

NOTICE OF OFFICE OF MANAGEMENT AND BUDGET ACTION

Date 06/07/2011

Department of Commerce  
National Oceanic and Atmospheric Administration  
FOR CERTIFYING OFFICIAL: Simon Szykman  
FOR CLEARANCE OFFICER: Diana Hynek

In accordance with the Paperwork Reduction Act, OMB has taken action on your request received 12/13/2010

ACTION REQUESTED: Extension without change of a currently approved collection  
TYPE OF REVIEW REQUESTED: Regular  
ICR REFERENCE NUMBER: 201012-0648-006  
AGENCY ICR TRACKING NUMBER:  
TITLE: Vessel Monitoring System Requirements in the Western Pacific Pelagic Longline Fishery, American Samoa Longline and Commonwealth of the Northern Mariana Islands Bottomfish Fisheries  
LIST OF INFORMATION COLLECTIONS: See next page

OMB ACTION: Approved without change  
OMB CONTROL NUMBER: 0648-0441  
The agency is required to display the OMB Control Number and inform respondents of its legal significance in accordance with 5 CFR 1320.5(b).

EXPIRATION DATE: 06/30/2014 DISCONTINUE DATE:

BURDEN:	RESPONSES	HOURS	COSTS
Previous	1,436,640	399	0
New	85	170	0
Difference			
Change due to New Statute	0	0	0
Change due to Agency Discretion	0	0	0
Change due to Agency Adjustment	-1,436,555	-229	0
Change Due to Potential Violation of the PRA	0	0	0

TERMS OF CLEARANCE:

OMB Authorizing Official: Kevin F. Neyland  
Deputy Administrator,  
Office Of Information And Regulatory Affairs

List of ICs

IC Title	Form No.	Form Name	CFR Citation
Vessel Monitoring System Requirements in the Western Pacific Pelagic Longline Fishery			50 CFR 665.19

# PAPERWORK REDUCTION ACT SUBMISSION

**Please read the instructions before completing this form. For additional forms or assistance in completing this form, contact your agency's Paperwork Clearance Officer. Send two copies of this form, the collection instrument to be reviewed, the supporting statement, and any additional documentation to: Office of Information and Regulatory Affairs, Office of Management and Budget, Docket Library, Room 10102, 725 17th Street NW, Washington, DC 20503.**

1. Agency/Subagency originating request	2. OMB control number <span style="float: right;">b. <input type="checkbox"/> None</span> a. _____ - _____
3. Type of information collection ( <i>check one</i> ) a. <input type="checkbox"/> New Collection b. <input type="checkbox"/> Revision of a currently approved collection c. <input type="checkbox"/> Extension of a currently approved collection d. <input type="checkbox"/> Reinstatement, without change, of a previously approved collection for which approval has expired e. <input type="checkbox"/> Reinstatement, with change, of a previously approved collection for which approval has expired f. <input type="checkbox"/> Existing collection in use without an OMB control number For b-f, note Item A2 of Supporting Statement instructions	4. Type of review requested ( <i>check one</i> ) a. <input type="checkbox"/> Regular submission b. <input type="checkbox"/> Emergency - Approval requested by _____ / _____ / _____ c. <input type="checkbox"/> Delegated
	5. Small entities Will this information collection have a significant economic impact on a substantial number of small entities? <input type="checkbox"/> Yes <input type="checkbox"/> No
	6. Requested expiration date a. <input type="checkbox"/> Three years from approval date b. <input type="checkbox"/> Other Specify: _____ / _____
7. Title	
8. Agency form number(s) ( <i>if applicable</i> )	
9. Keywords	
10. Abstract	
11. Affected public ( <i>Mark primary with "P" and all others that apply with "x"</i> ) a. ___ Individuals or households d. ___ Farms b. ___ Business or other for-profit e. ___ Federal Government c. ___ Not-for-profit institutions f. ___ State, Local or Tribal Government	12. Obligation to respond ( <i>check one</i> ) a. <input type="checkbox"/> Voluntary b. <input type="checkbox"/> Required to obtain or retain benefits c. <input type="checkbox"/> Mandatory
13. Annual recordkeeping and reporting burden a. Number of respondents _____ b. Total annual responses _____ 1. Percentage of these responses collected electronically _____ % c. Total annual hours requested _____ d. Current OMB inventory _____ e. Difference _____ f. Explanation of difference 1. Program change _____ 2. Adjustment _____	14. Annual reporting and recordkeeping cost burden ( <i>in thousands of dollars</i> ) a. Total annualized capital/startup costs _____ b. Total annual costs (O&M) _____ c. Total annualized cost requested _____ d. Current OMB inventory _____ e. Difference _____ f. Explanation of difference 1. Program change _____ 2. Adjustment _____
15. Purpose of information collection ( <i>Mark primary with "P" and all others that apply with "X"</i> ) a. ___ Application for benefits e. ___ Program planning or management b. ___ Program evaluation f. ___ Research c. ___ General purpose statistics g. ___ Regulatory or compliance d. ___ Audit	16. Frequency of recordkeeping or reporting ( <i>check all that apply</i> ) a. <input type="checkbox"/> Recordkeeping b. <input type="checkbox"/> Third party disclosure c. <input type="checkbox"/> Reporting 1. <input type="checkbox"/> On occasion 2. <input type="checkbox"/> Weekly 3. <input type="checkbox"/> Monthly 4. <input type="checkbox"/> Quarterly 5. <input type="checkbox"/> Semi-annually 6. <input type="checkbox"/> Annually 7. <input type="checkbox"/> Biennially 8. <input type="checkbox"/> Other (describe) _____
17. Statistical methods Does this information collection employ statistical methods <input type="checkbox"/> Yes <input type="checkbox"/> No	18. Agency Contact (person who can best answer questions regarding the content of this submission)  Name: _____ Phone: _____

## 19. Certification for Paperwork Reduction Act Submissions

On behalf of this Federal Agency, I certify that the collection of information encompassed by this request complies with 5 CFR 1320.9

**NOTE:** The text of 5 CFR 1320.9, and the related provisions of 5 CFR 1320.8(b)(3), appear at the end of the instructions. *The certification is to be made with reference to those regulatory provisions as set forth in the instructions.*

The following is a summary of the topics, regarding the proposed collection of information, that the certification covers:

- (a) It is necessary for the proper performance of agency functions;
- (b) It avoids unnecessary duplication;
- (c) It reduces burden on small entities;
- (d) It used plain, coherent, and unambiguous terminology that is understandable to respondents;
- (e) Its implementation will be consistent and compatible with current reporting and recordkeeping practices;
- (f) It indicates the retention period for recordkeeping requirements;
- (g) It informs respondents of the information called for under 5 CFR 1320.8(b)(3):
  - (i) Why the information is being collected;
  - (ii) Use of information;
  - (iii) Burden estimate;
  - (iv) Nature of response (voluntary, required for a benefit, mandatory);
  - (v) Nature and extent of confidentiality; and
  - (vi) Need to display currently valid OMB control number;
- (h) It was developed by an office that has planned and allocated resources for the efficient and effective management and use of the information to be collected (see note in Item 19 of instructions);
- (i) It uses effective and efficient statistical survey methodology; and
- (j) It makes appropriate use of information technology.

If you are unable to certify compliance with any of the provisions, identify the item below and explain the reason in Item 18 of the Supporting Statement.

Signature of Senior Official or designee

Date

Agency Certification (signature of Assistant Administrator, Deputy Assistant Administrator, Line Office Chief Information Officer, head of MB staff for L.O.s, or of the Director of a Program or StaffOffice)

Signature

Date

Signature of NOAA Clearance Officer

Signature

Date

**SUPPORTING STATEMENT**  
**VESSEL MONITORING SYSTEM REQUIREMENTS IN THE WESTERN PACIFIC**  
**PELAGIC LONGLINE FISHERY, AMERICAN SAMOA LONGLINE AND CNMI**  
**BOTTOMFISH FISHERIES**  
**OMB CONTROL NO. 0648-0441**

**INTRODUCTION**

This request is for renewal of this information collection, and a merging of OMB Control No. 0648-0519 and the portion of OMB Control No 0648-0584 pertaining to vessel monitoring systems (VMS) into it. Once this request is approved, OMB Control No. 0648-0519 will be discontinued, and we will submit a request to adjust the burden for 0648-0584 to reflect this partial merger.

**A. JUSTIFICATION**

**1. Explain the circumstances that make the collection of information necessary.**

The [Magnuson-Stevens Fishery Conservation and Management Act](#) (Magnuson-Stevens Act) established regional fishery management councils, such as the Western Pacific Fishery Management Council (Council), to develop fishery ecosystem plans (FEP) for fisheries in the United States (U.S.) Exclusive Economic Zone (EEZ). These plans, if approved by the Secretary of Commerce (Secretary), are implemented by National Oceanic and Atmospheric Administration (NOAA) National Marine Fisheries Service (NMFS) via Federal regulations that are enforced by the NOAA Office for Law Enforcement (NOAA OLE) and U.S. Coast Guard (USCG), in cooperation with State agencies to the extent possible. The FEPs ensure the long-term productivity and optimum yield of the resources for the benefit of the U.S.

The Council has management jurisdiction over fisheries in the Pacific Ocean in the EEZ around American Samoa, Guam, Hawaii, Northern Mariana Islands, and certain other remote U.S. Pacific island possessions<sup>1</sup>. The Council prepared, and the Secretary approved and implemented through regulations, FEPs for pelagic fisheries and archipelagic (island-based) fisheries in the western Pacific. The regulations include, but are not limited to, permit requirements, gear restrictions, temporal and spatial closures, harvest guidelines, reporting requirements, and protected species mitigation measures.

Regulations at [50 CFR Part 665](#), implementing the Fishery Ecosystem Plan for Pelagic Fisheries of the Western Pacific Region (Pelagics FEP) and the Fishery Ecosystem Plan for the Marianas Archipelago (Marianas FEP) require all vessels registered for use with Hawaii longline limited access permits, all large vessels (greater than 50 ft in overall length) registered for use with American Samoa longline limited access permits, and all medium and large vessels (40 ft or greater in overall length) registered to Northern Mariana Islands bottomfish permits to maintain and operate vessel monitoring systems (VMS) on their vessels, after they have been advised by NOAA OLE of a requirement to carry such units. NOAA OLE provides the units and installs

---

<sup>1</sup> Howland, Baker, Jarvis, Wake and Palmyra Islands, Johnston Atoll and Kingman Reef.

them for the permit holders. NOAA OLE arranges installation at times when the vessel is in port between trips to ensure minimal disruption of other activities by the vessel.

**2. Explain how, by whom, how frequently, and for what purpose the information will be used.**

On a broad level, the VMS vessel location reports are used to facilitate enforcement regarding prohibited or restricted fishing areas around American Samoa, Guam, Hawaii, Northern Mariana Islands, and Pacific Remote Island Areas, including Marine National Monuments closed to commercial fishing. The reports provide NOAA OLE and USCG real-time vessel location and activity information. The VMS reports also can be used to check the accuracy of vessel position information reported by the vessel operator in the daily fishing logbooks required by the regulations. This information is important in determining or verifying locations of catch by species and time as well as locations in which there were interactions with protected species, such as endangered and threatened sea turtles. The information provides a basis for determining whether changes in management are needed to protect sensitive species or to address fishery interaction problems and for evaluating the impacts of potential changes.

The information collected will be used internally by authorized users (NOAA OLE, USCG, NMFS and others per [NMFS Policy Directive PD 06-101, June 17, 2006, VMS Data Access and Dissemination Policy](#), and [NOAA Administrative Order NAO 0216-0100, Protection of Confidential Fisheries Statistics](#)). The information would not be disseminated to the public except in non-confidential or aggregate form in summary and analytical reports. See response to Question 10 of this Supporting Statement for more information on confidentiality and privacy. Prior to dissemination, the information will be subjected to quality control measures and a pre-dissemination review pursuant to [Section 515 of Public Law 106-554](#).

**3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological techniques or other forms of information technology.**

The VMS is an automated, satellite-based system that assists NOAA OLE and the USCG in monitoring compliance with closed areas in a reliable and cost-effective manner. Electronic VMS shipboard equipment installed permanently on board a vessel provides information about the vessel's position and activity. That information is communicated between the shipboard VMS unit and the monitoring agency's fishery monitoring center, where the identity and location of the vessels are shown on a map display, comparing vessel positions with features of interest, such as closed area boundaries.

**4. Describe efforts to identify duplication.**

There are no similar comparable programs to collect real-time vessel location information. Requiring vessel operators to make at-sea reports of vessel locations is much more costly and difficult, and would impose a direct reporting burden on the vessel operator. The VMS unit is passive and automatic, requiring no reporting burden on the vessel operator.

**5. If the collection of information involves small businesses or other small entities, describe the methods used to minimize burden.**

Vessels in the western Pacific fisheries generally range in size from 20 feet to 100 feet. Those who participate in the fisheries are categorized as “small businesses” which are affected in a similar manner by the VMS requirement. In all cases, NOAA OLE notifies the vessel owner when the requirement would take effect and arranges appointments for installation and maintenance inspections with the vessel owner and operator, to minimize time burden and business disruption by these activities. There is no reporting burden on vessel owners to arrange for VMS installation.

**6. Describe the consequences to the Federal program or policy activities if the collection is not conducted or is conducted less frequently.**

Without VMS, NOAA OLE and USCG would be tasked with monitoring closed areas via air and surface patrols. The annual cost of relying on traditional surveillance methods using air and surface patrols for time and area coverage is estimated at more than \$25 million. Comparatively, VMS provides 95 to 98 percent coverage at an estimated annual cost of \$300,000.

**7. Explain any special circumstances that require the collection to be conducted in a manner inconsistent with OMB guidelines.**

The collection is consistent with OMB guidelines except that the VMS reports more frequently than quarterly (multiple times per day). That interval is necessary for enforcing regulations.

**8. Provide information on the PRA Federal Register Notice that solicited public comments on the information collection prior to this submission. Summarize the public comments received in response to that notice and describe the actions taken by the agency in response to those comments. Describe the efforts to consult with persons outside the agency to obtain their views on the availability of data, frequency of collection, the clarity of instructions and recordkeeping, disclosure, or reporting format (if any), and on the data elements to be recorded, disclosed, or reported.**

A Federal Register Notice describing this revision was published on July 26, 2010 (75 FR 43487). One positive comment was received, supporting the cost-effectiveness of VMS for ensuring compliance with area-based management and its use by NOAA.

**9. Explain any decisions to provide payments or gifts to respondents, other than remuneration of contractors or grantees.**

No payments or gifts are provided.

**10. Describe any assurance or confidentiality provided to respondents and the basis for assurance in statute, regulation, or agency policy.**

Efforts were made in the design of the VMS program to ensure the security of all individual vessel location data, including analysis and storage. The system includes measures to minimize the risk of direct or inadvertent disclosure of fishing location information. Vessel operators consider these data proprietary, and NOAA OLE and USCG have taken steps to secure this information as “official use only” throughout the program design. Information submitted is confidential under the Magnuson-Stevens Act and NOAA regulations, except under certain circumstances as outlined in the Magnuson-Stevens Act.

*Additional protections:* Records are stored in computerized databases or CDs in locked rooms; paper records are stored in file folders in locked metal cabinets and/or locked rooms. Records are stored in buildings with doors that are locked during and after business hours. Visitors must register with security guards and must be accompanied by Federal personnel at all times. Records are organized and retrieved by NOAA internal identification number, name of entity, permit number, vessel name, or vessel identification number. Electronic records are protected by a user identification/password. The user identification/password is issued to individuals as authorized by authorized personnel.

All electronic information disseminated by NOAA adheres to the standards set out in [Appendix III, Security of Automated Information Resources, OMB Circular A-130](#); the [Computer Security Act](#); and the [Government Information Security Reform Act](#), and follows [NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems](#); [NIST SP 800-53, Recommended Security Controls for Federal Information Systems](#) and [NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans](#).

**11. Provide additional justification for any questions of a sensitive nature, such as sexual behavior and attitudes, religious beliefs, and other matters that are commonly considered private.**

No questions are asked of a sensitive nature.

**12. Provide an estimate in hours of the burden of the collection of information.**

Under the Hawaii longline limited entry program, 128 (164 maximum) vessels are currently registered, 39 large vessels are registered in the American Samoa longline limited entry program, and 5 medium-large vessels are registered to Northern Mariana Islands bottomfish permits. If all 164 Hawaii permits were registered, the total number of vessels requiring VMS would be 208.

The estimated time per response is 4 hours to install a VMS unit, 2 hours to replace a VMS unit, and 1.5 hours to maintain or repair a VMS unit.

The vessel owner or representative generally observes the initial installation, which involves a total of about 40 hours annually (estimated 10 replacement vessels x 4 hours per vessel). The vessel owner or representative may also observe any replacement, estimated at 70 hours per year annually (35 vessels x 2 hours per vessel) or maintenance and repair at 60 hours annually (40 vessels x 1.5 hours per vessel). Thus, the annual burden is 170 hours.

Annual Estimates:

10 vessels x 4 hours per vessel to install unit = 40 hours

35 vessels x 2 hours per year replacement = 70 hours

40 vessels x 1.5 hours per year maintenance and repair = 60 hours

Total estimated burden hours = 170 hrs

Total estimated responses = 85.

NOAA OLE Pacific Islands Division was consulted to develop these estimates.

Note: The number of VMS units maintained, repaired or replaced annually reflects current records. Annual maintenance/repair is not performed routinely, but only as clearly needed, due to budget constraints.

**13. Provide an estimate of the total annual cost burden to the respondents or record-keepers resulting from the collection.**

No direct or indirect costs are imposed on vessel operators by the VMS requirement. The initial installation and maintenance costs for VMS are sustained by NOAA OLE. The actual position report airtime costs are paid by NOAA OLE.

**14. Provide estimates of annualized cost to the Federal government.**

The estimated cost of the total program is \$300,000 per year, primarily for messaging costs.

**15. Explain the reasons for any program changes or adjustments.**

Current OMB inventory of 399 hours included automated transmissions from the Western Pacific pelagic longline VMS units. These transmissions from the VMS units are no longer counted in the total annual responses or burden hours because they require no action on the part of vessel owners or operators.

Adjustments were also made to the number of respondents for American Samoa longline and CNMI bottomfish fisheries. The revised responses and burden hours provided are estimates of the number of respondents needing initial installation, replacement, or maintenance and repair of VMS units.

**16. For collections whose results will be published, outline the plans for tabulation and publication.**

No formal scientific publications based on these collections are planned at this time. NMFS and the Council will use the data for management reports and fishery management plan amendments and evaluations. However, subsequent use of the data collected over a series of years may include scientific papers and publications.

**17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain the reasons why display would be inappropriate.**

Not Applicable.

**18. Explain each exception to the certification statement.**

Not Applicable.

**B. Collections of information employing statistical methods**

No statistical methods are employed.

**SEC. 303. CONTENTS OF FISHERY MANAGEMENT PLANS 16 U.S.C. 1853**

**95-354, 99-659, 101-627, 104-297**

(a) **REQUIRED PROVISIONS.**—Any fishery management plan which is prepared by any Council, or by the Secretary, with respect to any fishery, shall—

(1) contain the conservation and management measures, applicable to foreign fishing and fishing by vessels of the United States, which are—

(A) necessary and appropriate for the conservation and management of the fishery to prevent overfishing and rebuild overfished stocks, and to protect, restore, and promote the long-term health and stability of the fishery;

(B) described in this subsection or subsection (b), or both; and

(C) consistent with the national standards, the other provisions of this Act, regulations implementing recommendations by international organizations in which the United States participates (including but not limited to closed areas, quotas, and size limits), and any other applicable law;

(2) contain a description of the fishery, including, but not limited to, the number of vessels involved, the type and quantity of fishing gear used, the species of fish involved and their location, the cost likely to be incurred in management, actual and potential revenues from the fishery, any recreational interest in the fishery, and the nature and extent of foreign fishing and Indian treaty fishing rights, if any;

(3) assess and specify the present and probable future condition of, and the maximum sustainable yield and optimum yield from, the fishery, and include a summary of the information utilized in making such specification;

(4) assess and specify—

(A) the capacity and the extent to which fishing vessels of the United States, on an annual basis, will harvest the optimum yield specified under paragraph (3),

(B) the portion of such optimum yield which, on an annual basis, will not be harvested by fishing vessels of the United States and can be made available for foreign fishing, and

(C) the capacity and extent to which United States fish processors, on an annual basis, will process that portion of such optimum yield that will be harvested by fishing vessels of the United States;

**109-479**

(5) specify the pertinent data which shall be submitted to the Secretary with respect to commercial, recreational, charter fishing, and fish processing in the fishery, including, but not limited to, information regarding the type and quantity of fishing gear used, catch by species in numbers of fish or weight thereof, areas in which fishing was engaged in, time of fishing, number of hauls, economic information necessary to meet the requirements of this Act, and the estimated processing capacity of, and the actual processing capacity utilized by, United States fish processors;

(6) consider and provide for temporary adjustments, after consultation with the Coast Guard and persons utilizing the fishery, regarding access to the fishery for vessels otherwise prevented from harvesting because of weather or other ocean conditions affecting the safe conduct of the fishery; except that the adjustment shall not adversely affect conservation efforts in other fisheries or discriminate among participants in the affected fishery;

(7) describe and identify essential fish habitat for the fishery based on the guidelines established by the Secretary under section 305(b)(1)(A), minimize to the extent practicable adverse effects on such habitat caused by fishing, and identify other actions to encourage the conservation and enhancement of such habitat;

(8) in the case of a fishery management plan that, after January 1, 1991, is submitted to the Secretary for review under section 304(a) (including any plan for which an amendment is submitted to the Secretary for such review) or is prepared by the Secretary, assess and specify the nature and extent of scientific data which is needed for effective implementation of the plan;

**109-479**

(9) include a fishery impact statement for the plan or amendment (in the case of a plan or amendment thereto submitted to or prepared by the Secretary after October 1, 1990) which shall assess, specify, and analyze the likely effects, if any, including the cumulative conservation, economic, and social impacts, of the conservation and management measures on, and possible mitigation measures for—

(A) participants in the fisheries and fishing communities affected by the plan or amendment;

(B) participants in the fisheries conducted in adjacent areas under the authority of another Council, after consultation with such Council and representatives of those participants; and

(C) the safety of human life at sea, including whether and to what extent such measures may affect the safety of participants in the fishery;

(10) specify objective and measurable criteria for identifying when the fishery to which the plan applies is overfished (with an analysis of how the criteria were determined and the relationship of the criteria to the reproductive potential of stocks of fish in that fishery) and, in the case of a fishery which the Council or the Secretary has determined is approaching an overfished condition or is overfished, contain conservation and management measures to prevent overfishing or end overfishing and rebuild the fishery;

(11) establish a standardized reporting methodology to assess the amount and type of bycatch occurring in the fishery, and include conservation and management measures that, to the extent practicable and in the following priority—

(A) minimize bycatch; and

(B) minimize the mortality of bycatch which cannot be avoided;

**16 U.S.C. 1853**  
**MSA § 303**

(12) assess the type and amount of fish caught and released alive during recreational fishing under catch and release fishery management programs and the mortality of such fish, and include conservation and management measures that, to the extent practicable, minimize mortality and ensure the extended survival of such fish;

**109-479**

(13) include a description of the commercial, recreational, and charter fishing sectors which participate in the fishery, including its economic impact, and, to the extent practicable, quantify trends in landings of the managed fishery resource by the commercial, recreational, and charter fishing sectors;

**109-479**

(14) to the extent that rebuilding plans or other conservation and management measures which reduce the overall harvest in a fishery are necessary, allocate, taking into consideration the economic impact of the harvest restrictions or recovery benefits on the fishery participants in each sector, any harvest restrictions or recovery benefits fairly and equitably among the commercial, recreational, and charter fishing sectors in the fishery and;

**109-479**

(15) establish a mechanism for specifying annual catch limits in the plan (including a multiyear plan), implementing regulations, or annual specifications, at a level such that overfishing does not occur in the fishery, including measures to ensure accountability.

**97-453, 99-659, 101-627, 102-251, 104-297**

(b) DISCRETIONARY PROVISIONS.—Any fishery management plan which is prepared by any Council, or by the Secretary, with respect to any fishery, may—

(1) require a permit to be obtained from, and fees to be paid to, the Secretary, with respect to—

(A) any fishing vessel of the United States fishing, or wishing to fish, in the exclusive economic zone [or special areas,]\* or for anadromous species or Continental Shelf fishery resources beyond such zone [or areas]\*;

(B) the operator of any such vessel; or

(C) any United States fish processor who first receives fish that are subject to the plan;

**109-479**

(2)(A) designate zones where, and periods when, fishing shall be limited, or shall not be permitted, or shall be permitted only by specified types of fishing vessels or with specified types and quantities of fishing gear;

(B) designate such zones in areas where deep sea corals are identified under section 408, to protect deep sea corals from physical damage from fishing gear or to prevent loss or damage to such fishing gear from interactions with deep sea corals, after considering long-term sustainable uses of fishery resources in such areas; and

(C) with respect to any closure of an area under this Act that prohibits all fishing, ensure that such closure—

- (i) is based on the best scientific information available;
- (ii) includes criteria to assess the conservation benefit of the closed area;
- (iii) establishes a timetable for review of the closed area's performance that is consistent with the purposes of the closed area; and
- (iv) is based on an assessment of the benefits and impacts of the closure, including its size, in relation to other management measures (either alone or in combination with such measures), including the benefits and impacts of limiting access to: users of the area, overall fishing activity, fishery science, and fishery and marine conservation;

(3) establish specified limitations which are necessary and appropriate for the conservation and management of the fishery on the—

- (A) catch of fish (based on area, species, size, number, weight, sex, bycatch, total biomass, or other factors);
- (B) sale of fish caught during commercial, recreational, or charter fishing, consistent with any applicable Federal and State safety and quality requirements; and
- (C) transshipment or transportation of fish or fish products under permits issued pursuant to section 204;

(4) prohibit, limit, condition, or require the use of specified types and quantities of fishing gear, fishing vessels, or equipment for such vessels, including devices which may be required to facilitate enforcement of the provisions of this Act;

**109-479**

(5) incorporate (consistent with the national standards, the other provisions of this Act, and any other applicable law) the relevant fishery conservation and management measures of the coastal States nearest to the fishery and take into account the different circumstances affecting fisheries from different States and ports, including distances to fishing grounds and proximity to time and area closures;

**109-479**

(6) establish a limited access system for the fishery in order to achieve optimum yield if, in developing such system, the Council and the Secretary take into account—

- (A) present participation in the fishery;
- (B) historical fishing practices in, and dependence on, the fishery;
- (C) the economics of the fishery;
- (D) the capability of fishing vessels used in the fishery to engage in other fisheries;
- (E) the cultural and social framework relevant to the fishery and any affected fishing communities;
- (F) the fair and equitable distribution of access privileges in the fishery; and
- (G) any other relevant considerations;

**16 U.S.C. 1853**  
**MSA § 303**

(7) require fish processors who first receive fish that are subject to the plan to submit data which are necessary for the conservation and management of the fishery;

(8) require that one or more observers be carried on board a vessel of the United States engaged in fishing for species that are subject to the plan, for the purpose of collecting data necessary for the conservation and management of the fishery; except that such a vessel shall not be required to carry an observer on board if the facilities of the vessel for the quartering of an observer, or for carrying out observer functions, are so inadequate or unsafe that the health or safety of the observer or the safe operation of the vessel would be jeopardized;

(9) assess and specify the effect which the conservation and management measures of the plan will have on the stocks of naturally spawning anadromous fish in the region;

(10) include, consistent with the other provisions of this Act, conservation and management measures that provide harvest incentives for participants within each gear group to employ fishing practices that result in lower levels of bycatch or in lower levels of the mortality of bycatch;

(11) reserve a portion of the allowable biological catch of the fishery for use in scientific research;

**109-479**

(12) include management measures in the plan to conserve target and non-target species and habitats, considering the variety of ecological factors affecting fishery populations; and

(14)[sic]<sup>15</sup> prescribe such other measures, requirements, or conditions and restrictions as are determined to be necessary and appropriate for the conservation and management of the fishery.

**97-453, 104-297**

(c) PROPOSED REGULATIONS.—Proposed regulations which the Council deems necessary or appropriate for the purposes of—

(1) implementing a fishery management plan or plan amendment shall be submitted to the Secretary simultaneously with the plan or amendment under section 304; and

(2) making modifications to regulations implementing a fishery management plan or plan amendment may be submitted to the Secretary at any time after the plan or amendment is approved under section 304.

---

<sup>15</sup> So in original.

**P.L. 109-479, sec. 104(b), MSA § 303 note**

**16 U.S.C. 1853 note**

**EFFECTIVE DATES; APPLICATION TO CERTAIN SPECIES.**—The amendment made by subsection (a)(10)<sup>16</sup>—

(1) shall, unless otherwise provided for under an international agreement in which the United States participates, take effect—

(A) in fishing year 2010 for fisheries determined by the Secretary to be subject to overfishing; and

(B) in fishing year 2011 for all other fisheries; and

(2) shall not apply to a fishery for species that have a life cycle of approximately 1 year unless the Secretary has determined the fishery is subject to overfishing of that species; and

(3) shall not limit or otherwise affect the requirements of section 301(a)(1) or 304(e) of the Magnuson-Stevens Fishery Conservation and Management Act (16 U.S.C. 1851(a)(1) or 1854(e), respectively).

**109-479**

**SEC. 303A. LIMITED ACCESS PRIVILEGE PROGRAMS.**

**16 U.S.C. 1853a**

(a) **IN GENERAL.**—After the date of enactment of the Magnuson-Stevens Fishery Conservation and Management Reauthorization Act of 2006, a Council may submit, and the Secretary may approve, for a fishery that is managed under a limited access system, a limited access privilege program to harvest fish if the program meets the requirements of this section.

(b) **NO CREATION OF RIGHT, TITLE, OR INTEREST.**—Limited access privilege, quota share, or other limited access system authorization established, implemented, or managed under this Act—

(1) shall be considered a permit for the purposes of sections 307, 308, and 309;

(2) may be revoked, limited, or modified at any time in accordance with this Act, including revocation if the system is found to have jeopardized the sustainability of the stock or the safety of fishermen;

(3) shall not confer any right of compensation to the holder of such limited access privilege, quota share, or other such limited access system authorization if it is revoked, limited, or modified;

(4) shall not create, or be construed to create, any right, title, or interest in or to any fish before the fish is harvested by the holder; and

(5) shall be considered a grant of permission to the holder of the limited access privilege or quota share to engage in activities permitted by such limited access privilege or quota share.

---

<sup>16</sup> Section 104(a)(10) of P.L. 109-479 added section 303(a)(15).

(c) REQUIREMENTS FOR LIMITED ACCESS PRIVILEGES.—

(1) IN GENERAL.—Any limited access privilege program to harvest fish submitted by a Council or approved by the Secretary under this section shall—

(A) if established in a fishery that is overfished or subject to a rebuilding plan, assist in its rebuilding;

(B) if established in a fishery that is determined by the Secretary or the Council to have over-capacity, contribute to reducing capacity;

(C) promote—

(i) fishing safety;

(ii) fishery conservation and management; and

(iii) social and economic benefits;

(D) prohibit any person other than a United States citizen, a corporation, partnership, or other entity established under the laws of the United States or any State, or a permanent resident alien, that meets the eligibility and participation requirements established in the program from acquiring a privilege to harvest fish, including any person that acquires a limited access privilege solely for the purpose of perfecting or realizing on a security interest in such privilege;

(E) require that all fish harvested under a limited access privilege program be processed on vessels of the United States or on United States soil (including any territory of the United States);

(F) specify the goals of the program;

(G) include provisions for the regular monitoring and review by the Council and the Secretary of the operations of the program, including determining progress in meeting the goals of the program and this Act, and any necessary modification of the program to meet those goals, with a formal and detailed review 5 years after the implementation of the program and thereafter to coincide with scheduled Council review of the relevant fishery management plan (but no less frequently than once every 7 years);

(H) include an effective system for enforcement, monitoring, and management of the program, including the use of observers or electronic monitoring systems;

(I) include an appeals process for administrative review of the Secretary's decisions regarding initial allocation of limited access privileges;

(J) provide for the establishment by the Secretary, in consultation with appropriate Federal agencies, for an information collection and review process to provide any additional information needed to determine whether any illegal acts of anti-competition, anti-trust, price collusion, or price fixing have occurred among regional fishery associations or persons receiving limited access privileges under the program; and

(K) provide for the revocation by the Secretary of limited access privileges held by any person found to have violated the antitrust laws of the United States.

(2) WAIVER.—The Secretary may waive the requirement of paragraph (1)(E) if the Secretary determines that—

- (A) the fishery has historically processed the fish outside of the United States; and
- (B) the United States has a seafood safety equivalency agreement with the country where processing will occur.

(3) FISHING COMMUNITIES.—

(A) IN GENERAL.—

(i) ELIGIBILITY.—To be eligible to participate in a limited access privilege program to harvest fish, a fishing community shall—

- (I) be located within the management area of the relevant Council;
- (II) meet criteria developed by the relevant Council, approved by the Secretary, and published in the Federal Register;
- (III) consist of residents who conduct commercial or recreational fishing, processing, or fishery-dependent support businesses within the Council's management area; and
- (IV) develop and submit a community sustainability plan to the Council and the Secretary that demonstrates how the plan will address the social and economic development needs of coastal communities, including those that have not historically had the resources to participate in the fishery, for approval based on criteria developed by the Council that have been approved by the Secretary and published in the Federal Register.

(ii) FAILURE TO COMPLY WITH PLAN.—The Secretary shall deny or revoke limited access privileges granted under this section for any person who fails to comply with the requirements of the community sustainability plan. Any limited access privileges denied or revoked under this section may be reallocated to other eligible members of the fishing community.

- (B) PARTICIPATION CRITERIA.—In developing participation criteria for eligible communities under this paragraph, a Council shall consider—
- (i) traditional fishing or processing practices in, and dependence on, the fishery;
  - (ii) the cultural and social framework relevant to the fishery;
  - (iii) economic barriers to access to fishery;
  - (iv) the existence and severity of projected economic and social impacts associated with implementation of limited access privilege programs on harvesters, captains, crew, processors, and other businesses substantially dependent upon the fishery in the region or subregion;
  - (v) the expected effectiveness, operational transparency, and equitability of the community sustainability plan; and
  - (vi) the potential for improving economic conditions in remote coastal communities lacking resources to participate in harvesting or processing activities in the fishery.

(4) REGIONAL FISHERY ASSOCIATIONS.—

(A) IN GENERAL.—To be eligible to participate in a limited access privilege program to harvest fish, a regional fishery association shall—

- (i) be located within the management area of the relevant Council;
- (ii) meet criteria developed by the relevant Council, approved by the Secretary, and published in the Federal Register;
- (iii) be a voluntary association with established by-laws and operating procedures;
- (iv) consist of participants in the fishery who hold quota share that are designated for use in the specific region or subregion covered by the regional fishery association, including commercial or recreational fishing, processing, fishery-dependent support businesses, or fishing communities;
- (v) not be eligible to receive an initial allocation of a limited access privilege but may acquire such privileges after the initial allocation, and may hold the annual fishing privileges of any limited access privileges it holds or the annual fishing privileges that is [sic]<sup>17</sup> members contribute; and
- (vi) develop and submit a regional fishery association plan to the Council and the Secretary for approval based on criteria developed by the Council that have been approved by the Secretary and published in the Federal Register.

(B) FAILURE TO COMPLY WITH PLAN.—The Secretary shall deny or revoke limited access privileges granted under this section to any person participating in a regional fishery association who fails to comply with the requirements of the regional fishery association plan.

---

<sup>17</sup> So in original.

(C) PARTICIPATION CRITERIA.—In developing participation criteria for eligible regional fishery associations under this paragraph, a Council shall consider—

- (i) traditional fishing or processing practices in, and dependence on, the fishery;
- (ii) the cultural and social framework relevant to the fishery;
- (iii) economic barriers to access to fishery;
- (iv) the existence and severity of projected economic and social impacts associated with implementation of limited access privilege programs on harvesters, captains, crew, processors, and other businesses substantially dependent upon the fishery in the region or subregion;
- (v) the administrative and fiduciary soundness of the association; and
- (vi) the expected effectiveness, operational transparency, and equitability of the fishery association plan.

(5) ALLOCATION.—In developing a limited access privilege program to harvest fish a Council or the Secretary shall—

(A) establish procedures to ensure fair and equitable initial allocations, including consideration of—

- (i) current and historical harvests;
- (ii) employment in the harvesting and processing sectors;
- (iii) investments in, and dependence upon, the fishery; and
- (iv) the current and historical participation of fishing communities;

(B) consider the basic cultural and social framework of the fishery, especially through—

- (i) the development of policies to promote the sustained participation of small owner-operated fishing vessels and fishing communities that depend on the fisheries, including regional or port-specific landing or delivery requirements; and
- (ii) procedures to address concerns over excessive geographic or other consolidation in the harvesting or processing sectors of the fishery;

(C) include measures to assist, when necessary and appropriate, entry-level and small vessel owner-operators, captains, crew, and fishing communities through set-asides of harvesting allocations, including providing privileges, which may include set-asides or allocations of harvesting privileges, or economic assistance in the purchase of limited access privileges;

(D) ensure that limited access privilege holders do not acquire an excessive share of the total limited access privileges in the program by—

- (i) establishing a maximum share, expressed as a percentage of the total limited access privileges, that a limited access privilege holder is permitted to hold, acquire, or use; and
- (ii) establishing any other limitations or measures necessary to prevent an inequitable concentration of limited access privileges; and

(E) authorize limited access privileges to harvest fish to be held, acquired, used by, or issued under the system to persons who substantially participate in the fishery, including in a specific sector of such fishery, as specified by the Council.

(6) PROGRAM INITIATION.—

(A) LIMITATION.—Except as provided in subparagraph (D), a Council may initiate a fishery management plan or amendment to establish a limited access privilege program to harvest fish on its own initiative or if the Secretary has certified an appropriate petition.

(B) PETITION.—A group of fishermen constituting more than 50 percent of the permit holders, or holding more than 50 percent of the allocation, in the fishery for which a limited access privilege program to harvest fish is sought, may submit a petition to the Secretary requesting that the relevant Council or Councils with authority over the fishery be authorized to initiate the development of the program. Any such petition shall clearly state the fishery to which the limited access privilege program would apply. For multispecies permits in the Gulf of Mexico, only those participants who have substantially fished the species proposed to be included in the limited access program shall be eligible to sign a petition for such a program and shall serve as the basis for determining the percentage described in the first sentence of this subparagraph.

(C) CERTIFICATION BY SECRETARY.—Upon the receipt of any such petition, the Secretary shall review all of the signatures on the petition and, if the Secretary determines that the signatures on the petition represent more than 50 percent of the permit holders, or holders of more than 50 percent of the allocation in the fishery, as described by subparagraph (B), the Secretary shall certify the petition to the appropriate Council or Councils.

(D) NEW ENGLAND AND GULF REFERENDUM.—

(i) Except as provided in clause (iii) for the Gulf of Mexico commercial red snapper fishery, the New England and Gulf Councils may not submit, and the Secretary may not approve or implement, a fishery management plan or amendment that creates an individual fishing quota program, including a Secretarial plan, unless such a system, as ultimately developed, has been approved by more than 2/3 of those voting in a referendum among eligible permit holders, or other persons described in clause (v), with respect to the New England Council, and by a majority of those voting in the referendum among eligible permit holders with respect to the Gulf Council. For multispecies permits in the Gulf of Mexico, only those participants who have substantially fished the species proposed to be included in the individual fishing quota program shall be eligible to vote in such a referendum. If an individual fishing quota program fails to be approved by the requisite number of those voting, it may be revised and submitted for approval in a subsequent referendum.

(ii) The Secretary shall conduct a referendum under this subparagraph, including notifying all persons eligible to participate in the referendum and making available to them information concerning the schedule, procedures, and eligibility requirements for the referendum process and the proposed individual fishing quota program. Within 1 year after the date of enactment of the Magnuson-Stevens Fishery Conservation and Management Reauthorization Act of 2006, the Secretary shall publish guidelines and procedures to determine procedures and voting eligibility requirements for referenda and to conduct such referenda in a fair and equitable manner.

(iii) The provisions of section 407(c) of this Act shall apply in lieu of this subparagraph for an individual fishing quota program for the Gulf of Mexico commercial red snapper fishery.

(iv) Chapter 35 of title 44, United States Code, (commonly known as the Paperwork Reduction Act) does not apply to the referenda conducted under this subparagraph.

(v) The Secretary shall promulgate criteria for determining whether additional fishery participants are eligible to vote in the New England referendum described in clause (i) in order to ensure that crew members who derive a significant percentage of their total income from the fishery under the proposed program are eligible to vote in the referendum.

(vi) In this subparagraph, the term ‘individual fishing quota’ does not include a sector allocation.

(7) TRANSFERABILITY.—In establishing a limited access privilege program, a Council shall—

(A) establish a policy and criteria for the transferability of limited access privileges (through sale or lease), that is consistent with the policies adopted by the Council for the fishery under paragraph (5); and

(B) establish, in coordination with the Secretary, a process for monitoring of transfers (including sales and leases) of limited access privileges.

(8) PREPARATION AND IMPLEMENTATION OF SECRETARIAL PLANS.—This subsection also applies to a plan prepared and implemented by the Secretary under section 304(c) or 304(g).

(9) ANTITRUST SAVINGS CLAUSE.—Nothing in this Act shall be construed to modify, impair, or supersede the operation of any of the antitrust laws. For purposes of the preceding sentence, the term ‘antitrust laws’ has the meaning given such term in subsection (a) of the first section of the Clayton Act, except that such term includes section 5 of the Federal Trade Commission Act to the extent that such section 5 applies to unfair methods of competition.

**16 U.S.C. 1853a**  
**MSA § 303A**

(d) AUCTION AND OTHER PROGRAMS.—In establishing a limited access privilege program, a Council shall consider, and may provide, if appropriate, an auction system or other program to collect royalties for the initial, or any subsequent, distribution of allocations in a limited access privilege program if—

(1) the system or program is administered in such a way that the resulting distribution of limited access privilege shares meets the program requirements of this section; and

(2) revenues generated through such a royalty program are deposited in the Limited Access System Administration Fund established by section 305(h)(5)(B) and available subject to annual appropriations.

(e) COST RECOVERY.—In establishing a limited access privilege program, a Council shall—

(1) develop a methodology and the means to identify and assess the management, data collection and analysis, and enforcement programs that are directly related to and in support of the program; and

(2) provide, under section 304(d)(2), for a program of fees paid by limited access privilege holders that will cover the costs of management, data collection and analysis, and enforcement activities.

(f) CHARACTERISTICS.—A limited access privilege established after the date of enactment of the Magnuson-Stevens Fishery Conservation and Management Reauthorization Act of 2006 is a permit issued for a period of not more than 10 years that—

(1) will be renewed before the end of that period, unless it has been revoked, limited, or modified as provided in this subsection;

(2) will be revoked, limited, or modified if the holder is found by the Secretary, after notice and an opportunity for a hearing under section 554 of title 5, United States Code, to have failed to comply with any term of the plan identified in the plan as cause for revocation, limitation, or modification of a permit, which may include conservation requirements established under the plan;

(3) may be revoked, limited, or modified if the holder is found by the Secretary, after notice and an opportunity for a hearing under section 554 of title 5, United States Code, to have committed an act prohibited by section 307 of this Act; and

(4) may be acquired, or reacquired, by participants in the program under a mechanism established by the Council if it has been revoked, limited, or modified under paragraph (2) or (3).

(g) LIMITED ACCESS PRIVILEGE ASSISTED PURCHASE PROGRAM.—

(1) IN GENERAL.—A Council may submit, and the Secretary may approve and implement, a program which reserves up to 25 percent of any fees collected from a fishery under section 304(d)(2) to be used, pursuant to section 53706(a)(7) of title 46, United States Code, to issue obligations that aid in financing—

(A) the purchase of limited access privileges in that fishery by fishermen who fish from small vessels; and

(B) the first-time purchase of limited access privileges in that fishery by entry level fishermen.

(2) ELIGIBILITY CRITERIA.—A Council making a submission under paragraph (1) shall recommend criteria, consistent with the provisions of this Act, that a fisherman must meet to qualify for guarantees under subparagraphs (A) and (B) of paragraph (1) and the portion of funds to be allocated for guarantees under each subparagraph.

(h) EFFECT ON CERTAIN EXISTING SHARES AND PROGRAMS.—Nothing in this Act, or the amendments made by the Magnuson-Stevens Fishery Conservation and Management Reauthorization Act of 2006, shall be construed to require a reallocation or a reevaluation of individual quota shares, processor quota shares, cooperative programs, or other quota programs, including sector allocation in effect before the date of enactment of the Magnuson-Stevens Fishery Conservation and Management Reauthorization Act of 2006.

(i) TRANSITION RULES.—

(1) IN GENERAL.—The requirements of this section shall not apply to any quota program, including any individual quota program, cooperative program, or sector allocation for which a Council has taken final action or which has been submitted by a Council to the Secretary, or approved by the Secretary, within 6 months after the date of enactment of the Magnuson-Stevens Fishery Conservation and Management Reauthorization Act of 2006, except that—

(A) the requirements of section 303(d) of this Act in effect on the day before the date of enactment of that Act shall apply to any such program;

(B) the program shall be subject to review under subsection (c)(1)(G) of this section not later than 5 years after the program implementation; and

(C) nothing in this subsection precludes a Council from incorporating criteria contained in this section into any such plans.

(2) PACIFIC GROUND FISH PROPOSALS.—The requirements of this section, other than subparagraphs (A) and (B) of subsection (c)(1) and subparagraphs (A), (B), and (C) of paragraph (1) of this subsection, shall not apply to any proposal authorized under section 302(f) of the Magnuson-Stevens Fishery Conservation and Management Reauthorization Act of 2006 that is submitted within the timeframe prescribed by that section.

**16 U.S.C. 1853a note, 1854**  
**MSA §§ 303A note, 304**

**P.L. 109-479, sec. 106(e), MSA § 303A note**

**16 U.S.C. 1853a note**

**APPLICATION WITH AMERICAN FISHERIES ACT.**—Nothing in section 303A of the Magnuson-Stevens Fishery Conservation and Management Act (16 U.S.C. 1801 et seq.), as added by subsection (a) [P.L. 109-479], shall be construed to modify or supersede any provision of the American Fisheries Act (46 U.S.C. 12102 note; 16 U.S.C. 1851 note; et alia).

**P.L. 104-297, sec. 108(i), MSA § 303 note**

**EXISTING QUOTA PLANS.**—Nothing in this Act [P.L.104-297] or the amendments made by this Act shall be construed to require a reallocation of individual fishing quotas under any individual fishing quota program approved by the Secretary before January 4, 1995.

## **SEC. 304. ACTION BY THE SECRETARY**

**16 U.S.C. 1854**

### **104-297**

(a) REVIEW OF PLANS.—

(1) Upon transmittal by the Council to the Secretary of a fishery management plan or plan amendment, the Secretary shall—

(A) immediately commence a review of the plan or amendment to determine whether it is consistent with the national standards, the other provisions of this Act, and any other applicable law; and

(B) immediately publish in the Federal Register a notice stating that the plan or amendment is available and that written information, views, or comments of interested persons on the plan or amendment may be submitted to the Secretary during the 60-day period beginning on the date the notice is published.

(2) In undertaking the review required under paragraph (1), the Secretary shall—

(A) take into account the information, views, and comments received from interested persons;

(B) consult with the Secretary of State with respect to foreign fishing; and

(C) consult with the Secretary of the department in which the Coast Guard is operating with respect to enforcement at sea and to fishery access adjustments referred to in section 303(a)(6).

(3) The Secretary shall approve, disapprove, or partially approve a plan or amendment within 30 days of the end of the comment period under paragraph (1) by written notice to the Council. A notice of disapproval or partial approval shall specify—

(A) the applicable law with which the plan or amendment is inconsistent;

(B) the nature of such inconsistencies; and

(C) recommendations concerning the actions that could be taken by the Council to conform such plan or amendment to the requirements of applicable law.

If the Secretary does not notify a Council within 30 days of the end of the comment period of the approval, disapproval, or partial approval of a plan or amendment, then such plan or amendment shall take effect as if approved.

104-297

**SEC. 402. INFORMATION COLLECTION**

16 U.S.C. 1881a

109-479

(a) COLLECTION PROGRAMS.—

(1) COUNCIL REQUESTS.—If a Council determines that additional information would be beneficial for developing, implementing, or revising a fishery management plan or for determining whether a fishery is in need of management, the Council may request that the Secretary implement an information collection program for the fishery which would provide the types of information specified by the Council. The Secretary shall undertake such an information collection program if he determines that the need is justified, and shall promulgate regulations to implement the program within 60 days after such determination is made. If the Secretary determines that the need for an information collection program is not justified, the Secretary shall inform the Council of the reasons for such determination in writing. The determinations of the Secretary under this paragraph regarding a Council request shall be made within a reasonable period of time after receipt of that request.

(2) SECRETARIAL INITIATION.—If the Secretary determines that additional information is necessary for developing, implementing, revising, or monitoring a fishery management plan, or for determining whether a fishery is in need of management, the Secretary may, by regulation, implement an information collection or observer program requiring submission of such additional information for the fishery.

109-479

(b) CONFIDENTIALITY OF INFORMATION.—

(1) Any information submitted to the Secretary, a State fishery management agency, or a marine fisheries commission by any person in compliance with the requirements of this Act shall be confidential and shall not be disclosed except—

(A) to Federal employees and Council employees who are responsible for fishery management plan development, monitoring, or enforcement;

(B) to State or Marine Fisheries Commission employees as necessary to further the Department's mission, subject to a confidentiality agreement that prohibits public disclosure of the identity of business of any person;

(C) to State employees who are responsible for fishery management plan enforcement, if the States employing those employees have entered into a fishery enforcement agreement with the Secretary and the agreement is in effect;

(D) when required by court order;

(E) when such information is used by State, Council, or Marine Fisheries Commission employees to verify catch under a limited access program, but only to the extent that such use is consistent with subparagraph (B);

(F) when the Secretary has obtained written authorization from the person submitting such information to release such information to persons for reasons not otherwise provided for in this subsection, and such release does not violate other requirements of this Act;

(G) when such information is required to be submitted to the Secretary for any determination under a limited access program; or

(H) in support of homeland and national security activities, including the Coast Guard's homeland security missions as defined in section 888(a)(2) of the Homeland Security Act of 2002 (6 U.S.C. 468(a)(2)).

(2) Any observer information shall be confidential and shall not be disclosed, except in accordance with the requirements of subparagraphs (A) through (H) of paragraph (1), or—

(A) as authorized by a fishery management plan or regulations under the authority of the North Pacific Council to allow disclosure to the public of weekly summary bycatch information identified by vessel or for haul-specific bycatch information without vessel identification;

(B) when such information is necessary in proceedings to adjudicate observer certifications; or

(C) as authorized by any regulations issued under paragraph (3) allowing the collection of observer information, pursuant to a confidentiality agreement between the observers, observer employers, and the Secretary prohibiting disclosure of the information by the observers or observer employers, in order—

(i) to allow the sharing of observer information among observers and between observers and observer employers as necessary to train and prepare observers for deployments on specific vessels; or

(ii) to validate the accuracy of the observer information collected.

(3) The Secretary shall, by regulation, prescribe such procedures as may be necessary to preserve the confidentiality of information submitted in compliance with any requirement or regulation under this Act, except that the Secretary may release or make public any such information in any aggregate or summary form which does not directly or indirectly disclose the identity or business of any person who submits such information. Nothing in this subsection shall be interpreted or construed to prevent the use for conservation and management purposes by the Secretary, or with the approval of the Secretary, the Council, of any information submitted in compliance with any requirement or regulation under this Act or the use, release, or publication of bycatch information pursuant to paragraph (2)(A).

**(c) RESTRICTION ON USE OF CERTAIN INFORMATION.—**

(1) The Secretary shall promulgate regulations to restrict the use, in civil enforcement or criminal proceedings under this Act, the Marine Mammal Protection Act of 1972 (16 U.S.C. 1361 et seq.), and the Endangered Species Act (16 U.S.C. 1531 et seq.), of information collected by voluntary fishery data collectors, including sea samplers, while aboard any vessel for conservation and management purposes if the presence of such a fishery data collector aboard is not required by any of such Acts or regulations thereunder.

(2) The Secretary may not require the submission of a Federal or State income tax return or statement as a prerequisite for issuance of a permit until such time as the Secretary has promulgated regulations to ensure the confidentiality of information contained in such return or statement, to limit the information submitted to that necessary to achieve a demonstrated conservation and management purpose, and to provide appropriate penalties for violation of such regulations.

**16 U.S.C. 1881a-1881b**  
**MSA §§ 402-403**

(d) **CONTRACTING AUTHORITY.**—Notwithstanding any other provision of law, the Secretary may provide a grant, contract, or other financial assistance on a sole-source basis to a State, Council, or Marine Fisheries Commission for the purpose of carrying out information collection or other programs if—

(1) the recipient of such a grant, contract, or other financial assistance is specified by statute to be, or has customarily been, such State, Council, or Marine Fisheries Commission; or

(2) the Secretary has entered into a cooperative agreement with such State, Council, or Marine Fisheries Commission.

(e) **RESOURCE ASSESSMENTS.**—

(1) The Secretary may use the private sector to provide vessels, equipment, and services necessary to survey the fishery resources of the United States when the arrangement will yield statistically reliable results.

(2) The Secretary, in consultation with the appropriate Council and the fishing industry--

(A) may structure competitive solicitations under paragraph (1) so as to compensate a contractor for a fishery resources survey by allowing the contractor to retain for sale fish harvested during the survey voyage;

(B) in the case of a survey during which the quantity or quality of fish harvested is not expected to be adequately compensatory, may structure those solicitations so as to provide that compensation by permitting the contractor to harvest on a subsequent voyage and retain for sale a portion of the allowable catch of the surveyed fishery; and

(C) may permit fish harvested during such survey to count toward a vessel's catch history under a fishery management plan if such survey was conducted in a manner that precluded a vessel's participation in a fishery that counted under the plan for purposes of determining catch history.

(3) The Secretary shall undertake efforts to expand annual fishery resource assessments in all regions of the Nation.

**104-297**

**SEC. 403. OBSERVERS**

**16 U.S.C. 1881b**

(a) **GUIDELINES FOR CARRYING OBSERVERS.**—Within one year after the date of enactment of the Sustainable Fisheries Act, the Secretary shall promulgate regulations, after notice and opportunity for public comment, for fishing vessels that carry observers. The regulations shall include guidelines for determining—

(1) when a vessel is not required to carry an observer on board because the facilities of such vessel for the quartering of an observer, or for carrying out observer functions, are so inadequate or unsafe that the health or safety of the observer or the safe operation of the vessel would be jeopardized; and

(2) actions which vessel owners or operators may reasonably be required to take to render such facilities adequate and safe.

**e-CFR Data is current as of November 25, 2010**

**Title 50: Wildlife and Fisheries**

[PART 665—FISHERIES IN THE WESTERN PACIFIC](#)

[Subpart A—General](#)

**§ 665.19 Vessel monitoring system.**

(a) *Applicability.* The holder of any of the following permits is subject to the vessel monitoring system requirements in this part:

- (1) Hawaii longline limited access permit issued pursuant to §665.801(b);
- (2) American Samoa longline limited entry permit, for vessel size Class C or D, issued pursuant to §665.801(c);
- (3) Vessels permitted to fish in Crustacean Permit Area 1 VMS Subarea; or
- (4) CNMI commercial bottomfish permit, if the vessel is a medium or large bottomfish vessel, issued pursuant to §665.404(a)(2).

(b) *VMS unit.* Only a VMS unit owned by NMFS and installed by NMFS complies with the requirement of this subpart.

(c) *Notification.* After a permit holder subject to §665.19(a) has been notified by the SAC of a specific date for installation of a VMS unit on the permit holder's vessel, the vessel must carry and operate the VMS unit after the date scheduled for installation.

(d) *Fees and charges.* During the experimental VMS program, the holder of a permit subject to §665.19(a) shall not be assessed any fee or other charges to obtain and use a VMS unit, including the communication charges related directed to requirements under this section. Communication charges related to any additional equipment attached to the VMS unit by the owner or operator shall be the responsibility of the owner or operator and not NMFS.

(e) *Permit holder duties.* The holder of a permit subject to §665.19(a) and master of the vessel must:

- (1) Provide opportunity for the SAC to install and make operational a VMS unit after notification.
- (2) Carry and continuously operate the VMS unit on board whenever the vessel is at sea.
- (3) Not remove, relocate, or make non-operational the VMS unit without prior approval from the SAC.

(f) *Authorization by the SAC.* The SAC has authority over the installation and operation of the VMS unit. The SAC may authorize the connection or order the disconnection of additional equipment, including a computer, to any VMS unit when deemed appropriate by the SAC.

## **Appendix III to OMB Circular No. A-130 - Security of Federal Automated Information Resources**

### A. Requirements.

#### 1. Purpose

This Appendix establishes a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123. The Appendix revises procedures formerly contained in Appendix III to OMB Circular No. A-130 (50 FR 52730; December 24, 1985), and incorporates requirements of the Computer Security Act of 1987 (P.L. 100-235) and responsibilities assigned in applicable national security directives.

#### 2. Definitions

The term:

- a. "adequate security" means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.
- b. "application" means the use of information resources (information and information technology) to satisfy a specific set of user requirements.
- c. "general support system" or "system" means an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).
- d. "major application" means an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

3. Automated Information Security Programs. Agencies shall implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications.

Each agency's program shall implement policies, standards and procedures which are consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce, the General Services Administration and the Office of Personnel Management (OPM). Different or more stringent requirements for securing national security information should be incorporated into agency programs as required by appropriate national security directives. At a minimum, agency programs shall include the following controls in their general support systems and major applications:

a. Controls for general support systems.

1) Assign Responsibility for Security. Assign responsibility for security in each system to an individual knowledgeable in the information technology used in the system and in providing security for such technology.

2) System Security Plan. Plan for adequate security of each general support system as part of the organization's information resources management (IRM) planning process. The security plan shall be consistent with guidance issued by the National Institute of Standards and Technology (NIST). Independent advice and comment on the security plan shall be solicited prior to the plan's implementation. A summary of the security plans shall be incorporated into the strategic IRM plan required by the Paperwork Reduction Act (44 U.S.C. Chapter 35) and Section 8(b) of this circular. Security plans shall include:

a) Rules of the System. Establish a set of rules of behavior concerning use of, security in, and the acceptable level of risk for, the system. The rules shall be based on the needs of the various users of the system. The security required by the rules shall be only as stringent as necessary to provide adequate security for information in the system. Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the system. They shall also include appropriate limits on interconnections to other systems and shall define service provision and restoration priorities. Finally, they shall be clear about the consequences of behavior not consistent with the rules.

b) Training. Ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. Such training shall assure that employees are versed in the rules of the system, be consistent with guidance issued by NIST and OPM, and apprise them about available assistance and technical security products and techniques. Behavior consistent with the rules of the system

and periodic refresher training shall be required for continued access to the system.

c) Personnel Controls. Screen individuals who are authorized to bypass significant technical and operational security controls of the system commensurate with the risk and magnitude of harm they could cause. Such screening shall occur prior to an individual being authorized to bypass controls and periodically thereafter.

d) Incident Response Capability. Ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. This capability shall share information with other organizations, consistent with NIST coordination, and should assist the agency in pursuing appropriate legal action, consistent with Department of Justice guidance.

e) Continuity of Support. Establish and periodically test the capability to continue providing service within a system based upon the needs and priorities of the participants of the system.

f) Technical Security. Ensure that cost-effective security products and techniques are appropriately used within the system.

g) System Interconnection. Obtain written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems. Where connection is authorized, controls shall be established which are consistent with the rules of the system and in accordance with guidance from NIST.

3) Review of Security Controls. Review the security controls in each system when significant modifications are made to the system, but at least every three years. The scope and frequency of the review should be commensurate with the acceptable level of risk for the system. Depending on the potential risk and magnitude of harm that could occur, consider identifying a deficiency pursuant to OMB Circular No. A-123, "Management Accountability and Control" and the Federal Managers' Financial Integrity Act (FMFIA), if there is no assignment of security responsibility, no security plan, or no authorization to process for a system.

4) Authorize Processing. Ensure that a management official authorizes in writing the use of each general support system based on implementation of its security plan before beginning or significantly changing processing in the system. Use of the system shall be re-authorized at least every three years.

b. Controls for Major Applications.

1) Assign Responsibility for Security. Assign responsibility for security of

each major application to a management official knowledgeable in the nature of the information and process supported by the application and in the management, personnel, operational, and technical controls used to protect it. This official shall assure that effective security products and techniques are appropriately used in the application and shall be contacted when a security incident occurs concerning the application.

2) Application Security Plan. Plan for the adequate security of each major application, taking into account the security of all systems in which the application will operate. The plan shall be consistent with guidance issued by NIST. Advice and comment on the plan shall be solicited from the official responsible for security in the primary system in which the application will operate prior to the plan's implementation. A summary of the security plans shall be incorporated into the strategic IRM plan required by the Paperwork Reduction Act. Application security plans shall include:

a) Application Rules. Establish a set of rules concerning use of and behavior within the application. The rules shall be as stringent as necessary to provide adequate security for the application and the information in it. Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the application. In addition, the rules shall be clear about the consequences of behavior not consistent with the rules.

b) Specialized Training. Before allowing individuals access to the application, ensure that all individuals receive specialized training focused on their responsibilities and the application rules. This may be in addition to the training required for access to a system. Such training may vary from a notification at the time of access (e.g., for members of the public using an information retrieval application) to formal training (e.g., for an employee that works with a high-risk application).

c) Personnel Security. Incorporate controls such as separation of duties, least privilege and individual accountability into the application and application rules as appropriate. In cases where such controls cannot adequately protect the application or information in it, screen individuals commensurate with the risk and magnitude of the harm they could cause. Such screening shall be done prior to the individuals' being authorized to access the application and periodically thereafter.

d) Contingency Planning. Establish and periodically test the capability to perform the agency function supported by the application in the event of failure of its automated support.

e) Technical Controls. Ensure that appropriate security controls are specified, designed into, tested, and accepted in the application in

accordance with appropriate guidance issued by NIST.

f) Information Sharing. Ensure that information shared from the application is protected appropriately, comparable to the protection provided when information is within the application.

g) Public Access Controls. Where an agency's application promotes or permits public access, additional security controls shall be added to protect the integrity of the application and the confidence the public has in the application. Such controls shall include segregating information made directly accessible to the public from official agency records.

3) Review of Application Controls. Perform an independent review or audit of the security controls in each application at least every three years. Consider identifying a deficiency pursuant to OMB Circular No. A-123, "Management Accountability and Control" and the Federal Managers' Financial Integrity Act if there is no assignment of responsibility for security, no security plan, or no authorization to process for the application.

4) Authorize Processing. Ensure that a management official authorizes in writing use of the application by confirming that its security plan as implemented adequately secures the application. Results of the most recent review or audit of controls shall be a factor in management authorizations. The application must be authorized prior to operating and re-authorized at least every three years thereafter. Management authorization implies accepting the risk of each system used by the application.

#### 4. Assignment of Responsibilities

a. Department of Commerce. The Secretary of Commerce shall:

1) Develop and issue appropriate standards and guidance for the security of sensitive information in Federal computer systems.

2) Review and update guidelines for training in computer security awareness and accepted computer security practice, with assistance from OPM.

3) Provide agencies guidance for security planning to assist in their development of application and system security plans.

4) Provide guidance and assistance, as appropriate, to agencies concerning cost-effective controls when interconnecting with other systems.

5) Coordinate agency incident response activities to promote sharing of incident response information and related vulnerabilities.

6) Evaluate new information technologies to assess their security vulnerabilities, with technical assistance from the Department of Defense, and apprise Federal agencies of such vulnerabilities as soon as they are known.

b. Department of Defense. The Secretary of Defense shall:

1) Provide appropriate technical advice and assistance (including work products) to the Department of Commerce.

2) Assist the Department of Commerce in evaluating the vulnerabilities of emerging information technologies.

c. Department of Justice. The Attorney General shall:

1) Provide appropriate guidance to agencies on legal remedies regarding security incidents and ways to report and work with law enforcement concerning such incidents.

2) Pursue appropriate legal actions when security incidents occur.

d. General Services Administration. The Administrator of General Services shall:

1) Provide guidance to agencies on addressing security considerations when acquiring automated data processing equipment (as defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949, as amended).

2) Facilitate the development of contract vehicles for agencies to use in the acquisition of cost-effective security products and services (e.g., back-up services).

3) Provide appropriate security services to meet the needs of Federal agencies to the extent that such services are cost-effective.

e. Office of Personnel Management. The Director of the Office of Personnel Management shall:

1) Assure that its regulations concerning computer security training for Federal civilian employees are effective.

2) Assist the Department of Commerce in updating and maintaining guidelines for training in computer security awareness and accepted computer security practice.

f. Security Policy Board. The Security Policy Board shall coordinate the activities of the Federal government regarding the security of information technology that processes classified information in accordance with applicable national security directives;

## 5. Correction of Deficiencies and Reports

a. Correction of Deficiencies. Agencies shall correct deficiencies which are identified through the reviews of security for systems and major applications described above.

b. Reports on Deficiencies. In accordance with OMB Circular No. A-123, "Management Accountability and Control", if a deficiency in controls is judged by the agency head to be material when weighed against other agency deficiencies, it shall be included in the annual FMFIA report. Less significant deficiencies shall be reported and progress on corrective actions tracked at the appropriate agency level.

c. Summaries of Security Plans. Agencies shall include a summary of their system security plans and major application plans in the strategic plan required by the Paperwork Reduction Act (44 U.S.C. 3506).

### B. Descriptive Information.

The following descriptive language is explanatory. It is included to assist in understanding the requirements of the Appendix.

The Appendix re-orientes the Federal computer security program to better respond to a rapidly changing technological environment. It establishes government-wide responsibilities for Federal computer security and requires Federal agencies to adopt a minimum set of management controls. These management controls are directed at individual information technology users in order to reflect the distributed nature of today's technology.

For security to be most effective, the controls must be part of day-to-day operations. This is best accomplished by planning for security not as a separate activity, but as an integral part of overall planning.

"Adequate security" is defined as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." This definition explicitly emphasizes the risk-based policy for cost-effective security established by the Computer Security Act.

The Appendix no longer requires the preparation of formal risk analyses. In the past, substantial resources have been expended doing complex analyses of specific risks to systems, with limited tangible benefit in terms of improved security for the systems. Rather than continue to try to precisely measure risk, security efforts are better served by generally assessing risks and taking actions to manage them. While formal risk analyses need not be performed, the need to determine adequate security will require that a risk-based approach be used. This risk assessment approach should include a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards. Additional guidance on effective risk assessment is available in "An Introduction to Computer Security: The NIST Handbook" (March 16, 1995).

Discussion of the Appendix's Major Provisions. The following discussion is provided to aid reviewers in understanding the changes in emphasis in the Appendix.

Automated Information Security Programs. Agencies are required to establish controls to assure adequate security for all information processed, transmitted, or stored in Federal automated information systems. This Appendix emphasizes management controls affecting individual users of information technology. Technical and operational controls support management controls. To be effective, all must interrelate. For example, authentication of individual users is an important management control, for which password protection is a technical control. However, password protection will only be effective if both a strong technology is employed, and it is managed to assure that it is used correctly.

Four controls are set forth: assigning responsibility for security, security planning, periodic review of security controls, and management authorization. The Appendix requires that these management controls be applied in two areas of management responsibility: one for general support systems and one for major applications.

The terms "general support system" and "major application" were used in OMB Bulletins Nos. 88-16 and 90-08. A general support system is "an interconnected set of information resources under the same direct management control which shares common functionality." Such a system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization. Normally, the purpose of a general support system is to provide processing or communications support.

A major application is a use of information and information technology to satisfy a specific set of user requirements that requires special management attention to security due to the risk and magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of the information in the application. All applications require some level of security, and adequate security for most of them should be provided by security of the general support systems in which they operate. However, certain applications, because of the nature of the information in them, require special management oversight and should be treated as major. Agencies are expected to exercise management judgement in determining which of their applications are major.

The focus of OMB Bulletins Nos. 88-16 and 90-08 was on identifying and securing both general support systems and applications which contained sensitive information. The Appendix requires the establishment of security controls in all general support systems, under the presumption that all contain some sensitive information, and focuses extra security controls on a limited number of particularly high-risk or major applications.

a. General Support Systems. The following controls are required in all general support systems:

1) Assign Responsibility for Security. For each system, an individual should be a focal point for assuring there is adequate security within the system, including ways

to prevent, detect, and recover from security problems. That responsibility should be assigned in writing to an individual trained in the technology used in the system and in providing security for such technology, including the management of security controls such as user identification and authentication.

2) Security Plan. The Computer Security Act requires that security plans be developed for all Federal computer systems that contain sensitive information. Given the expansion of distributed processing since passage of the Act, the presumption in the Appendix is that all general support systems contain some sensitive information which requires protection to assure its integrity, availability, or confidentiality, and therefore all systems require security plans.

Previous guidance on security planning was contained in OMB Bulletin No. 90-08. This Appendix supersedes OMB Bulletin 90-08 and expands the coverage of security plans from Bulletin 90-08 to include rules of individual behavior as well as technical security. Consistent with OMB Bulletin 90-08, the Appendix directs NIST to update and expand security planning guidance and issue it as a Federal Information Processing Standard (FIPS). In the interim, agencies should continue to use the Appendix of OMB Bulletin No. 90-08 as guidance for the technical portion of their security plans.

The Appendix continues the requirement that independent advice and comment on the security plan for each system be sought. The intent of this requirement is to improve the plans, foster communication between managers of different systems, and promote the sharing of security expertise.

This Appendix also continues the requirement from the Computer Security Act that summaries of security plans be included in agency strategic information resources management plans. OMB will provide additional guidance about the contents of those strategic plans, pursuant to the Paperwork Reduction Act of 1995.

The following specific security controls should be included in the security plan for a general support system:

a) Rules. An important new requirement for security plans is the establishment of a set of rules of behavior for individual users of each general support system. These rules should clearly delineate responsibilities of and expectations for all individuals with access to the system. They should be consistent with system-specific policy as described in "An Introduction to Computer Security: The NIST Handbook" (March 16, 1995). In addition, they should state the consequences of non-compliance. The rules should be in writing and will form the basis for security awareness and training.

The development of rules for a system must take into consideration the needs of all parties who use the system. Rules should be as stringent as necessary to provide adequate security. Therefore, the acceptable level of risk for the system must be established and should form the basis for determining

the rules.

Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of government equipment, the assignment and limitation of system privileges, and individual accountability. Often rules should reflect technical security controls in the system. For example, rules regarding password use should be consistent with technical password features in the system. Rules may be enforced through administrative sanctions specifically related to the system (e.g. loss of system privileges) or through more general sanctions as are imposed for violating other rules of conduct. In addition, the rules should specifically address restoration of service as a concern of all users of the system.

b) Training. The Computer Security Act requires Federal agencies to provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use or operation of a Federal computer system within or under the supervision of the Federal agency. This includes contractors as well as employees of the agency. Access provided to members of the public should be constrained by controls in the applications through which access is allowed, and training should be within the context of those controls. The Appendix enforces such mandatory training by requiring its completion prior to granting access to the system. Each new user of a general support system in some sense introduces a risk to all other users. Therefore, each user should be versed in acceptable behavior -- the rules of the system -- before being allowed to use the system. Training should also inform the individual how to get help in the event of difficulty with using or security of the system.

Training should be tailored to what a user needs to know to use the system securely, given the nature of that use. Training may be presented in stages, for example as more access is granted. In some cases, the training should be in the form of classroom instruction. In other cases, interactive computer sessions or well-written and understandable brochures may be sufficient, depending on the risk and magnitude of harm.

Over time, attention to security tends to dissipate. In addition, changes to a system may necessitate a change in the rules or user procedures. Therefore, individuals should periodically have refresher training to assure that they continue to understand and abide by the applicable rules.

To assist agencies, the Appendix requires NIST, with assistance from the Office of Personnel Management (OPM), to update its existing guidance. It also proposes that OPM assure that its rules for computer security training for Federal civilian employees are effective.

c) Personnel Controls. It has long been recognized that the greatest harm has come from authorized individuals engaged in improper activities, whether intentional or accidental. In every general support system, a number of technical, operational, and management controls are used to prevent and detect harm. Such controls include individual accountability, "least privilege," and separation of duties.

Individual accountability consists of holding someone responsible for his or her actions. In a general support system, accountability is normally accomplished by identifying and authenticating users of the system and subsequently tracing actions on the system to the user who initiated them. This may be done, for example, by looking for patterns of behavior by users.

Least privilege is the practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform his or her job.

Separation of duties is the practice of dividing the steps in a critical function among different individuals. For example, one system programmer can create a critical piece of operating system code, while another authorizes its implementation. Such a control keeps a single individual from subverting a critical process.

Nevertheless, in some instances, individuals may be given the ability to bypass some significant technical and operational controls in order to perform system administration and maintenance functions (e.g., LAN administrators or systems programmers). Screening such individuals in positions of trust will supplement technical, operational, and management controls, particularly where the risk and magnitude of harm is high.

d) Incident Response Capability. Security incidents, whether caused by viruses, hackers, or software bugs, are becoming more common. When faced with a security incident, an agency should be able to respond in a manner that both protects its own information and helps to protect the information of others who might be affected by the incident. To address this concern, agencies should establish formal incident response mechanisms. Awareness and training for individuals with access to the system should include how to use the system's incident response capability.

To be fully effective, incident handling must also include sharing information concerning common vulnerabilities and threats with those in other systems and other agencies. The Appendix directs agencies to effectuate such sharing, and tasks NIST to coordinate those agency activities government-wide.

The Appendix also directs the Department of Justice to provide appropriate guidance on pursuing legal remedies in the case of serious incidents.

e) Continuity of Support. Inevitably, there will be service interruptions. Agency plans should assure that there is an ability to recover and provide service sufficient to meet the minimal needs of users of the system. Manual procedures are generally NOT a viable back-up option. When automated support is not available, many functions of the organization will effectively cease. Therefore, it is important to take cost-effective steps to manage any disruption of service.

Decisions on the level of service needed at any particular time and on priorities in service restoration should be made in consultation with the users of the system and incorporated in the system rules. Experience has shown that recovery plans that are periodically tested are substantially more viable than those that are not. Moreover, untested plans may actually create a false sense of security.

f) Technical Security. Agencies should assure that each system appropriately uses effective security products and techniques, consistent with standards and guidance from NIST. Often such techniques will correspond with system rules of behavior, such as in the proper use of password protection.

The Appendix directs NIST to continue to issue computer security guidance to assist agencies in planning for and using technical security products and techniques. Until such guidance is issued, however, the planning guidance included in OMB Bulletin 90-08 can assist in determining techniques for effective security in a system and in addressing technical controls in the security plan.

g) System Interconnection. In order for a community to effectively manage risk, it must control access to and from other systems. The degree of such control should be established in the rules of the system and all participants should be made aware of any limitations on outside access. Technical controls to accomplish this should be put in place in accordance with guidance issued by NIST.

There are varying degrees of how connected a system is. For example, some systems will choose to isolate themselves, others will restrict access such as allowing only e-mail connections or remote access only with sophisticated authentication, and others will be fully open. The management decision to interconnect should be based on the availability and use of technical and non-technical safeguards and consistent with the acceptable level of risk defined in the system rules.

3) Review of Security Controls. The security of a system will degrade over time, as the technology evolves and as people and procedures change. Reviews should assure that management, operational, personnel, and technical controls are functioning effectively. Security controls may be reviewed by an independent audit or a self review. The type and rigor of review or audit should be commensurate with the acceptable level of risk that is established in the rules for the system and the likelihood of learning useful information to improve security. Technical tools such as virus scanners, vulnerability assessment products (which look for known security problems, configuration errors, and the installation of the latest patches), and penetration testing can assist in the on-going review of different facets of systems. However, these tools are no substitute for a formal management review at least every three years. Indeed, for some high-risk systems with rapidly changing technology, three years will be too long.

Depending upon the risk and magnitude of harm that could result, weaknesses identified during the review of security controls should be reported as deficiencies in accordance with OMB Circular No. A-123, "Management Accountability and Control" and the Federal Managers' Financial Integrity Act. In particular, if a basic management control such as assignment of responsibility, a workable security plan, or management authorization are missing, then consideration should be given to identifying a deficiency.

4) Authorize Processing. The authorization of a system to process information, granted by a management official, provides an important quality control (some agencies refer to this authorization as accreditation). By authorizing processing in a system, a manager accepts the risk associated with it. Authorization is not a decision that should be made by the security staff.

Both the security official and the authorizing management official have security responsibilities. In general, the security official is closer to the day-to-day operation of the system and will direct or perform security tasks. The authorizing official will normally have general responsibility for the organization supported by the system.

Management authorization should be based on an assessment of management, operational, and technical controls. Since the security plan establishes the security controls, it should form the basis for the authorization, supplemented by more specific studies as needed. In addition, the periodic review of controls should also contribute to future authorizations. Some agencies perform "certification reviews" of their systems periodically. These formal technical evaluations lead to a management accreditation, or "authorization to process." Such certifications (such as those using the methodology in FIPS Pub 102 "Guideline for Computer Security Certification and Accreditation") can provide useful information to assist management in authorizing a system, particularly when combined with a review of the broad behavioral controls envisioned in the security plan required by the Appendix.

Re-authorization should occur prior to a significant change in processing, but at

least every three years. It should be done more often where there is a high risk and potential magnitude of harm.

b. Controls in Major Applications. Certain applications require special management attention due to the risk and magnitude of harm that could occur. For such applications, the controls of the support system(s) in which they operate are likely to be insufficient. Therefore, additional controls specific to the application are required. Since the function of applications is the direct manipulation and use of information, controls for securing applications should emphasize protection of information and the way it is manipulated.

1) Assign Responsibility for Security. By definition, major applications are high risk and require special management attention. Major applications usually support a single agency function and often are supported by more than one general support system. It is important, therefore, that an individual be assigned responsibility in writing to assure that the particular application has adequate security. To be effective, this individual should be knowledgeable in the information and process supported by the application and in the management, personnel, operational, and technical controls used to protect the application.

2) Application Security Plans. Security for each major application should be addressed by a security plan specific to the application. The plan should include controls specific to protecting information and should be developed from the application manager's perspective. To assist in assuring its viability, the plan should be provided to the manager of the primary support system which the application uses for advice and comment. This recognizes the critical dependence of the security of major applications on the underlying support systems they use. Summaries of application security plans should be included in strategic information resource management plans in accordance with this Circular.

a) Application Rules. Rules of behavior should be established which delineate the responsibilities and expected behavior of all individuals with access to the application. The rules should state the consequences of inconsistent behavior. Often the rules will be associated with technical controls implemented in the application. Such rules should include, for example, limitations on changing data, searching databases, or divulging information.

b) Specialized Training. Training is required for all individuals given access to the application, including members of the public. It should vary depending on the type of access allowed and the risk that access represents to the security of the application and information in it. This training will be in addition to that required for access to a support system.

c) Personnel Security. For most major applications, management controls such as individual accountability requirements, separation of duties enforced by access controls, or limitations on the processing privileges of individuals,

are generally more cost-effective personnel security controls than background screening. Such controls should be implemented as both technical controls and as application rules. For example, technical controls to ensure individual accountability, such as looking for patterns of user behavior, are most effective if users are aware that there is such a technical control. If adequate audit or access controls (through both technical and non-technical methods) cannot be established, then it may be cost-effective to screen personnel, commensurate with the risk and magnitude of harm they could cause. The change in emphasis on screening in the Appendix should not affect background screening deemed necessary because of other duties that an individual may perform.

d) Contingency Planning. Normally the Federal mission supported by a major application is critically dependent on the application. Manual processing is generally NOT a viable back-up option. Managers should plan for how they will perform their mission and/or recover from the loss of existing application support, whether the loss is due to the inability of the application to function or a general support system failure. Experience has demonstrated that testing a contingency plan significantly improves its viability. Indeed, untested plans or plans not tested for a long period of time may create a false sense of ability to recover in a timely manner.

e) Technical Controls. Technical security controls, for example tests to filter invalid entries, should be built into each application. Often these controls will correspond with the rules of behavior for the application. Under the previous Appendix, application security was focused on the process by which sensitive, custom applications were developed. While that process is not addressed in detail in this Appendix, it remains an effective method for assuring that security controls are built into applications. Additionally, the technical security controls defined in OMB Bulletin No. 90-08 will continue, until that guidance is replaced by NIST's security planning guidance.

f) Information Sharing. Assure that information which is shared with Federal organizations, State and local governments, and the private sector is appropriately protected comparable to the protection provided when the information is within the application. Controls on the information may stay the same or vary when the information is shared with another entity. For example, the primary user of the information may require a high level of availability while the secondary user does not, and can therefore relax some of the controls designed to maintain the availability of the information. At the same time, however, the information shared may require a level of confidentiality that should be extended to the secondary user. This normally requires notification and agreement to protect the information prior to its being shared.

g) Public Access Controls. Permitting public access to a Federal

application is an important method of improving information exchange with the public. At the same time, it introduces risks to the Federal application. To mitigate these risks, additional controls should be in place as appropriate. These controls are in addition to controls such as "firewalls" that are put in place for security of the general support system.

In general, it is more difficult to apply conventional controls to public access systems, because many of the users of the system may not be subject to individual accountability policies. In addition, public access systems may be a target for mischief because of their higher visibility and published access methods.

Official records need to be protected against loss or alteration. Official records in electronic form are particularly susceptible since they can be relatively easy to change or destroy. Therefore, official records should be segregated from information made directly accessible to the public. There are different ways to segregate records. Some agencies and organizations are creating dedicated information dissemination systems (such as bulletin boards or World Wide Web servers) to support this function. These systems can be on the outside of secure gateways which protect internal agency records from outside access.

In order to secure applications that allow direct public access, conventional techniques such as least privilege (limiting the processing capability as well as access to data) and integrity assurances (such as checking for viruses, clearly labeling the age of data, or periodically spot checking data) should also be used. Additional guidance on securing public access systems is available from NIST Computer Systems Laboratory Bulletin "Security Issues in Public Access Systems" (May, 1993).

3) Review of Application Controls. At least every three years, an independent review or audit of the security controls for each major application should be performed. Because of the higher risk involved in major applications, the review or audit should be independent of the manager responsible for the application. Such reviews should verify that responsibility for the security of the application has been assigned, that a viable security plan for the application is in place, and that a manager has authorized the processing of the application. A deficiency in any of these controls should be considered a deficiency pursuant to the Federal Manager's Financial Integrity Act and OMB Circular No. A-123, "Management Accountability and Control."

The review envisioned here is different from the system test and certification process required in the current Appendix. That process, however, remains useful for assuring that technical security features are built into custom-developed software applications. While the controls in that process are not specifically called for in this Appendix, they remain in Bulletin No. 90-08, and are recommended in appropriate

circumstances as technical controls.

4) Authorize Processing. A major application should be authorized by the management official responsible for the function supported by the application at least every three years, but more often where the risk and magnitude of harm is high. The intent of this requirement is to assure that the senior official whose mission will be adversely affected by security weaknesses in the application periodically assesses and accepts the risk of operating the application. The authorization should be based on the application security plan and any review(s) performed on the application. It should also take into account the risks from the general support systems used by the application.

4. Assignment of Responsibilities. The Appendix assigns government-wide responsibilities to agencies that are consistent with their missions and the Computer Security Act.

a. Department of Commerce. The Department of Commerce, through NIST, is assigned the following responsibilities consistent with the Computer Security Act.

1) Develop and issue security standards and guidance.

2) Review and update, with assistance from OPM, the guidelines for security training issued in 1988 pursuant to the Computer Security Act to assure they are effective.

3) Replace and update the technical planning guidance in the appendix to OMB Bulletin 90-08 This should include guidance on effective risk-based security absent a formal risk analysis.

4) Provide agencies with guidance and assistance concerning effective controls for systems when interconnecting with other systems, including the Internet. Such guidance on, for example, so-called "firewalls" is becoming widely available and is critical to agencies as they consider how to interconnect their communications capabilities.

5) Coordinate agency incident response activities. Coordination of agency incident response activities should address both threats and vulnerabilities as well as improve the ability of the Federal government for rapid and effective cooperation in response to serious security breaches.

6) Assess security vulnerabilities in new information technologies and apprise Federal agencies of such vulnerabilities. The intent of this new requirement is to help agencies understand the security implications of technology before they purchase and field it. In the past, there have been too many instances where agencies have acquired and implemented technology, then found out about vulnerabilities in the technology and had to retrofit security measures. This activity is intended to help avoid such difficulties in the future.

b. Department of Defense. The Department, through the National Security Agency, should provide technical advice and assistance to NIST, including work products such as technical security guidelines, which NIST can draw upon for developing standards and guidelines for protecting sensitive information in Federal computers.

Also, the Department, through the National Security Agency, should assist NIST in evaluating vulnerabilities in emerging technologies. Such vulnerabilities may present a risk to national security information as well as to unclassified information.

c. Department of Justice. The Department of Justice should provide appropriate guidance to Federal agencies on legal remedies available to them when serious security incidents occur. Such guidance should include ways to report incidents and cooperate with law enforcement.

In addition, the Department should pursue appropriate legal actions on behalf of the Federal government when serious security incidents occur.

d. General Services Administration. The General Services Administration should provide agencies guidance for addressing security considerations when acquiring information technology products or services. This continues the current requirement.

In addition, where cost-effective to do so, GSA should establish government-wide contract vehicles for agencies to use to acquire certain security services. Such vehicles already exist for providing system back-up support and conducting security analyses.

GSA should also provide appropriate security services to assist Federal agencies to the extent that provision of such services is cost-effective. This includes providing, in conjunction with the Department of Defense and the Department of Commerce, appropriate services which support Federal use of the National Information Infrastructure (e.g., use of digital signature technology).

e. Office of Personnel Management. In accordance with the Computer Security Act, OPM should review its regulations concerning computer security training and assure that they are effective.

In addition, OPM should assist the Department of Commerce in the review and update of its computer security awareness and training guidelines. OPM worked closely with NIST in developing the current guidelines and should work with NIST in revising those guidelines.

f. Security Policy Board. The Security Policy Board is assigned responsibility for national security policy coordination in accordance with the appropriate Presidential directive. This includes policy for the security of information technology used to process classified information.

Circular A-130 and this Appendix do not apply to information technology that supports certain critical national security missions, as defined in 44 U.S.C. 3502(9) and 10 U.S.C.

2315. Policy and procedural requirements for the security of national security systems (telecommunications and information systems that contain classified information or that support those critical national security missions (44 U.S.C. 3502(9) and 10 U.S.C. 2315)) is assigned to the Department of Defense pursuant to Presidential directive. The Circular clarifies that information classified for national security purposes should also be handled in accordance with appropriate national security directives. Where classified information is required to be protected by more stringent security requirements, those requirements should be followed rather than the requirements of this Appendix.

5. Reports. The Appendix requires agencies to provide two reports to OMB:

The first is a requirement that agencies report security deficiencies and material weaknesses within their FMFIA reporting mechanisms as defined by OMB Circular No. A-123, "Management Accountability and Control," and take corrective actions in accordance with that directive.

The second, defined by the Computer Security Act, requires that a summary of agency security plans be included in the information resources management plan required by the Paperwork Reduction Act.

under section 764.8 of the EAR. The information collected will allow BIS to conduct investigations of the disclosed incidents more immediately by than would be the case if BIS had to detect the violations without such disclosures.

## II. Method of Collection

Submitted in paper form.

## III. Data

*OMB Control Number:* 0694-0132.

*Form Number(s):* None.

*Type of Review:* Regular submission.

*Affected Public:* Business or other for-profit organizations.

*Estimated Number of Respondents:* 10.

*Estimated Time per Response:* 10 to 600 hours (depending on the size of the company).

*Estimated Total Annual Burden Hours:* 1,280.

*Estimated Total Annual Cost to Public:* \$0.

## IV. Request for Comments

Comments are invited on: (a) Whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden (including hours and cost) of the proposed collection of information; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or other forms of information technology.

Comments submitted in response to this notice will be summarized and/or included in the request for OMB approval of this information collection; they also will become a matter of public record.

Dated: July 21, 2010.

### Gwellnar Banks,

*Management Analyst, Office of the Chief Information Officer.*

[FR Doc. 2010-18161 Filed 7-23-10; 8:45 am]

**BILLING CODE 3510-33-P**

## DEPARTMENT OF COMMERCE

### National Oceanic and Atmospheric Administration

#### Proposed Information Collection; Comment Request; Vessel Monitoring System Requirements in Western Pacific Pelagic and Bottomfish Fisheries

**AGENCY:** National Oceanic and Atmospheric Administration (NOAA).

**ACTION:** Notice.

**SUMMARY:** The Department of Commerce, as part of its continuing effort to reduce paperwork and respondent burden, invites the general public and other Federal agencies to take this opportunity to comment on proposed and/or continuing information collections, as required by the Paperwork Reduction Act of 1995.

**DATES:** Written comments must be submitted on or before September 24, 2010.

**ADDRESSES:** Direct all written comments to Diana Hynek, Departmental Paperwork Clearance Officer, Department of Commerce, Room 6616, 14th and Constitution Avenue, NW., Washington, DC 20230 (or via the Internet at [dHynek@doc.gov](mailto:dHynek@doc.gov)).

**FOR FURTHER INFORMATION CONTACT:** Requests for additional information or copies of the information collection instrument and instructions should be directed to Walter Ikehara, (808) 944-2275 or [Walter.Ikehara@noaa.gov](mailto:Walter.Ikehara@noaa.gov).

#### SUPPLEMENTARY INFORMATION:

##### I. Abstract

This request is for a revision of a currently approved information collection. As part of fishery management plans developed under the authority of the Magnuson-Stevens Fishery Conservation and Management Act (MSA), owners of commercial fishing vessels in the Hawaii pelagic longline fishery, American Samoa pelagic longline fishery (only vessels longer than 50 feet), and Northern Mariana Islands bottomfish fishery (only vessels longer than 40 feet) must allow the National Oceanic and Atmospheric Administration (NOAA) to install vessel monitoring system (VMS) units on their vessels when directed to do so by NOAA enforcement personnel. VMS units automatically send periodic reports on the position of the vessel. NOAA uses the reports to monitor the vessel's location and activities, primarily to enforce regulated fishing areas. NOAA pays for the units and messaging. There is no public burden for the automatic messaging; however,

VMS installation and annual maintenance are considered public burden.

This request combines three OMB approved collections for VMS requirements, OMB Control No. 0648-0441 (Vessel Monitoring System Requirements in the Western Pacific Pelagic Longline Fishery), OMB Control No. 0648-0519 (Vessel Monitoring System Requirement for American Samoa Pelagic Longline Fishery), and the VMS requirement from OMB Control No. 0648-0584 (Permitting, Vessel Identification and Vessel Monitoring System Requirements for the Commercial Bottomfish Fishery in the Commonwealth of the Northern Mariana Islands), into one collection (OMB Control No. 0648-0441).

## II. Method of Collection

Automatic.

## III. Data

*OMB Control Number:* 0648-0441.

*Form Number:* None.

*Type of Review:* Regular submission (revision of a currently approved information collection).

*Affected Public:* Business or other for-profit organizations.

*Estimated Number of Respondents:* 209.

*Estimated Time per Response:* 4 hours for installation or replacement of a VMS unit; 2 hours for annual maintenance.

*Frequency:* Annually and on occasion.

*Respondent's Obligation:* Mandatory.

*Estimated Total Annual Burden Hours:* 478 (estimated 15 installations per year).

*Estimated Total Annual Cost to Public:* \$0 in recordkeeping/reporting costs.

## IV. Request for Comments

Comments are invited on: (a) Whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden (including hours and cost) of the proposed collection of information; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or other forms of information technology.

Comments submitted in response to this notice will be summarized and/or included in the request for OMB approval of this information collection; they also will become a matter of public record.

Dated: July 21, 2010.

**Gwellnar Banks,**

*Management Analyst, Office of the Chief Information Officer.*

[FR Doc. 2010-18205 Filed 7-23-10; 8:45 am]

BILLING CODE 3510-22-P

**DEPARTMENT OF COMMERCE**

**International Trade Administration**

[C-533-821]

**Certain Hot-Rolled Carbon Steel Flat Products From India: Final Results of Countervailing Duty Administrative Review**

**AGENCY:** Import Administration, International Trade Administration, Department of Commerce.

**SUMMARY:** On January 11, 2010, the U.S. Department of Commerce (the Department) published in the **Federal Register** its preliminary results of the administrative review of the countervailing duty (CVD) order on certain hot-rolled carbon steel flat products (hot-rolled carbon steel) from India for the period of review (POR) January 1, 2008, through December 31, 2008. See *Certain Hot-Rolled Carbon Steel Flat Products from India: Preliminary Results of Countervailing Duty Administrative Review*; 75 FR 1495 (January 11, 2010) (*Preliminary Results*). We preliminarily found that Tata Steel Limited (Tata) received countervailable subsidies during the POR. We received comments on our *Preliminary Results* from the Government of India (GOI), petitioners, and the respondent company, Tata.<sup>1</sup> The final results are listed in the section "Final Results of Review" below.

**DATES:** *Effective Date:* July 26, 2010.

**FOR FURTHER INFORMATION CONTACT:** Gayle Longest at (202) 482-3338, AD/CVD Operations, Office 3, Import Administration, International Trade Administration, U.S. Department of Commerce, 14th Street and Constitution Ave., NW., Washington, DC 20230.

**SUPPLEMENTARY INFORMATION:**

**Background**

On December 3, 2001, the Department published in the **Federal Register** the CVD order on certain hot-rolled carbon steel flat products from India. See *Notice of Amended Final Determination and Notice of Countervailing Duty Order: Certain Hot-Rolled Carbon Steel Flat Products from India*, 66 FR 60198 (December 3, 2001). On February 2,

2009, the Department initiated an administrative review covering Essar Steel Limited (Essar), Ispat Industries Limited (Ispat), JSW Steel Limited (JSW), and Tata. See *Initiation of Antidumping and Countervailing Duty Administrative Reviews and Requests for Revocation in Part*, 74 FR 5821 (February 2, 2009) (*Initiation*). As a result of withdrawals of request for review, the Department rescinded this review, in part, with respect to Essar, Ispat, and JSW. See *Certain Hot-Rolled Carbon Steel Flat Products from India: Partial Rescission of Countervailing Duty Administrative Review*, 74 FR 26847 (June 4, 2009).

On January 11, 2010, the Department published in the **Federal Register** its *Preliminary Results* of the administrative review of this order for the period January 1, 2008, through December 31, 2008. See *Preliminary Results*, 75 FR 1495. In accordance with 19 CFR 351.213(b), this administrative review covers Tata, a producer and exporter of subject merchandise.

In the *Preliminary Results*, we invited interested parties to submit briefs or request a hearing. On February 12, 2010, we received comments from the GOI and Tata. On February 19, 2010, we received rebuttal comments from petitioners.

**Scope of Order**

The merchandise subject to this order is certain hot-rolled carbon-quality steel products of a rectangular shape, of a width of 0.5 inch or greater, neither clad, plated, nor coated with metal and whether or not painted, varnished, or coated with plastics or other non-metallic substances, in coils (whether or not in successively superimposed layers), regardless of thickness, and in straight lengths, of a thickness of less than 4.75 mm and of a width measuring at least 10 times the thickness.

Universal mill plate (*i.e.*, flat-rolled products rolled on four faces or in a closed box pass, or a width exceeding 150 mm, but not exceeding 1250 mm, and of a thickness of not less than 4 mm, not in coils and without patterns in relief) of a thickness not less than 4.0 mm is not included within the scope of this order.

Specifically included in the scope of this order are vacuum degassed, fully stabilized (commonly referred to as interstitial-free (IF) steels, high-strength low-alloy (HSLA) steels, and the substrate for motor lamination steels. IF steels are recognized as low-carbon steels with micro-alloying levels of elements such as titanium or niobium (also commonly referred to as columbium), or both, added to stabilize

carbon and nitrogen elements. HSLA steels are recognized as steels with micro-alloying levels of elements such as chromium, copper, niobium, vanadium, and molybdenum. The substrate for motor lamination steels contains micro-alloying levels of elements such as silicon and aluminum.

Steel products included in the scope of this order, regardless of definitions in the Harmonized Tariff Schedule of the United States (HTS), are products in which: (i) Iron predominates, by weight, over each of the other contained elements; (ii) the carbon content is 2 percent or less, by weight; and (iii) none of the elements listed below exceeds the quantity, by weight, respectively indicated:

1.80 percent of manganese, or  
2.25 percent of silicon, or  
1.00 percent of copper, or  
0.50 percent of aluminum, or  
1.25 percent of chromium, or  
0.30 percent of cobalt, or  
0.40 percent of lead, or  
1.25 percent of nickel, or  
0.30 percent of tungsten, or  
0.10 percent of molybdenum, or  
0.10 percent of niobium, or  
0.15 percent of vanadium, or  
0.15 percent of zirconium.

All products that meet the physical and chemical description provided above are within the scope of this order unless otherwise excluded. The following products, by way of example, are outside or specifically excluded from the scope of this order.

- Alloy hot-rolled steel products in which at least one of the chemical elements exceeds those listed above (including, *e.g.*, ASTM specifications A543, A387, A514, A517, A506).
- SAE/AISI grades of series 2300 and higher.
- Ball bearings steels, as defined in the HTS.
- Tool steels, as defined in the HTS.
- Silico-manganese (as defined in the HTS) or silicon electrical steel with a silicon level exceeding 2.25 percent.
- ASTM specifications A710 and A736.
- USS Abrasion-resistant steels (USS AR 400, USS AR 500).
- All products (proprietary or otherwise) based on an alloy ASTM specification (sample specifications: ASTM A506, A507).
- Non-rectangular shapes, not in coils, which are the result of having been processed by cutting or stamping and which have assumed the character of articles or products classified outside chapter 72 of the HTS.

The merchandise subject to this order is currently classifiable in the HTS at

<sup>1</sup>Petitioners are the United States Steel Corporation and Nucor Corporation (collectively, petitioners).