(b) *Section 18 emergency exemptions.* [Reserved]

* * * * *

■ 29. In § 180.479, revise paragraph (b) to read as follows:

§ 180.479 Halosulfuron-methyl; tolerances for residues.

* * * * *

(b) *Section 18 emergency exemptions.* [Reserved]

* * * * *

■ 30. In § 180.480, revise paragraph (b) to read as follows:

§ 180.480 Fenbuconazole; tolerances for residues.

* * * * *

(b) *Section 18 emergency exemptions.* [Reserved]

* * * * *

§ 180.483 [Removed]

■ 31. Remove § 180.483.

■ 32. In § 180.493, revise paragraph (d) to read as follows:

§ 180.493 Dimethomorph; tolerances for residues.

* * * * *

(d) *Indirect or inadvertent residues.* [Reserved]

■ 33. In § 180.515, revise paragraph (b) to read as follows:

§ 180.515 Carfentrazone-ethyl; tolerances for residues.

* * * * *

(b) *Section 18 emergency exemptions.* [Reserved]

* * * * *

■ 34. In § 180.544, revise paragraph (d) to read as follows:

§ 180.544 Methoxyfenozide; tolerances for residues.

* * * * *

(d) *Indirect or inadvertent residues.* [Reserved]

§ 180.549 [Amended]

■ 35. In § 180.549, remove paragraph (a)(2) and redesignate paragraph (a)(1) as paragraph (a).

■ 36. In § 180.561, revise paragraph (b) to read as follows:

§ 180.561 Acibenzolar-S-methyl; tolerances for residues.

* * * * *

(b) *Section 18 emergency exemptions.* [Reserved]

* * * * *

■ 37. In § 180.571, revise paragraph (b) to read as follows:

§ 180.571 Mesotrione; tolerances for residues.

* * * * *

(b) *Section 18 emergency exemptions.* [Reserved]

* * * * *

■ 38. In § 180.586, revise paragraph (b) to read as follows:

§ 180.586 Clothianidin; tolerances for residues.

* * * * *

(b) *Section 18 emergency exemptions.* [Reserved]

* * * * *

[FR Doc. 2011–14569 Filed 6–14–11; 8:45 am]

BILLING CODE 6560–50–P

GENERAL SERVICES ADMINISTRATION

48 CFR Parts 539 and 552

[GSAR Amendment 2011–02; GSAR Case 2011–G503; (Change 50); Docket 2011–0012, Sequence 1]

RIN 30900–AJ15

General Services Administration Acquisition Regulation; Implementation of Information Technology Security Provision

AGENCY: Office of Acquisition Policy, General Services Administration (GSA).

ACTION: Interim rule.

SUMMARY: The General Services Administration (GSA) is issuing an interim rule amending the General Services Administration Acquisition Regulation (GSAR) to revise sections to implement policy and guidelines for contracts and orders that include information technology (IT) supplies, services and systems with security requirements.

DATES: *Effective Date:* June 15, 2011.

Applicability Date: This amendment applies to contracts and orders awarded after the effective date that include information technology (IT) supplies, services and systems with security requirements.

Comment Date: Interested parties should submit written comments to the Regulatory Secretariat at the address shown below on or before August 15, 2011 to be considered in the formulation of a final rule.

ADDRESSES: Submit comments identified by GSAR Case 2011–G503, by any of the following methods:

- *Regulations.gov: http://www.regulations.gov.* Submit comments via the Federal eRulemaking portal by inputting ''GSAR Case 2011–G503'' under the heading ''Enter Keyword or ID'' and selecting ''Search.'' Select the link ''Submit a Comment'' that corresponds with ''GSAR Case 2011–G503.'' Follow the instructions provided at the ''Submit a Comment'' screen. Please include your name, company name (if any), and ''GSAR Case 2011–G503'' on your attached document.
- *Fax:* (202) 501–4067.
- *Mail:* General Services Administration, Regulatory Secretariat (MVCB), ATTN: Hada Flowers, 1275 First Street, NE., 7th Floor, Washington, DC 20417.

Instructions: Please submit comments only and cite GSAR Case 2011–G503, in all correspondence related to this case. All comments received will be posted without change to *http://www.regulations.gov,* including any personal and/or business confidential information provided.

FOR FURTHER INFORMATION CONTACT: Ms. Deborah Lague, Procurement Analyst, at (202) 694–8149, for clarification of content. For information pertaining to status or publication schedules, contact the Regulatory Secretariat at (202) 501–4755. Please cite GSAR Case 2011–G503.

SUPPLEMENTARY INFORMATION:

I. Background

To verify that GSA has met the requirements of the Federal Information Security Management Act of 2002 (FISMA), GSA's Office of the Inspector General (OIG) conducted an audit of GSA's information and information technology systems. In regards to the regulatory process, a recommendation was made by the OIG to strengthen the requirements in contracts and orders for information technology supplies, services and systems. Working with the Office of the Chief Information Officer (CIO), the Office of Acquisition Policy developed the policy, guidance and requirements that would be utilized to protect GSA's information and information technology systems, regardless of the location. The actual requirements are currently being utilized in solicitations, contracts and orders issued by the CIO; however, they were not included in the GSAR. By revising the GSAR to include these requirements, GSA is agreeing with the recommendation of the OIG and strengthens the protection of information and information systems.

II. GSAR Changes

The following are the changes to GSAR part 507, Acquisition Planning; Subpart 511.1, Selecting and Developing Requirement Documents; part 539,

Acquisition of Information Technology; and part 552, Solicitation Provisions and Contract Clauses.

This interim rule amends the title of GSAM Subpart 507.70 to clarify that this part only applies to requirements for the purchase of information technology in support of national security systems involving weapons systems. The GSAM is a non-regulatory portion of the manual.

GSAM 511.102 is being added to provide the policy as it relates to contracts and orders for government data, information technology, supplies, services and systems in accordance with GSA policy and procedures guide. The GSAM is a non-regulatory portion of the manual.

GSAM 539.001 is amended to indicate that this subpart does not apply to information technology supplies, services and systems in support of national security systems. The GSAM is a non-regulatory portion of the manual.

New subpart 539.70 is added to provide the policy as it relates to contracts and orders for information technology supplies, services and systems that do not involve national security systems.

GSAR part 552 was amended to add a new provision, 552.239–70, Information Technology Security Plan and Security Authorization; and a new clause, 552.239–71, Security Requirements for Unclassified Information Technology Resources, that relates to the policy requirements described in GSAR Part 539.

III. Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This is a significant regulatory action and, therefore, was subject to review under Section 6(b) of E.O. 12866, Regulatory Planning and Review, dated September 30, 1993. This rule is not a major rule under 5 U.S.C. 804.

IV. Regulatory Flexibility Act

This interim rule may 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 the rule requires contractors, within 30 days after contract award to submit an IT Security Plan to the Contracting Officer and Contracting Officer's Representative that describes the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under the contract. The rule will also require that contractors submit written proof of IT security authorization six months after award, and verify that the IT Security Plan remains valid annually. Where this information is not already available, this may mean small businesses will need to become familiar with the requirements, research the requirements, develop the documents, submit the information, and create the infrastructure to track, monitor and report compliance with the requirements. However, GSA expects that the impact will be minimal, because the clause includes requirements that IT service contractors should be familiar with through other agency clauses, existing GSA IT security requirements, and Federal laws and guidance. Small businesses are active providers of IT services.

The Regulatory Secretariat has submitted a copy of the Initial Regulatory Flexibility Analysis (IRFA) to the Chief Counsel for Advocacy of the Small Business Administration. A copy of the IRFA may be obtained from the Regulatory Secretariat. The Councils invite comments from small business concerns and other interested parties on the expected impact of this rule on small entities.

GSA will also consider comments from small entities concerning the existing regulations in subparts affected by this rule in accordance with 5 U.S.C. 610. Interested parties must submit such comments separately and should cite 5 U.S.C. 610 (GSAR Case 2011–G503) in correspondence.

The analysis is summarized as follows:

This rule will require that contractors submit an IT Security Plan that complies with applicable Federal laws including, 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 GSA policies and procedures.

GSA will use this information to verify that the contractor is securing GSA's information technology data and systems from unauthorized use, as well as use the information to assess compliance and measure progress in carrying out the requirements for IT security.

The requirements for submission of the plan will be inserted in solicitations that include information technology supplies, services or systems in which the contractor will have physical or electronic access to government information that directly supports the mission of GSA. As such it is believed that contract actions awarded to small business will be identified in FPDS under the Product Service Code D—ADP and Telecommunication Services. The requirements of the plan apply to all work performed under the contract; whether performed by the prime contractor or subcontractor.

Based on the average of Fiscal Years 2009 and 2010 Federal Procurement Data System retrieved, it is estimated that 80 small businesses will be affected annually.

GSA did not identify any significant alternatives that would accomplish the objectives of the rule. Collection of information on a basis other than by individual contractors is not practical. The contractor is the only one who has the records necessary for the collection.

V. Paperwork Reduction Act

The Paperwork Reduction Act (44 U.S.C. chapter 35) applies because the interim rule contains information collection requirements. Accordingly, the Regulatory Secretariat will submit a request for approval of a new information collection requirement concerning Security Requirements for Unclassified Information Technology Resources (GSAR 552.239–70) to the Office of Management and Budget.

Annual Reporting Burden

Public reporting burden for this collection of information is estimated to average 5 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information.

The annual reporting burden is estimated as follows:

Respondents: 147.
Responses per respondent: 2.
Total annual responses: 294.
Preparation hours per response: 5.
Total response burden hours: 1,470.

VI. Request for Comments Regarding Paperwork Burden

Submit comments, including suggestions for reducing this burden, not later than August 15, 2011 by any of the following methods:

- *Regulations.gov: http://www.regulations.gov.*

Submit comments via the Federal eRulemaking portal by inputting ''GSAR case 2011–G503'' under the heading ''Enter Keyword or ID'' and selecting ''Search''. Select the link ''Submit a Comment'' that corresponds with ''GSAR case 2011–G503''. Follow the instructions provided at the ''Submit a Comment'' screen. Please include your

name, company name (if any), and ''GSAR case 2011–G503'' on your attached document.

- *Fax:* 202–501–4067.
- *Mail:* General Services Administration, Regulatory Secretariat (MVCB), 1275 First Street, NE., Washington, DC 20417. ATTN: Hada Flowers/GSAR case 2011–G503.

Instructions: Please submit comments only and cite GSAR case 2011–G503, in all correspondence related to this collection. All comments received will be posted without change to *http://www.regulations.gov,* including any personal and/or business confidential information provided.

Public comments are particularly invited on: Whether this collection of information is necessary for the proper performance of functions of the GSAR, and will have practical utility; whether our estimate of the public burden of this collection of information is accurate, and based on valid assumptions and methodology; ways to enhance the quality, utility, and clarity of the information to be collected; and ways in which we can minimize the burden of the collection of information on those who are to respond, through the use of appropriate technological collection techniques or other forms of information technology.

Requester may obtain a copy of the supporting statement from the General Services Administration, Regulatory Secretariat (MVCB), 1275 First Street, NE., 7th Floor, Washington, DC 20417. Please cite OMB Control Number 3090–0294, Title: Security Requirements for Unclassified Information Technology Resources (GSAR 552.239–71), in correspondence.

VII. Determination To Issue an Interim Rule

A determination has been made under the authority of the Administrator of General Services (GSA) that urgent and compelling reasons exist to promulgate this interim rule without prior opportunity for public comment. This action is necessary because GSA must provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Section 3544(a)(1)(A)(ii) of the Federal Information Security Management Act (FISMA) describes Federal agency security responsibilities as including ''information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.''

However, pursuant to 41 U.S.C. 418b and FAR 1.501, GSA will consider public comments received in response to this interim rule in the formation of the final rule.

List of Subjects in 48 CFR Parts 539 and 552

Government procurement.

Dated: June 9, 2011.

Joseph A. Neurauter,

Senior Procurement Executive, Office of Acquisition Policy, General Services Administration.

Therefore, GSA amends 48 CFR parts 539 and 552 as set forth below:

■ 1. Part 539 is added to read as follows:

PART 539—ACQUISITION OF INFORMATION TECHNOLOGY

Subpart 539.70—Additional Requirements for Purchases Not in Support of National Security Systems

Sec.

Authority: 40 U.S.C. 121(c).

Subpart 539.70—Additional Requirements for Purchases Not in Support of National Security Systems

539.7000 Scope of subpart.

This subpart prescribes acquisition policies and procedures for use in acquiring information technology supplies, services and systems not in support of national security systems, as defined by FAR part 39.

539.7001 Policy.

(a) GSA must provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Section 3544(a)(1)(A)(ii) of the Federal Information Security Management Act (FISMA) describes Federal agency security responsibilities as including ''information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.''

(b) Employees responsible for or procuring information technology supplies, services and systems shall possess the appropriate security clearance associated with the level of security classification related to the acquisition. They include, but are not limited to contracting officers, contract specialists, project/program managers, and contracting officer representatives.

(c) Contracting activities shall coordinate with requiring activities and program officials to ensure that the solicitation documents include the appropriate information security requirements. The information security requirements must be sufficiently detailed to enable service providers to fully understand the information security regulations, mandates, and requirements that they will be subject to under the contract or task order.

(d) GSA's Office of the Senior Agency Information Security Officer issued CIO IT Security Procedural Guide 09–48, ''Security Language for Information Technology Acquisitions Efforts,'' to provide IT security standards, policies and reporting requirements that shall be inserted in all solicitations and contracts or task orders where an information system is contractor owned and operated on behalf of the Federal Government. The guide can be accessed at *http://www.gsa.gov/portal/category/25690.*

539.7002 Solicitation provisions and contract clauses.

(a) The contracting officer shall insert the provision at 552.239–70, Information Technology Security Plan and Security Authorization, in solicitations that include information technology supplies, services or systems in which the contractor will have physical or electronic access to government information that directly supports the mission of GSA.

(b) The contracting officer shall insert the clause at 552.239–71, Security Requirements for Unclassified Information Technology Resources, in solicitations and contracts containing the provision at 552.239–70. The provision and clause shall not be inserted in solicitations and contracts for personal services with individuals.

PART 552—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

■ 2. The authority citation for 48 CFR part 552 continues to read as follows:

Authority: 40 U.S.C. 121(c).

■ 3. Add sections 552.239–70 and 552.239–71 to read as follows:

552.239–70 Information Technology Security Plan and Security Authorization.

As prescribed in 539.7002(a), insert the following provision:

Information Technology Security Plan and Security Authorization (JUN 2011)

All offers/bids submitted in response to this solicitation must address the approach for completing the security plan and certification and security authorization requirements as required by the clause at 552.239–71, Security Requirements for

Unclassified Information Technology Resources.

(End of provision)

552.239–71 Security Requirements for Unclassified Information Technology Resources.

As prescribed in 539.7002(b), insert the following clause:

Security Requirements for Unclassified Information Technology Resources (JUN 2011)

(a) *General.* The Contractor shall be responsible for information technology (IT) security, based on General Services Administration (GSA) risk assessments, for all systems connected to a GSA network or operated by the Contractor for GSA, 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 GSA's information that directly supports the mission of GSA, as indicated by GSA. 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, control, display, switching, interchange, transmission, or reception of data or information. This includes major applications as defined by OMB Circular A–130. Examples of tasks that require security provisions include:

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

(2) Acquisition, transmission, or analysis of data owned by GSA with significant replacement cost should the Contractors copy be corrupted;

(3) Access to GSA major applications at a level beyond that granted the general public; *e.g.*, bypassing a firewall; and

(4) Any new information technology systems acquired for operations within the GSA must comply with the requirements of HSPD–12 and OMB M–11–11. Usage of the credentials must be implemented in accordance with OMB policy and NIST guidelines (*e.g.,* NIST SP 800–116). The system must operate within the GSA's access management environment. Exceptions must be requested in writing and can only be granted by the GSA Senior Agency Information Security Officer.

(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 Contractors 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 GSA policies and procedures. GSA's Office of the Chief Information Officer issued ''CIO IT Security Procedural Guide 09–48, Security Language for Information Technology Acquisitions Efforts,'' to provide IT security standards, policies and reporting requirements. This document is incorporated by reference in all solicitations and contracts or task orders where an information system is contractor owned and operated on behalf of the Federal Government. The guide can be accessed at *http://www.gsa.gov/portal/category/25690.* Specific security requirements not specified in ''CIO IT Security Procedural Guide 09–48, Security Language for Information Technology Acquisitions Efforts'' shall be provided by the requiring activity.

(c) *Submittal of IT Security Plan.* Within 30 calendar days after contract award, the Contractor shall submit the IT Security Plan to the Contracting Officer and Contracting Officers Representative (COR) for acceptance. This plan shall be consistent with and further detail the approach contained in the contractors 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) *Submittal of a Continuous Monitoring Plan.* The Contractor must develop a continuous monitoring strategy that includes:

(1) A configuration management process for the information system and its constituent components;

(2) A determination of the security impact of changes to the information system and environment of operation;

(3) Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;

(4) Reporting the security state of the information system to appropriate GSA officials; and

(5) All GSA general support systems and applications must implement continuous monitoring activities in accordance with this guide and NIST SP 800–37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.*

(e) *Security authorization.* Within six (6) months after contract award, the Contractor shall submit written proof of IT security authorization for acceptance by the Contracting Officer. Such written proof may be furnished either by the Contractor or by a third party. The security authorization must be in accordance with NIST Special Publication 800–37. This security authorization will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This security authorization, 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 security authorization documentation.

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

(g) *Warning notices.* The Contractor shall ensure that the following banners are displayed on all GSA 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 General Services Administration policy, and may result in criminal or administrative penalties. Users shall not access other users or system files without proper authority. Absence of access controls IS NOT authorization for access! GSA 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**

(h) *Privacy Act notification.* The Contractor shall ensure that the following banner is displayed on all GSA 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.

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

(j) *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 the rules of behavior.

(k) *Government access.* The Contractor shall afford the Government access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, IT systems and devices, and personnel used in performance of the contract, regardless of the location. Access shall be provided to the extent required, in the Government's judgment, to conduct an IT inspection, investigation or audit, including vulnerability testing to safeguard against

threats and hazards to the integrity, availability and confidentiality of GSA data or to the function of information technology systems operated on behalf of GSA, and to preserve evidence of computer crime. This information shall be available to GSA upon request.

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

(m) *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 GSA information systems or data. If an employee's employment is terminated, for any reason, access to GSA's information systems or data shall be immediately disabled and the credentials used to access the information systems or data shall be immediately confiscated.

(n) *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)

[FR Doc. 2011–14728 Filed 6–14–11; 8:45 am]

BILLING CODE 6820–61–P

DEPARTMENT OF TRANSPORTATION

Federal Railroad Administration

49 CFR Part 213

[Docket No. FRA–2009–0007, Notice No. 3]

RIN 2130–AC01

Track Safety Standards; Concrete Crossties

AGENCY: Federal Railroad Administration (FRA), Department of Transportation (DOT).

ACTION: Final rule; delay of effective date.

SUMMARY: This document delays the effectiveness of the final rule, which mandates specific requirements for effective concrete crossties, for rail fastening systems connected to concrete crossties, and for automated inspections of track constructed with concrete crossties. The Track Safety Standards were amended via final rule on April 1, 2011, and the final rule was scheduled to take effect on July 1, 2011. FRA received two petitions for reconsideration in response to the final rule that contain substantive issues requiring a detailed response. Accordingly, in order to fully respond to the petitions for reconsideration, this document delays the effective date of the final rule until October 1, 2011.

DATES: The effective date for the final rule published April 1, 2011, at 76 FR 18073, effective July 1, 2011, is delayed until October 1, 2011.

FOR FURTHER INFORMATION CONTACT: Kenneth Rusk, Staff Director, Office of Railroad Safety, FRA, 1200 New Jersey Avenue, SE., Washington, DC 20590 (telephone: (202) 493–6236); or Veronica Chittim, Trial Attorney, Office of Chief Counsel, FRA, 1200 New Jersey Avenue, SE., Washington, DC 20950 (telephone: (202) 493–0273).

SUPPLEMENTARY INFORMATION: On April 1, 2011, FRA published a final rule mandating specific requirements for effective concrete crossties, for rail fastening systems connected to concrete crossties, and for automated inspections of track constructed with concrete crossties. See 76 FR 18073. The effective date of this final rule was to be July 1, 2011. FRA received two petitions for reconsideration in response to the final rule that contain substantive issues requiring a detailed response from FRA. Accordingly, in order to allow FRA appropriate time to consider and fully respond to the petitions for reconsideration, this document delays the effective date of the final rule until October 1, 2011. Therefore, any requirements imposed by the final rule need not be complied with until October 1, 2011.

List of Subjects in 49 CFR Part 213

Penalties, Railroad safety, Reporting and recordkeeping requirements.

The Final Rule

In consideration of the foregoing, FRA delays the effective date of the final rule until October 1, 2011.

Issued in Washington, DC, on June 9, 2011.

Joseph C. Szabo,

Administrator.

[FR Doc. 2011–14835 Filed 6–10–11; 4:15 pm]

BILLING CODE 4910–06–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

50 CFR Part 300

[Docket No. 110601314–1313–01]

RIN 0648–BA99

Pacific Halibut Fisheries; Limited Access for Guided Sport Charter Vessels in Alaska

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

ACTION: Interpretative rule.

SUMMARY: This rule clarifies regulations that apply to vessels operating in the guided sport (charter) fishery for halibut in International Pacific Halibut Commission Regulatory Area 2C (Southeast Alaska) and Area 3A (Central Gulf of Alaska). Under regulations implementing the charter halibut limited access program, operators of a vessel in Area 2C or Area 3A with one or more charter vessel anglers onboard that catch and retain halibut must have an Alaska Department of Fish and Game (ADF&G) Saltwater Charter Logbook onboard which specifies the person named on the charter halibut permit(s) being used onboard the vessel, and the charter halibut permit number(s) being used onboard the vessel. This interpretation clarifies that a charter operator may use the ADF&G Saltwater Charter Logbook issued for the vessel to record the charter halibut permit information. A charter vessel operator is not required to have a separate ADF&G Saltwater Charter Logbook issued in the name of the charter halibut permit holder.

DATES: This rule is effective on June 15, 2011.

ADDRESSES: Electronic copies of this action and other related documents are available from *http://www.regulations.gov* or from the NMFS Alaska Region Web site at *http://alaskafisheries.noaa.gov*.

FOR FURTHER INFORMATION CONTACT: Gwen Herrewig, 907–586–7228.

SUPPLEMENTARY INFORMATION:

Background

The International Pacific Halibut Commission (IPHC) and NMFS manage fishing for Pacific halibut (*Hippoglossus stenolepis*) through regulations established under authority of the Northern Pacific Halibut Act of 1982 (Halibut Act). Sections 773c(a) and (b) of the Halibut Act provide the Secretary of Commerce (Secretary) with general responsibility to carry out the Convention between the United States and Canada for the Preservation of the Halibut Fishery of the North Pacific Ocean and Bering Sea and the Halibut Act. Section 773c(c) of the Halibut Act also authorizes the North Pacific Fishery Management Council (Council) to develop regulations, including limited access regulations, that are in addition to, and not in conflict with, approved IPHC regulations. Such Council-developed regulations may be implemented by NMFS only after approval by the Secretary. The Council has exercised this authority in the development of its limited access program for charter vessels in the