for an NACI (National Agency Check with Inquiries) and a new clearance will need to be obtained under the latter standard.

NASA Response: The screening requirement is established by Homeland Security Presidential Directive (HSPD)–12 for all Federal agencies, and NASA does not have the discretion to revise this standard.

Comment: Paragraph (d) of the proposed clause at 1852.204–76 permits the contracting officer to grant waivers to certain of its requirements, but does not provide approval criteria to assist the contracting officer review of the request.

NASA Response: Approval of waiver requests depends on the individual circumstances associated with each contract; therefore, a blanket set of approval criteria is inappropriate. Waiver requests will be reviewed and approved as necessary on a case-by-case basis.

Comment: The change of the physical security requirement in the proposed rule from a National Agency Check to a National Agency Check with Inquiries creates a concern in that the security measures cited pertain to personnel, not physical, security controls.

NASA Response: The cited requirement does not pertain to physical security controls, but rather physical and logical access of personnel into NASA facilities. NASA believes that the clause is clear on this issue and no further change is necessary.

Although NASA has not made changes to the proposed rule as a result of public comments, the following changes have been made to the clause at 1852.204–76. These changes are intended to improve the readability and clarify specific requirements of the clause, and NASA does not believe that these changes require publication for public comment. NASA is also deleting NFS 1804.402 since it contains obsolete references.

1. Paragraph (a) of the clause is restructured into two subparagraphs to improve readability.

2. Paragraph (b)(3) is revised to cite the specific NIST SP 800–61 standard for incident reporting and the U.S. Computer Emergency Readiness Team's (US–CERT) Concept of Operations for reporting security incidents.

3. Paragraph (b)(6) is clarified to specify which system administrators are subject to the NASA System Administrator Security Certification Program.

4. Paragraph (b)(7) is moved to a new paragraph (b)(8).

5. Paragraph (b)(7) is clarified to specify that sensitive but unclassified information is required to be encrypted.

6. Paragraph (f)(2) is clarified to specify closeout procedures related to IT resources at the completion or expiration of the contract.

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 final 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 rule merely summarizes 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.

Sheryl Goddard,

Acting Assistant 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

1804.402 [Removed]

■ 2. Section 1804.402 is removed.

■ 3. Sections 1804.470, 1804.470–1, 1804.470–2 , 1804.470–3, and 1804.470–4 are revised 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.*), 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, processed, 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, process, 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

■ 4. Section 1852.204–76 is revised 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 (MAY 2007)

(a) The Contractor shall be responsible for information and information technology (IT) security when—

(1) 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

(2) 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, processed, 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 (NASIRC) and the NASA Security Operations Center, ensuring that incidents are reported consistent with NIST SP 800–61, Computer Security Incident Reporting Guide, and the United States Computer Emergency Readiness Team's (US–CERT) Concept of Operations for reporting security incidents. Specifically, any confirmed incident of a system containing NASA data or controlling NASA assets shall be reported to NASIRC within one hour that results in unauthorized access, loss or modification of NASA data, or denial of service affecting the availability of NASA data.

(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 system administrators who perform tasks that have a material impact on IT security and operations 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 (including network services, file storage, and/or web services) to someone 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) The Contractor shall ensure that NASA's Sensitive But Unclassified (SBU) information as defined in NPR 1600.1, NASA Security Program Procedural Requirements, which includes privacy information, is encrypted in storage and transmission.

(8) 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 email 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) At the completion of the contract, the contractor shall return all NASA information and IT resources provided to the contractor during the performance of the contract and certify that all NASA information has been purged from contractor-owned systems used in the performance of the contract.

(g) The Contractor shall insert this clause, including this paragraph (g), in all subcontracts:

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

(2) Use information systems to generate, store, process, 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.

(End of clause)

[FR Doc. E7–9057 Filed 5–9–07; 8:45 am]

BILLING CODE 7510–01–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

50 CFR Part 648

[Docket No. 070321063–7098–02; I.D. 031607E]

RIN 0648–AV22

Magnuson-Stevens Fishery Conservation and Management Act Provisions; Fisheries of the Northeastern United States; Northeast Multispecies Fishery; 2007 Georges Bank Cod Fixed Gear Sector Operations Plan and Agreement and Allocation of Georges Bank Cod Total Allowable Catch

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

ACTION: Final rule.

SUMMARY: NMFS announces approval of an Operations Plan and Sector Contract for the Georges Bank (GB) Cod Fixed Gear Sector (Fixed Gear Sector) entitled: ''GB Cod Fixed Gear Sector Operations Plan and Agreement'' (together referred to as the Sector Operations Plan), and the associated allocation of GB cod for fishing year (FY) 2007. The intent of this action is to allow regulated harvest of Northeast (NE) multispecies by the Fixed Gear Sector, consistent with the Operations Plan and objectives of the NE Multispecies Fishery Management Plan (FMP).

DATES: Effective May 4, 2007, through April 30, 2008.

ADDRESSES: Copies of the Fixed Gear Sector Operations Plan and the Environmental Assessment (EA) are available upon request from the NE Regional Office at the following mailing address: George H. Darcy, Assistant Regional Administrator for Sustainable Fisheries, NMFS, Northeast Regional Office, 1 Blackburn Drive, Gloucester, MA 01930. These documents may also be requested by calling (978) 281–9315.

FOR FURTHER INFORMATION CONTACT: Mark Grant, Fishery Management Specialist, phone (978) 281–9145, fax (978) 281–9135, e-mail *Mark.Grant@NOAA.gov*.

SUPPLEMENTARY INFORMATION: Framework Adjustment (FW) 42 (71 FR 62156, October 23, 2006) authorized the Fixed Gear Sector and authorized the Regional Administrator to allocate a GB cod total allowable catch (TAC) to the Fixed Gear Sector and exempt members from FMP restrictions on an annual