

NOTICE OF OFFICE OF MANAGEMENT AND BUDGET ACTION

Date 12/04/2008

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

In accordance with the Paperwork Reduction Act, OMB has taken action on your request received 05/26/2008

ACTION REQUESTED: Extension without change of a currently approved collection
TYPE OF REVIEW REQUESTED: Regular
ICR REFERENCE NUMBER: 200805-0648-003
AGENCY ICR TRACKING NUMBER:
TITLE: Vessel Monitoring System Requirement for American Samoa Pelagic Longline Fishery
LIST OF INFORMATION COLLECTIONS: See next page

OMB ACTION: Approved without change
OMB CONTROL NUMBER: 0648-0519
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: 12/31/2011 DISCONTINUE DATE:

BURDEN:	RESPONSES	HOURS	COSTS
Previous	297,840	167	0
New	44	96	0
Difference			
Change due to New Statute	0	0	0
Change due to Agency Discretion	0	0	0
Change due to Agency Adjustment	-297,796	-71	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 Requirement for American Samoa Pelagic Longline Fishery - VMS installation			50 CFR 665.25
Vessel Monitoring System Requirement for American Samoa Pelagic Longline Fishery - VMS Maintenance			50 CFR 665.25

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 b. <input type="checkbox"/> None 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
7. Title	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
8. Agency form number(s) (<i>if applicable</i>)	6. Requested expiration date a. <input type="checkbox"/> Three years from approval date b. <input type="checkbox"/> Other Specify: _____ / _____
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 REQUIREMENT
FOR AMERICAN SAMOA PELAGIC LONGLINE FISHERY
OMB CONTROL NO. 0648-0519**

INTRODUCTION

This Supporting Statement describes a renewal of the existing information collection under Office of Management and Budget (OMB) Control No. 0648-0519.

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 (WPFMC or Council), to develop fishery management plans (FMP) 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 Marine Fisheries Service (NMFS) via Federal regulations that are enforced by the National Oceanic and Atmospheric Administration, Office for Law Enforcement (NOAA OLE) and U.S. Coast Guard (USCG), in cooperation with State agencies to the extent possible. FMP regulate fishing to ensure the long-term productivity and optimum yield of the resources for the benefit of the U.S.

The WPFMC has management jurisdiction over fisheries in the Pacific Ocean seaward of American Samoa, Guam, Hawaii, Northern Mariana Islands, and certain other remote U.S. Pacific island possessions¹. The Council has prepared, and the Secretary has approved and implemented through regulations, FMP for crustaceans, precious coral, pelagic, and bottomfish/seamount groundfish fisheries and coral reef ecosystems in the western Pacific region. 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 665.25**, implementing the Fishery Management Plan for Pelagic Fisheries of the Western Pacific Region (Pelagics FMP), require all large vessels (greater than 50 ft in overall length) registered for use with American Samoa longline limited access permits to maintain and operate 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 them at no cost to 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.

¹ Howland, Baker, Jarvis, Wake and Palmyra Islands, Johnston Atoll and Kingman Reef.

2. Explain how, by whom, how frequently, and for what purpose the information will be used. If the information collected will be disseminated to the public or used to support information that will be disseminated to the public, then explain how the collection complies with all applicable Information Quality Guidelines.

On a broad level, the Vessel Monitoring System (VMS) vessel location reports are used to facilitate enforcement of the 50 nautical mileage vessel prohibited area around American Samoa (50 CFR 665.37). 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 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 not be disseminated to the public inasmuch as it is primarily for use internally by NOAA OLE and USCG. The information will enable both agencies to effectively monitor any potential for violations of the American Samoa large vessel prohibited area regulation. The information may be used by NMFS scientists to cross-check the accuracy of logbook information submitted to NMFS by the vessel operators. Any of the information that might be used to support publicly disseminated information would first be aggregated and/or summarized to maintain the confidentiality of the information pertaining to the individual vessels. See response #10 of this Supporting Statement for more information on confidentiality and privacy. If NMFS makes public non-confidential information, then 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 requirement integrates current information technology in the fishery management and monitoring process. The collection of information is automatic and invisible. Many vessel owners have taken advantage of this technology by linking personal computers to VMS units to improve communication with other vessels. Although not related directly to VMS, the system could be used by fishermen to transmit their catch and effort data to NMFS on a real-time basis. The NMFS is implementing a program to enable electronic reporting to take the place of paper logbooks. This program is expected to be operational by the end of 2008 or early 2009.

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 are 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 time of 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 times when installation of the unit could be performed to minimize interfering with vessel operations. 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 cost of \$100,000.

There is no reporting frequency requirement for the vessel owner. The frequency with which a vessel VMS is polled to determine location is set by NOAA OLE and USCG.

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 frequency 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 renewal was published on December 10, 2007 (72 FR 69669). No comments were received. The NOAA Office for Law Enforcement was consulted for the accuracy of estimates and burden.

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 as 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; the Government Information Security Reform Act and follows NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems; NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems; NIST SP 800-53, Recommended Security Controls for Federal Information Systems.

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 American Samoa longline limited access permit program, 35 large vessels (greater than 50 ft in length) are currently registered in the fishery. The limited access program allows up to 12 Class A size vessel permits (up to 40 ft in length) to be upgraded to large vessels; four have already been upgraded and registered. If all remaining permit upgrades are used, the maximum number of large vessels possible would be 47. It is not likely that all permit upgrades would be used, however, as Class A vessels are not currently showing a great deal of profit; therefore, the estimate of 47 will not be used, but rather an estimate of 40 respondents.

This collection includes burden estimates for installation/replacement of a VMS unit and repair and maintenance of a unit. The actual VMS reporting is automatic and is thus not counted as respondent burden.

The estimated time per response is 4 hours to install a VMS unit (4 vessels per year estimated) and 2 hours per year to repair and maintain a VMS unit.

The vessel owner or representative generally observes the initial installation, which involves a total of about 16 hours (4 vessels x 4 hours per vessel). The vessel owner or representative also may observe any maintenance or repairs estimated at 80 hours per year (40 vessels x 2 hours per vessel per year).

4 vessels x 4 hours per vessel to install unit = 16 hours
40 vessels x 2 hours per year maintenance = 80 hours
Total estimated burden hours = 96 hrs
Total estimated responses = 44.

13. Provide an estimate of the total annual cost burden to the respondents or record-keepers resulting from the collection (excluding the value of the burden hours in #12 above).

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 the government.

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

The initial cost to the government during the first year of the program included 36 VMS units, software, installation, and equipment for a base station, with a total estimated cost of approximately \$170,000. For subsequent years, the estimated cost of the total program is \$100,000 per year, primarily for messaging costs.

15. Explain the reasons for any program changes or adjustments reported in Items 13 or 14 of the OMB 83-I.

Adjustments were made to the burden estimate based on a revised estimate of responses: 1) since the first request involving 34 vessels, an additional five vessels have been affected and one more may be added, adding 12 hours for maintenance; however, 2) based on the OMB clarification that automatic transmission time does not equal burden hours for the respondent, the previous 83 hours for transmission have been removed, and no transmission burden hours have been added for the six additional vessels.

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. The 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.

N/A

18. Explain each exception to the certification statement identified in Item 19 of the OMB 83-I.

N/A

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]¹⁵ 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.

¹⁵ 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)¹⁶—

(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.

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

§ 665.24

notice must provide the official number of the vessel, the name of the vessel, the intended departure date, time, and location, the name of the operator of the vessel, and the name and telephone number of the agent designated by the permit holder to be available between 8 a.m. and 5 p.m. (local time) on weekdays for NMFS to contact to arrange observer placement. Permit holders for vessels registered for use under Hawaii longline limited access permits must also provide notification of the trip type (either deep-setting or shallow-setting).

(b) The operator of any vessel subject to the requirements of this subpart who does not have on board a VMS unit while transiting the protected species zone as defined in § 665.12, must notify the NMFS Special-Agent-In-Charge immediately upon entering and immediately upon departing the protected species zone. The notification must include the name of the vessel, name of the operator, date and time (GMT) of access or exit from the protected species zone, and location by latitude and longitude to the nearest minute.

(c) The permit holder for any American Samoa longline limited access permit, or an agent designated by the permit holder, must notify the Regional Administrator in writing within 30 days of any change to the permit holder's contact information or any change to the vessel documentation associated with a permit registered to an American Samoa longline limited access permit. Complete changes in the ownership of the vessel registered to an American Samoa longline limited access permit must also be reported to PIRO in writing within 30 days of the change. Failure to report such changes may result in a delay in processing an application, permit holders failing to receive important notifications, or sanctions pursuant to the Magnuson-Stevens Act at 16 U.S.C. § 1858(g) or 15 CFR part 904, subpart D.

[70 FR 29654, May 24, 2005]

§ 665.24 Gear identification.

(a) *Identification.* The operator of each permitted vessel in the fishery management area must ensure that the official number of the vessel be affixed to every longline buoy and float, in-

50 CFR Ch. VI (10-1-06 Edition)

cluding each buoy and float that is attached to a radar reflector, radio antenna, or flag marker, whether attached to a deployed longline or possessed on board the vessel. Markings must be legible and permanent, and must be of a color that contrasts with the background material.

(b) *Enforcement action.* Longline gear not marked in compliance with paragraph (a) of this section and found deployed in the EEZ will be considered unclaimed or abandoned property, and may be disposed of in any manner considered appropriate by NMFS or an authorized officer.

§ 665.25 Vessel monitoring system.

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

(b) *Notification.* After a Hawaii longline limited access permit holder or size Class C or D American Samoa longline limited access permit holder 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 the VMS unit after the date scheduled for installation.

(c) *Fees and charges.* During the experimental VMS program, a Hawaii longline limited access permit holder or size Class C or D American Samoa longline permit holder with a size Class D or D permit 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.

(d) *Permit holder duties.* The holder of a Hawaii longline limited access permit or a size Class C or D American Samoa longline permit and master of the vessel must:

(1) Provide opportunity for the SAC to install and make operational a VMS unit after notification.

(2) Carry the VMS unit on board whenever the vessel is at sea.

(3) Not remove or relocate the VMS unit without prior approval from the SAC.

Fishery Conservation and Management

§ 665.27

(e) *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.

[61 FR 34572, July 2, 1996, as amended at 70 FR 29654, May 24, 2005]

§ 665.26 Longline fishing prohibited area management.

(a) *Prohibited areas.* Longline fishing shall be prohibited in the longline fishing prohibited areas as defined in paragraphs (b), (c), and (d) of this section.

(b) *Longline protected species zone.* The protected species zone is 50 nm from the center geographical positions of Nihoa Island, Necker Island, French Frigate Shoals, Gardner Pinnacles, Maro Reef, Laysan Island, Lisianski Island, Pearl and Hermes Reef, Midway Islands, and Kure Island, as defined in § 665.12.

(c) *Main Hawaiian Islands.* (1) From February 1 through September 30 each year, the longline fishing prohibited area around the main Hawaiian Islands is the portion of the EEZ seaward of Hawaii bounded by straight lines connecting the following coordinates in the order listed:

Point	N. lat.	DW. long.
A	18°05'	155°40'
B	18°20'	156°25'
C	20°00'	157°30'
D	20°40'	161°40'
E	21°40'	161°55'
F	23°00'	161°30'
G	23°05'	159°30'
H	22°55'	157°30'
I	21°30'	155°30'
J	19°50'	153°50'
K	19°00'	154°05'
A	18°05'	155°40'

(2) From October 1 through the following January 31 each year, the longline fishing prohibited area around the main Hawaiian Islands is the portion of the EEZ seaward of Hawaii bounded by straight lines connecting the following coordinates in the order listed:

Point	N. lat.	W. long.
A	18°05'	155°40'
L	18°25'	155°40'
M	19°00'	154°45'

Point	N. lat.	W. long.
N	19°15'	154°25'
O	19°40'	154°20'
P	20°20'	154°55'
Q	20°35'	155°30'
R	21°00'	155°35'
S	22°30'	157°35'
T	22°40'	159°35'
U	22°25'	160°20'
V	21°55'	160°55'
W	21°40'	161°00'
E	21°40'	161°55'
D	20°40'	161°40'
C	20°00'	157°30'
B	18°20'	156°25'
A	18°05'	155°40'

(d) *Guam.* The longline fishing prohibited area around Guam is the waters seaward of Guam bounded by straight lines connecting the following coordinates in the order listed:

Point	N. lat.	E. long.
A	14°25'	144°00'
B	14°00'	143°38'
C	13°41'	143°33'33"
D	13°00'	143°25'30"
E	12°20'	143°37'
F	11°40'	144°09'
G	12°00'	145°00'
H	13°00'	145°42'
I	13°27'	145°51'

[61 FR 34572, July 2, 1996, as amended at 71 FR 10869, Mar. 3, 2006]

§ 665.27 Exemptions for longline fishing prohibited areas; procedures.

(a) An exemption permitting a person to use longline gear to fish in a portion(s) of the Hawaii longline fishing prohibited area will be issued to a person who can document that he or she:

(1) Currently owns a Hawaii longline limited access permit issued under this part and registered for use with his or her vessel.

(2) Before 1970, was the owner or operator of a vessel when that vessel landed Pacific pelagic management unit species taken on longline gear in an area that is now within the Hawaii longline fishing prohibited area.

(3) Was the owner or operator of a vessel that landed Pacific pelagic management unit species taken on longline gear in an area that is now within the Hawaii longline fishing prohibited area, in at least 5 calendar years after 1969, which need not be consecutive.

(4) In any one of the 5 calendar years, was the owner or operator of a vessel that harvested at least 80 percent of its

§ 665.37

50 CFR Ch. VI (10–1–06 Edition)

(ii) Any person with documented participation in the pelagic longline fishery in the EEZ around American Samoa.

(2) *Class A Permits.* An American Samoa longline limited access permit of Class A may be transferred (by sale, gift, bequest, intestate succession, barter, or trade) to the following persons only:

(i) A family member of the permit holder,

(ii) A Western Pacific community located in American Samoa that meets the criteria set forth in section 305(I)(2) of the Magnuson-Stevens Act, 16 U.S.C. 1855(I)(2), and its implementing regulations, or

(iii) Any person with documented participation in the pelagic longline fishery on a Class A size vessel in the EEZ around American Samoa prior to March 22, 2002.

(3) *Class B-1, C-1, and D-1 Permits.* Class B-1, C-1, and D-1 permits may not be transferred to a different owner for 3 years from the date of initial issuance, except by bequest or intestate succession if the permit holder dies during those 3 years. After the initial 3 years, Class B-1, C-1, and D-1 permits may be transferred only in accordance with the restrictions in paragraph (I)(1) of this section.

(j) *Permit renewal and registration of vessels—(1) Use requirements.* An American Samoa longline limited access permit will not be renewed following 3 consecutive calendar years (beginning with the year after the permit was issued in the name of the current permit holder) in which the vessel(s) to which it is registered landed less than:

(i) For permit size Classes A or B: a total of 1,000 lb (455 kg) of Pacific pelagic management unit species harvested in the EEZ around American Samoa using longline gear, or

(ii) For permit size Classes C or D: a total of 5,000 lb (2,273 kg) of Pacific pelagic management unit species harvested in the EEZ around American Samoa using longline gear.

(k) *Concentration of ownership of permits.* No more than 10 percent of the maximum number of permits, of all size classes combined, may be held by the same permit holder. Fractional interest will be counted as a full permit

for the purpose of calculating whether the 10-percent standard has been reached.

(l) *Three year review.* Within 3 years of the effective date of this final rule the Council shall consider appropriate revisions to the American Samoa limited entry program after reviewing the effectiveness of the program with respect to its biological and socio-economic objectives, concerning gear conflict, overfishing, enforceability, compliance, and other issues.

[70 FR 29654, May 24, 2005; 70 FR 33719, June 9, 2005]

§ 665.37 American Samoa pelagic fishery area management.

(a) *Large vessel prohibited areas.* A large vessel of the United States may not be used to fish for Pacific pelagic management unit species in the American Samoa large vessel prohibited areas as defined in paragraphs (b) and (c) of this section, except as allowed pursuant to an exemption issued under § 665.38.

(b) *Tutuila Island, Manu'a Islands, and Rose Atoll (AS-1).* The large vessel prohibited area around Tutuila Island, the Manu'a Islands, and Rose Atoll consists of the waters of the EEZ around American Samoa enclosed by straight lines connecting the following coordinates:

Point	S. lat.	W. long.
AS-1-A	13°30'	167°25'
AS-1-B	15°13'	167°25'

and from Point AS-1-A westward along the latitude 13°30' S. until intersecting the U.S. EEZ boundary with Samoa, and from Point AS-1-B westward along the latitude 15°13' S. until intersecting the U.S. EEZ boundary with Samoa.

(c) *Swains Island (AS-2).* The large vessel prohibited area around Swains Island consists of the waters of the EEZ around American Samoa enclosed by straight lines connecting the following coordinates:

Point	S. lat.	W. long.
AS-2-A	11°48'	171°50'
AS-2-B	11°48'	170°20'

and from Point AS-2-A northward along the longitude 171°50' W. until

Fishery Conservation and Management

§ 665.41

intersecting the U.S. EEZ boundary with Tokelau, and from Point AS-2-B northward along the longitude 170°20' W. until intersecting the U.S. EEZ boundary with Tokelau.

[67 FR 4371, Jan. 30, 2002]

§ 665.38 Exemptions for American Samoa large vessel prohibited areas.

(a) An exemption will be issued to a person who currently owns a large vessel, to use that vessel to fish for Pacific pelagic management unit species in the American Samoa large vessel prohibited management areas, if he or she had been the owner of that vessel when it was registered for use with a Western Pacific general longline permit and made at least one landing of Pacific pelagic management unit species in American Samoa on or prior to November 13, 1997.

(b) A landing of Pacific pelagic management unit species for the purpose of this section must have been properly recorded on a NMFS Western Pacific Federal daily longline form that was submitted to NMFS, as required in § 665.14.

(c) An exemption is valid only for a vessel that was registered for use with a Western Pacific general longline permit and landed Pacific pelagic management unit species in American Samoa on or prior to November 13, 1997, or for a replacement vessel of equal or smaller LOA than the vessel that was initially registered for use with a Western Pacific general longline permit on or prior to November 13, 1997.

(d) An exemption is valid only for the vessel for which it is registered. An exemption not registered for use with a particular vessel may not be used.

(e) An exemption may not be transferred to another person.

(f) If more than one person, e.g., a partnership or corporation, owned a large vessel when it was registered for use with a Western Pacific general longline permit and made at least one landing of Pacific pelagic management unit species in American Samoa on or prior to November 13, 1997, an exemption issued under this section will be issued to only one person.

[67 FR 4371, Jan. 30, 2002, as amended at 70 FR 29657, May 24, 2005]

Subpart D—Western Pacific Crustacean Fisheries

SOURCE: 61 FR 34572, July 2, 1996, unless otherwise noted. Redesignated at 71 FR 17989, Apr. 10, 2006.

§ 665.41 Permits.

(a) *Applicability.* (1) The owner of any vessel used to fish for lobster in Permit Area 1 must have a limited access permit issued for such vessel. Only one permit will be assigned to any vessel.

(2) The owner of any vessel used to fish for lobster in Permit Area 2 or Permit Area 3, must have a permit issued for such a vessel.

(3) No vessel owner will have permits for a single vessel to harvest lobsters in Permit Areas 1 and 2 at the same time.

(4) A limited access permit is valid for fishing only in Permit Area 1.

(b) *General requirements.* General requirements governing application information, issuance, fees, expiration, replacement, transfer, alteration, display, sanctions, and appeals for permits issued under this section, as applicable, are contained in § 665.13.

(c) *Application.* An application for a permit required under this section will be submitted to the Pacific Islands Regional Office as described in § 665.13. If the application for a limited access permit is submitted on behalf of a partnership or corporation, the application must be accompanied by a supplementary information sheet obtained from the Pacific Islands Regional Office and contain the names and mailing addresses of all partners or shareholders and their respective percentage of ownership in the partnership or corporation.

(d) *Number of permits.* A maximum of 15 limited access permits can be valid at any time.

(e) *Transfer or sale of limited access permits.* (1) Permits may be transferred or sold, but no one individual, partnership, or corporation will be allowed to hold a whole or partial interest in more than one permit, except that an owner who qualifies initially for more than one permit may maintain those permits, but may not obtain additional permits. Layering of partnerships or

CIRCULAR NO. A-130

Revised, (Transmittal Memorandum No. 4)

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES SUBJECT: Management of Federal

Information Resources

1. Purpose
2. Rescissions
3. Authorities
4. Applicability and Scope
5. Background
6. Definitions
7. Basic Considerations and Assumptions
8. Policy
9. Assignment of Responsibilities
10. Oversight
11. Effectiveness
12. Inquiries
13. Sunset Review Date

Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals Appendix II, Implementation of the Government Paperwork Elimination Act Appendix III, Security of Federal Automated Information Resources Appendix IV, Analysis of Key Sections

1. **Purpose:** This Circular establishes policy for the management of Federal information resources. OMB includes procedural and analytic guidelines for implementing specific aspects of these policies as appendices.

2. **Rescissions:** This Circular rescinds OMB Memoranda M-96-20, [^]Implementation of the Information Technology Management Reform Act of 1996; [®] M-97-02, [^]Funding Information Systems Investments; [®] M-97-09, [^]Interagency Support for Information Technology; [®] M-97-15, [^]Local Telecommunications Services Policy; [®] M-97-16, "Information Technology Architectures" [®].

3. **Authorities:** OMB issues this Circular pursuant to the Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35); the Clinger-Cohen Act (also known as Information Technology Management Reform Act of 1996[®]) (Pub. L. 104-106, Division E); the Privacy Act, as amended (5 U.S.C. 552a); the Chief Financial Officers Act (31 U.S.C. 3512 et seq.); the Federal Property and Administrative Services Act, as amended (40 U.S.C. 487); the Computer Security Act of 1987 (Pub. L. 100-235); the Budget and Accounting Act, as amended (31 U.S.C. Chapter 11); the Government Performance and Results Act of 1993(GPRA); the Office of Federal Procurement Policy Act (41 U.S.C. Chapter 7); the Government Paperwork Elimination Act of 1998 (Pub. L. 105-277, Title XVII), Executive Order No. 12046 of March 27, 1978; Executive Order No. 12472 of April 3, 1984; and Executive Order No. 13011 of July 17, 1996.

4. Applicability and Scope:

- a. The policies in this Circular apply to the information activities of all agencies of the executive branch of the Federal government.
- b. Information classified for national security purposes should also be handled in accordance with the appropriate national security directives. National security emergency preparedness activities should be conducted in accordance with Executive Order No. 12472.

5. Background: The Clinger-Cohen Act supplements the information resources management policies contained in the PRA by establishing a comprehensive approach for executive agencies to improve the acquisition and management of their information resources, by:

1. focusing information resource planning to support their strategic missions;
2. implementing a capital planning and investment control process that links to budget formulation and execution; and
3. rethinking and restructuring the way they do their work before investing in information systems.

The PRA establishes a broad mandate for agencies to perform their information resources management activities in an efficient, effective, and economical manner. To assist agencies in an integrated approach to information resources management, the PRA requires that the Director of OMB develop and implement uniform and consistent information resources management policies; oversee the development and promote the use of information management principles, standards, and guidelines; evaluate agency information resources management practices in order to determine their adequacy and efficiency; and determine compliance of such practices with the policies, principles, standards, and guidelines promulgated by the Director.

6. Definitions:

- a. The term "agency" means any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the Federal government, or any independent regulatory agency. Within the Executive Office of the President, the term includes only OMB and the Office of Administration.

- b. The term "audiovisual production" means a unified presentation, developed according to a plan or script, containing visual imagery, sound or both, and used to convey information.
- c. The term "capital planning and investment control process" means a management process for ongoing identification, selection, control, and evaluation of investments in information resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes.
- d. The term "Chief Information Officers Council" (CIO Council) means the Council established in Section 3 of Executive Order 13011.
- e. The term "dissemination" means the government initiated distribution of information to the public. Not considered dissemination within the meaning of this Circular is distribution limited to government employees or agency contractors or grantees, intra- or inter-agency use or sharing of government information, and responses to requests for agency records under the Freedom of Information Act (5 U.S.C. 552) or Privacy Act.
- f. The term "executive agency" has the meaning defined in section 4(1) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(1)).
- g. The term "full costs," when applied to the expenses incurred in the operation of an information processing service organization (IPSO), is comprised of all direct, indirect, general, and administrative costs incurred in the operation of an IPSO. These costs include, but are not limited to, personnel, equipment, software, supplies, contracted services from private sector providers, space occupancy, intra-agency services from within the agency, inter-agency services from other Federal agencies, other services that are provided by State and local governments, and Judicial and Legislative branch organizations.
- h. The term "government information" means information created, collected, processed, disseminated, or disposed of by or for the Federal Government.
- i. The term "government publication" means information which is published as an individual document at government expense, or as required by law. (44 U.S.C. 1901)
- j. The term "information" means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.
- k. The term "information dissemination product" means any book, paper, map, machine-readable material, audiovisual production, or other documentary material, regardless of physical form or characteristic, disseminated by an agency to the public.
- l. The term "information life cycle" means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.
- m. The term "information management" means the planning, budgeting, manipulating, and controlling of information throughout its life cycle.
- n. The term "information resources" includes both government information and information technology.
- o. The term "information processing services organization" (IPSO) means a discrete set of personnel, information technology, and support equipment with the primary function of providing services to more than one agency on a reimbursable basis.
- p. The term "information resources management" means the process of managing information resources to accomplish agency missions. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and information technology.
- q. The term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.
- r. The term "information system life cycle" means the phases through which an information system passes, typically characterized as initiation, development, operation, and termination.
- s. The term "information technology" means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "information technology" does not include national security systems as defined in the Clinger-Cohen Act of 1996 (40 U.S.C. 1452).
- t. The term "Information Technology Resources Board" (Resources Board) means the board established by Section 5 of Executive Order 13011.
- u. The term "major information system" means an information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.
- v. The term "national security system" means any telecommunications or information system operated by the United States Government, the function, operation, or use of which (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons system; or (5) is critical to the direct fulfillment of military or intelligence missions, but excluding any system that is to be administrative and business applications (including payroll, finance, logistics, and personnel management applications). The policies and procedures established in this Circular will apply to national security systems in a manner consistent with the applicability and related limitations regarding such systems set out in Section 5141 of the Clinger-Cohen Act (Pub. L. 104-106, 40 U.S.C. 1451). Applicability of Clinger-Cohen Act to national security systems shall include budget document preparation requirements set forth in OMB Circular A-11. The resultant budget document may be classified in accordance with the provisions of Executive Order 12958.

w. The term "records" means all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of the data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included. (44 U.S.C. 3301)

x. The term "records management" means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations. (44 U.S.C. 2901(2))

y. The term "service recipient" means an agency organizational unit, programmatic entity, or chargeable account that receives information processing services from an information processing service organization (IPSO). A service recipient may be either internal or external to the organization responsible for providing information resources services, but normally does not report either to the manager or director of the IPSO or to the same immediate supervisor.

7. Basic Considerations and Assumptions:

a. The Federal Government is the largest single producer, collector, consumer, and disseminator of information in the United States. Because of the extent of the government's information activities, and the dependence of those activities upon public cooperation, the management of Federal information resources is an issue of continuing importance to all Federal agencies, State and local governments, and the public.

b. Government information is a valuable national resource. It provides the public with knowledge

of the government, society, and economy -- past, present, and future. It is a means to ensure the accountability of government, to manage the government's operations, to maintain the healthy performance of the economy, and is itself a commodity in the marketplace.

c. The free flow of information between the government and the public is essential to a democratic society. It is also essential that the government minimize the Federal paperwork burden on the public, minimize the cost of its information activities, and maximize the usefulness of government information.

d. In order to minimize the cost and maximize the usefulness of government information, the expected public and private benefits derived from government information should exceed the public and private costs of the information, recognizing that the benefits to be derived from government information may not always be quantifiable.

e. The nation can benefit from government information disseminated both by Federal agencies and by diverse nonfederal parties, including State and local government agencies, educational and other not-for-profit institutions, and for-profit organizations..

f. Because the public disclosure of government information is essential to the operation of a democracy, the management of Federal information resources should protect the public's right of access to government information.

g. The individual's right to privacy must be protected in Federal Government information activities involving personal information.

h. Systematic attention to the management of government records is an essential component of sound public resources management which ensures public accountability. Together with records preservation, it protects the government's historical record and guards the legal and financial rights of the government and the public.

i. Strategic planning improves the operation of government programs. The agency strategic plan will shape the redesign of work processes and guide the development and maintenance of an Enterprise Architecture and a capital planning and investment control process. This management approach promotes the appropriate application of Federal information resources

j. Because State and local governments are important producers of government information for many areas such as health, social welfare, labor, transportation, and education, the Federal Government must cooperate with these governments in the management of information resources.

k. The open and efficient exchange of scientific and technical government information, subject to applicable national security controls and the proprietary rights of others, fosters excellence in scientific research and effective use of Federal research and development funds.

l. Information technology is not an end in itself. It is one set of resources that can improve the effectiveness and efficiency of Federal program delivery.

m. Federal Government information resources management policies and activities can affect, and be affected by, the information policies and activities of other nations.

n. Users of Federal information resources must have skills, knowledge, and training to manage information resources, enabling the Federal government to effectively serve the public through automated means.

o. The application of up-to-date information technology presents opportunities to promote fundamental changes in agency structures, work processes, and ways of interacting with the public that improve the effectiveness and efficiency of Federal agencies.

p. The availability of government information in diverse media, including electronic formats, permits agencies and the public greater flexibility in using the information.

q. Federal managers with program delivery responsibilities should recognize the importance of information resources management to mission performance.

r. The Chief Information Officers Council and the Information Technology Resources Board will help in the development and operation of interagency and interoperable shared information resources to support the performance of government missions.

8. Policy:

a. Information Management Policy

1. How will agencies conduct Information Management Planning?

Agencies must plan in an integrated manner for managing information throughout its life cycle. Agencies will:

- (a) Consider, at each stage of the information life cycle, the effects of decisions and actions on other stages of the life cycle, particularly those concerning information dissemination;
- (b) Consider the effects of their actions on members of the public and ensure consultation with the public as appropriate;
- (c) Consider the effects of their actions on State and local governments and ensure consultation with those governments as appropriate;
- (d) Seek to satisfy new information needs through interagency or intergovernmental sharing of information, or through commercial sources, where appropriate, before creating or collecting new information;
- (e) Integrate planning for information systems with plans for resource allocation and use, including budgeting, acquisition, and use of information technology;
- (f) Train personnel in skills appropriate to management of information;
- (g) Protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information;
- (h) Use voluntary standards and Federal Information Processing Standards where appropriate or required;
- (i) Consider the effects of their actions on the privacy rights of individuals, and ensure that appropriate legal and technical safeguards are implemented;
- (j) Record, preserve, and make accessible sufficient information to ensure the management and accountability of agency programs, and to protect the legal and financial rights of the Federal Government;

(k) Incorporate records management and archival functions into the design, development, and implementation of information systems;

1. Provide for public access to records where required or appropriate.

2. What are the guidelines for Information Collection?

Agencies must collect or create only that information necessary for the proper performance of agency functions and which has practical utility.

3. What are the guidelines for Electronic Information Collection?

Executive agencies under Sections 1703 and 1705 of the Government Paperwork Elimination Act (GPEA), P. L. 105-277, Title XVII, are required to provide, by October 21, 2003, the (1) option of the electronic maintenance, submission, or disclosure of information, when practicable as a substitute for paper; and (2) use and acceptance of electronic signatures, when practicable. Agencies will follow the provisions in OMB Memorandum M-00-10, Procedures and Guidance on Implementing of the Government Paperwork Elimination Act.⁶

4. How must agencies implement Records Management? Agencies will:

- (a) Ensure that records management programs provide adequate and proper documentation of agency activities;
- (b) Ensure the ability to access records regardless of form or medium;
- (c) In a timely fashion, establish, and obtain the approval of the Archivist of the United States for retention schedules for Federal records; and
- (d) Provide training and guidance as appropriate to all agency officials and employees and contractors regarding their Federal records management responsibilities.

5. How must an agency provide information to the public?

Agencies have a responsibility to provide information to the public consistent with their missions. Agencies will discharge this responsibility by:

- (a) Providing information, as required by law, describing agency organization, activities, programs, meetings, systems of records, and other information holdings, and how the public may gain access to agency information resources;
- (b) Providing access to agency records under provisions of the Freedom of Information Act and the Privacy Act, subject to the protections and limitations provided for in these Acts;
- (c) Providing such other information as is necessary or appropriate for the proper performance of agency functions; and
- (d) In determining whether and how to disseminate information to the public, agencies will:
 - (i) Disseminate information in a manner that achieves the best balance between the goals of maximizing the usefulness of the information and minimizing the cost to the government and the public;
 - (ii) Disseminate information dissemination products on equitable and timely terms;
 - (iii) Take advantage of all dissemination channels, Federal and nonfederal, including State and local governments, libraries and

private sector entities, in discharging agency information dissemination responsibilities;

(iv) Help the public locate government information maintained by or for the agency.

6. What is an Information Dissemination Management System?

Agencies will maintain and implement a management system for all information dissemination products which must, at a minimum:

- (a) Assure that information dissemination products are necessary for proper performance of agency functions (44 U.S.C. 1108);
- (b) Consider whether an information dissemination product available from other Federal or nonfederal sources is equivalent to an agency information dissemination product and reasonably fulfills the dissemination responsibilities of the agency;
- (c) Establish and maintain inventories of all agency information dissemination products;
- (d) Develop such other aids to locating agency information dissemination products including catalogs and directories, as may reasonably achieve agency information dissemination objectives;
- (e) Identify in information dissemination products the source of the information, if from another agency;
- (f) Ensure that members of the public with disabilities whom the agency has a responsibility to inform have a reasonable ability to access the information dissemination products;
- (g) Ensure that government publications are made available to depository libraries through the facilities of the Government Printing Office, as required by law (44 U.S.C. Part 19);
- (h) Provide electronic information dissemination products to the Government Printing Office for distribution to depository libraries;
- (i) Establish and maintain communications with members of the public and with State and local governments so that the agency creates information dissemination products that meet their respective needs;
- (j) Provide adequate notice when initiating, substantially modifying, or terminating significant information dissemination products; and
- (k) Ensure that, to the extent existing information dissemination policies or practices are inconsistent with the requirements of this Circular, a prompt and orderly transition to compliance with the requirements of this Circular is made.

7. How must agencies avoid improperly restrictive practices? Agencies will:

- (a) Avoid establishing, or permitting others to establish on their behalf, exclusive, restricted, or other distribution arrangements that interfere with the availability of information dissemination products on a timely and equitable basis;
- (b) Avoid establishing restrictions or regulations, including the charging of fees or royalties, on the reuse, resale, or redissemination of Federal information dissemination products by the public; and,
- (c) Set user charges for information dissemination products at a level sufficient to recover the cost of dissemination but no higher. They must exclude from calculation of the charges costs associated with original collection and processing of the information. Exceptions to this policy are:
 - (i) Where statutory requirements are at variance with the policy;
 - (ii) Where the agency collects, processes, and disseminates the information for the benefit of a specific identifiable group beyond the benefit to the general public;
 - (iii) Where the agency plans to establish user charges at less than cost of dissemination because of a determination that higher charges would constitute a significant barrier to properly performing the agency's functions, including reaching members of the public whom the agency has a responsibility to inform; or
 - (iv) Where the Director of OMB determines an exception is warranted.

8. How will agencies carry out electronic information dissemination?

Agencies will use electronic media and formats, including public networks, as appropriate and within budgetary constraints, in order to make government information more easily accessible and useful to the public. The use of electronic media and formats for information dissemination is appropriate under the following conditions:

- (a) The agency develops and maintains the information electronically;
- (b) Electronic media or formats are practical and cost effective ways to provide public access to a large, highly detailed volume of information;
- (c) The agency disseminates the product frequently;
- (d) The agency knows a substantial portion of users have ready access to the necessary information technology and training to use electronic information dissemination products;
- (e) A change to electronic dissemination, as the sole means of disseminating the product, will not impose substantial acquisition or training costs on users, especially State and local governments and small business entities.

9. What safeguards must agencies follow? Agencies will:

- (a) Ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or

unauthorized access to or modification of such information;

(b) Limit the collection of information which identifies individuals to that which is legally authorized and necessary for the proper performance of agency functions;

(c) Limit the sharing of information that identifies individuals or contains proprietary information to that which is legally authorized, and impose appropriate conditions on use where a continuing obligation to ensure the confidentiality of the information exists;

(d) Provide individuals, upon request, access to records about them maintained in Privacy Act systems of records, and permit them to amend such records as are in error consistent with the provisions of the Privacy Act.

b. How Will Agencies Manage Information Systems and Information Technology?

(1) How will agencies use capital planning and investment control process?

Agencies must establish and maintain a capital planning and investment control process that links mission needs, information, and information technology in an effective and efficient manner. The process will guide both strategic and operational IRM, IT planning, and the Enterprise Architecture by integrating the agency's IRM plans, strategic and performance plans prepared pursuant to the Government Performance and Results Act of 1993, financial management plans prepared pursuant to the Chief Financial Officer Act of 1990 (31 U.S.C. 902a5), acquisition under the Federal Acquisition Streamlining Act of 1994, and the agency's budget formulation and execution processes. The capital planning and investment control process includes all stages of capital programming, including planning, budgeting, procurement, management, and assessment.

As outlined below, the capital planning and investment control process has three components: selection, control, and evaluation. The process must be iterative, with inputs coming from all of the agency plans and the outputs feeding into the budget and investment control processes. The goal is to link resources to results (for further guidance on Capital Planning refer to OMB Circular A-11). The agency's capital planning and investment control process must build from the agency's current Enterprise Architecture (EA) and its transition from current architecture to target architecture. The Capital Planning and Investment Control processes must be documented, and provided to OMB consistent with the budget process. The Enterprise Architecture must be documented and provided to OMB as significant changes are incorporated.

(a) What plans are associated with the capital planning and investment control process?

In the capital planning and investment control process, there are two separate and distinct plans that address IRM and IT planning requirements for the agency. The IRM Strategic Plan is strategic in nature and addresses all information resources management of the agency. Agencies must develop and maintain the agency Information Resource Management Strategic Plan (IRM) as required by 44 U.S.C. 3506 (b) (2). IRM Strategic Plans should support the agency Strategic Plan required in OMB Circular A-11, provide a description of how information resources management activities help accomplish agency missions, and ensure that IRM decisions are integrated with organizational planning, budget, procurement, financial management, human resources management, and program decisions.

The IT Capital Plan is operational in nature, supports the goals and missions identified in the IRM Strategic Plan, is a living document, and must be updated twice yearly. This IT Capital Plan is the implementation plan for the budget year. The IT Capital Plan should also reflect the goals of the agency's Annual Performance Plan, the agency's Government Paperwork Elimination Act (GPEA) Plan, the agency's EA, and agency's business planning processes. The IT Capital Plan must be submitted annually to OMB with the agency budget submission. annually. The IT Capital Plan must include the following components:

(i) A component, derived from the agency's capital planning and investment control process under OMB Circular A-11, Section 300 and the OMB Capital Programming Guide, that specifically includes all IT Capital Asset Plans for major information systems or projects. This component must also demonstrate how the agency manages its other IT investments, as required by the Clinger-Cohen Act.

(ii) A component that addresses two other sections of OMB Circular A-11: a section for Information on Financial Management, including the Report on Financial Management Activities and the Agency's Financial Management Plan, and a section entitled Information Technology, including the Agency IT Investment Portfolio.

(iii) A component, derived from the agency's capital planning and investment control process, that demonstrates the criteria it will use to select the investments into the portfolio, how it will control and manage the investments, and how it will evaluate the investments based on planned performance versus actual accomplishments.

(iv) A component that includes a summary of the security plan from the agency's five-year plan as required by the PRA and Appendix III of this Circular. The plan must demonstrate that IT projects and the EA include security controls for components, applications, and systems that are consistent with the agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality; and explain any planned or actual variance from National Institute of Standards and Technology (NIST) security guidance.

(b) What must an agency do as part of the selection component of the capital planning process? It must:

(i) Evaluate each investment in information resources to determine whether the investment will support core mission functions that must be performed by the Federal government;

(ii) Ensure that decisions to improve existing information systems or develop new information systems are initiated only when no alternative private sector or governmental source can efficiently meet the need;

(iii) Support work processes that it has simplified or otherwise redesigned to reduce costs, improve effectiveness, and make maximum use of commercial, off-the-shelf technology;

(iv) Reduce risk by avoiding or isolating custom designed components, using components that can be fully tested or prototyped prior to production, and ensuring involvement and support of users;

(v) Demonstrate a projected return on the investment that is clearly equal to or better than alternative uses of available public resources. The return may include improved mission performance in accordance with GPRA measures, reduced cost, increased quality, speed, or flexibility; as well as increased customer and employee satisfaction. The return should reflect such risk factors as the project's technical complexity, the agency's management capacity, the likelihood of cost overruns, and the consequences of under- or non-performance. Return on investment should, where appropriate, reflect actual returns observed through pilot projects and prototypes;

(vi) Prepare and update a benefit-cost analysis (BCA) for each information system throughout its life cycle. A BCA will provide a level of detail proportionate to the size of the investment, rely on systematic measures of mission performance, and be consistent with the methodology described in OMB Circular No. A-94, "Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs";

(vii) Prepare and maintain a portfolio of major information systems that monitors investments and prevents redundancy of existing or shared IT capabilities. The portfolio will provide information demonstrating the impact of alternative IT investment strategies and funding levels, identify opportunities for sharing resources, and consider the agency's inventory of information resources;

(viii) Ensure consistency with Federal, agency, and bureau Enterprise architectures, demonstrating such consistency through compliance with agency business requirements and standards, as well as identification of milestones, as defined in the EA;

(ix) Ensure that improvements to existing information systems and the development of planned information systems do not unnecessarily duplicate IT capabilities within the same agency, from other agencies, or from the private sector;

(x) Ensure that the selected system or process maximizes the usefulness of information, minimizes the burden on the public, and preserves the appropriate integrity, usability, availability, and confidentiality of information throughout the life cycle of the information, as determined in accordance with the PRA and the Federal Records Act. This portion must specifically address the planning and budgeting for the information collection burden imposed on the public as defined by 5 CFR 1320;

(xi) Establish oversight mechanisms, consistent with Appendix III of this Circular, to evaluate systematically and ensure the continuing security, interoperability, and availability of systems and their data;

(xii) Ensure that Federal information system requirements do not unnecessarily restrict the prerogatives of state, local and tribal governments;

(xiii) Ensure that the selected system or process facilitates accessibility under the Rehabilitation Act of 1973, as amended.

(c) What must an agency do as part of the control component of the capital planning process? It must:

(i) Institute performance measures and management processes that monitor actual performance compared to expected results. Agencies must use a performance based management system that provides timely information regarding the progress of an information technology investment. The system must also measure progress towards milestones in an independently verifiable basis, in terms of cost, capability of the investment to meet specified requirements, timeliness, and quality;

(ii) Establish oversight mechanisms that require periodic review of information systems to determine how mission requirements might have changed, and whether the information system continues to fulfill ongoing and anticipated mission requirements. These mechanisms must also require information regarding the future levels of performance, interoperability, and maintenance necessary to ensure the information system meets mission requirements cost effectively;

(iii) Ensure that major information systems proceed in a timely fashion towards agreed upon milestones in an information system life cycle. Information systems must also continue to deliver intended benefits to the agency and customers, meet user requirements, and identify and offer security protections;

(iv) Prepare and update a strategy that identifies and mitigates risks associated with each information system;

(iv) Ensure that financial management systems conform to the requirements of OMB Circular No. A-127, "Financial Management Systems;"

(v) Provide for the appropriate management and disposition of records in accordance with the Federal Records Act.

(vi) Ensure that agency EA procedures are being followed. This includes ensuring that EA milestones are reached and documentation is updated as needed.

(d) What must an agency do as part of the evaluation component of the capital planning process?

It must:

(i) Conduct post-implementation reviews of information systems and information resource management processes to validate estimated benefits and costs, and document effective management practices for broader use;

(ii) Evaluate systems to ensure positive return on investment and decide whether continuation, modification, or termination of the systems is necessary to meet agency mission requirements.

(iii) Document lessons learned from the post-implementation reviews. Redesign oversight mechanisms and performance levels to incorporate acquired knowledge.

(iv) Re-assess an investment's business case, technical compliance, and compliance against the EA.

(v) Update the EA and IT capital planning processes as needed. (2) The Enterprise

Architecture

Agencies must document and submit their initial EA to OMB. Agencies must submit updates when significant changes to the Enterprise Architecture occur.

(a) What is the Enterprise Architecture?

An EA is the explicit description and documentation of the current and desired relationships among business and management processes and information technology. It describes the "current architecture" and "target architecture" to include the rules and standards and systems life cycle information to optimize and maintain the environment which the agency wishes to create and maintain by managing its IT portfolio. The EA must also provide a strategy that will enable the agency to support its current state and also act as the roadmap for transition to its target environment. These transition processes will include an agency's capital planning and investment control processes, agency EA planning processes, and agency systems life cycle

methodologies. The EA will define principles and goals and set direction on such issues as the promotion of interoperability, open systems, public access, compliance with GPEA, end user satisfaction, and IT security. The agency must support the EA with a complete inventory of agency information resources, including personnel, equipment, and funds devoted to information resources management and information technology, at an appropriate level of detail. Agencies must implement the EA consistent with following principles:

- (i) Develop information systems that facilitate interoperability, application portability, and scalability of electronic applications across networks of heterogeneous hardware, software, and telecommunications platforms;
- (ii) Meet information technology needs through cost effective intra-agency and interagency sharing, before acquiring new information technology resources; and
- (iii) Establish a level of security for all information systems that is commensurate to the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access to, or modification of the information stored or flowing through these systems.

(b) How do agencies create and maintain the EA?

As part of the EA effort, agencies must use or create an Enterprise Architecture Framework. The Framework must document linkages between mission needs, information content, and information technology capabilities. The Framework must also guide both strategic and operational IRM planning.

Once a framework is established, an agency must create the EA. In the creation of an EA, agencies must identify and document:

- (i) Business Processes - Agencies must identify the work performed to support its mission, vision and performance goals. Agencies must also document change agents, such as legislation or new technologies that will drive changes in the EA.
- (ii) Information Flow and Relationships - Agencies must analyze the information utilized by the agency in its business processes, identifying the information used and the movement of the information. These information flows indicate where the information is needed and how the information is shared to support mission functions.
- (iii) Applications - Agencies must identify, define, and organize the activities that capture, manipulate, and manage the business information to support business processes. The EA also describes the logical dependencies and relationships among business activities.
- (iv) Data Descriptions and Relationships - Agencies must identify how data is created, maintained, accessed, and used. At a high level, agencies must define the data and describe the relationships among data elements used in the agency's information systems.
- (v) Technology Infrastructure - Agencies must describe and identify the functional characteristics, capabilities, and interconnections of the hardware, software, and telecommunications.

(c) What are the Technical Reference Model and Standards Profile?

The EA must also include a Technical Reference Model (TRM) and Standards Profile. (i) The TRM identifies and describes the information services (such as database, communications, intranet, etc.) used throughout the agency.

- (ii) The Standards Profile defines the set of IT standards that support the services articulated in the TRM. Agencies are expected to adopt standards necessary to support the entire EA, which must be enforced consistently throughout the agency.
- (iii) As part of the Standards Profile, agencies must create a Security Standards Profile that is specific to the security services specified in the EA and covers such services as identification, authentication, and non-repudiation; audit trail creation and analysis; access controls; cryptography management; virus protection; fraud prevention; detection and mitigation; and intrusion prevention and detection.

(3) How Will Agencies Ensure Security in Information Systems?

Agencies must incorporate security into the architecture of their information and systems to ensure that security supports agency business operations and that plans to fund and manage security are built into life-cycle budgets for information systems.

(a) To support more effective agency implementation of both agency computer security and critical infrastructure protection programs, agencies must implement the following:

- (i) Prioritize key systems (including those that are most critical to agency operations);
- (ii) Apply OMB policies and, for non-national security applications, NIST guidance to achieve adequate security commensurate with the level of risk and magnitude of harm;

(b) Agencies must make security's role explicit in information technology investments and capital programming. Investments in the development of new or the continued operation of existing information systems, both general support systems and major applications must:

- (i) Demonstrate that the security controls for components, applications, and systems are consistent with, and an integral part of, the EA of the agency;
- (ii) Demonstrate that the costs of security controls are understood and are explicitly incorporated into the life-cycle planning of the overall system in a manner consistent with OMB guidance for capital programming;
- (iii) Incorporate a security plan that complies with Appendix III of this Circular and in a manner that is consistent with NIST guidance on security planning;
- (iv) Demonstrate specific methods used to ensure that risks and the potential for loss are understood and continually assessed, that steps are taken to maintain risk at an acceptable level, and that procedures are in place to ensure that controls are implemented effectively and remain effective over time;
- (v) Demonstrate specific methods used to ensure that the security controls are commensurate with the risk and magnitude of harm that may result from the loss, misuse, or unauthorized access to or modification of the system itself or the information it manages;
- (vi) Identify additional security controls that are necessary to minimize risk to and potential loss from those systems that promote or permit public access, other externally accessible systems, and those systems that are interconnected with systems over which program officials have little or no control;

(vii) Deploy effective security controls and authentication tools consistent with the protection of privacy, such as public-key based digital signatures, for those systems that promote or permit public access;

(viii) Ensure that the handling of personal information is consistent with relevant government-wide and agency policies;

(ix) Describe each occasion the agency decides to employ standards and guidance that are more stringent than those promulgated by NIST to ensure the use of risk-based cost-effective security controls for non-national security applications;

(c) OMB will consider for new or continued funding only those system investments that satisfy these criteria. New information technology investments must demonstrate that existing agency systems also meet these criteria in order to qualify for funding.

(4) How Will Agencies Acquire Information Technology? Agencies must:

(a) Make use of adequate competition, allocate risk between government and contractor, and maximize return on investment when acquiring information technology;

(b) Structure major information systems into useful segments with a narrow scope and brief duration. This should reduce risk, promote flexibility and interoperability, increase accountability, and better match mission need with current technology and market conditions;

(c) Acquire off-the-shelf software from commercial sources, unless the cost effectiveness of developing custom software is clear and has been documented through pilot projects or prototypes; and

(d) Ensure accessibility of acquired information technology pursuant to the Rehabilitation Act of 1973, as amended (Pub. Law 105-220, 29 U.S.C.794d).

9. Assignment of Responsibilities:

a. All Federal Agencies. The head of each agency must:

1. Have primary responsibility for managing agency information resources;

2. Ensure that the agency implements appropriately all of the information policies, principles, standards, guidelines, rules, and regulations prescribed by OMB;

3. Appoint a Chief Information Officer, as required by 44 U.S.C. 3506(a), who must report directly to the agency head to carry out the responsibilities of the agencies listed in the Paperwork Reduction Act (44 U.S.C. 3506), the Clinger Cohen Act (40 U.S.C. 1425(b) & (c)), as well as Executive Order 13011. The head of the agency must consult with the Director of OMB prior to appointing a Chief Information Officer, and will advise the Director on matters regarding the authority, responsibilities, and organizational resources of the Chief Information Officer. For purposes of this paragraph, military departments and the Office of the Secretary of Defense may each appoint one official. The Chief Information Officer must, among other things:

(a) Be an active participant during all agency strategic management activities, including the development, implementation, and maintenance of agency strategic and operational plans;

(b) Advise the agency head on information resource implications of strategic planning decisions;

(c) Advise the agency head on the design, development, and implementation of information resources.

(i) Monitor and evaluate the performance of information resource investments through a capital planning and investment control process, and advise the agency head on whether to continue, modify, or terminate a program or project;

(ii) Advise the agency head on budgetary implications of information resource decisions; and

(d) Be an active participant throughout the annual agency budget process in establishing investment priorities for agency information resources;

4. Direct the Chief Information Officer to monitor agency compliance with the policies, procedures, and guidance in this Circular. Acting as an ombudsman, the Chief Information Officer must consider alleged instances of agency failure to comply with this Circular, and recommend or take appropriate corrective action. The Chief Information Officer will report instances of alleged failure and their resolution annually to the Director of OMB, by February 1 st of each year.

5. Develop internal agency information policies and procedures and oversee, evaluate, and otherwise periodically review agency information resources management activities for conformity with the policies set forth in this Circular;

6. Develop agency policies and procedures that provide for timely acquisition of required information technology;

7. Maintain the following, as required by the Paperwork Reduction Act (44 U.S.C. 3506(b)(4) and 3511) and the Freedom of Information Act (5 U.S.C. 552(g)): an inventory of the agency's major information systems, holdings, and dissemination products; an agency information locator service; a description of the agency's major information and record locator systems; an inventory of the agency's other information resources, such as personnel and funding (at the level of detail that the agency determines is most appropriate for its use in managing the agency's information resources); and a handbook for persons to obtain public information from the agency pursuant to these Acts.

8. Implement and enforce applicable records management policies and procedures, including requirements for archiving information maintained in electronic format, particularly in the planning, design and operation of information systems.

9. Identify to the Director of OMB any statutory, regulatory, and other impediments to efficient management of Federal information resources, and recommend to the Director legislation, policies, procedures, and other guidance to improve such management;

10. Assist OMB in the performance of its functions under the PRA, including making services, personnel, and facilities available to OMB for this purpose to the extent practicable;

11. Ensure that the agency:

- (a) cooperates with other agencies in the use of information technology to improve the productivity, effectiveness, and efficiency of Federal programs;
- (b) promotes a coordinated, interoperable, secure, and shared government wide infrastructure that is provided and supported by a diversity of private sector suppliers; and
- (c) develops a well-trained corps of information resource professionals.

12. Use the guidance provided in OMB Circular A-11, "Planning, Budgeting, and Acquisition of Fixed Assets," to promote effective and efficient capital planning within the organization;

13. Ensure that the agency provides budget data pertaining to information resources to OMB, consistent with the requirements of OMB Circular A-11,

14. Ensure, to the extent reasonable, that in the design of information systems with the purpose of disseminating information to the public, an index of information disseminated by the system will be included in the directory created by the Superintendent of Documents pursuant to 41 U.S.C. 4101. (Nothing in this paragraph authorizes the dissemination of information to the public unless otherwise authorized.)

15. Permit, to the extent practicable, the use of one agency's contract by another agency or the award of multi-agency contracts, provided the action is within the scope of the contract and consistent with OMB guidance; and

16. As designated by the Director of OMB, act as executive agent for the government-wide acquisition of information technology.

b. Department of State. The Secretary of State must:

1. Advise the Director of OMB on the development of United States positions and policies on international information policy and technology issues affecting Federal government activities and the development of international information technology standards; and

2. Be responsible for liaison, consultation, and negotiation with foreign governments and intergovernmental organizations on all matters related to information resources management, including federal information technology. The Secretary must also ensure, in consultation with the Secretary of Commerce, that the United States is represented in the development of international standards and recommendations affecting information technology. These responsibilities may also require the Secretary to consult, as appropriate, with affected domestic agencies, organizations, and other members of the public.

c. Department of Commerce. The Secretary of Commerce must:

1. Develop and issue Federal Information Processing Standards and guidelines necessary to ensure the efficient and effective acquisition, management, security, and use of information technology, while taking into consideration the recommendations of the agencies and the CIO Council;

2. Advise the Director of OMB on the development of policies relating to the procurement and management of Federal telecommunications resources;

3. Provide OMB and the agencies with scientific and technical advisory services relating to the development and use of information technology;

4. Conduct studies and evaluations concerning telecommunications technology, and concerning the improvement, expansion, testing, operation, and use of Federal telecommunications systems, and advise the Director of OMB and appropriate agencies of the recommendations that result from such studies;

5. Develop, in consultation with the Secretary of State and the Director of OMB, plans, policies, and programs relating to international telecommunications issues affecting government information activities;

6. Identify needs for standardization of telecommunications and information processing technology, and develop standards, in consultation with the Secretary of Defense and the Administrator of General Services, to ensure efficient application of such technology;

7. Ensure that the Federal Government is represented in the development of national and, in consultation with the Secretary of State, international information technology standards, and advise the Director of OMB on such activities.

d. Department of Defense. The Secretary of Defense will develop, in consultation with the Administrator of General Services, uniform Federal telecommunications standards and guidelines to ensure national security, emergency preparedness, and continuity of government.

e. General Services Administration. The Administrator of General Services must:

1. Continue to manage the FTS2001 program and coordinate the follow-up to that program, on behalf of and with the advice of agencies;

2. Develop, maintain, and disseminate for the use of the Federal community (as requested by OMB or the agencies) recommended methods and strategies for the development and acquisition of information technology;

3. Conduct and manage outreach programs in cooperation with agency managers;

4. Be a liaison on information resources management (including Federal information technology) with State and local governments. GSA must also be a liaison with nongovernmental international organizations, subject to prior consultation with the Secretary of State to ensure consistency with the overall United States foreign policy objectives;

5. Support the activities of the Secretary of State for liaison, consultation, and negotiation with intergovernmental organizations on information resource management matters;

6. Provide support and assistance to the CIO Council and the Information Technology Resources Board.

7. Manage the Information Technology Fund in accordance with the Federal Property and Administrative Services Act, as amended;

f. Office of Personnel Management. The Director, Office of Personnel Management, will:

1. Develop and conduct training programs for Federal personnel on information resources management, including end-user computing;
2. Evaluate periodically future personnel management and staffing requirements for Federal information resources management;
3. Establish personnel security policies and develop training programs for Federal personnel associated with the design, operation, or maintenance of information systems.

g. National Archives and Records Administration. The Archivist of the United States will:

1. Administer the Federal records management program in accordance with the National Archives and Records Act;
2. Assist the Director of OMB in developing standards and guidelines relating to the records management program.

h. Office of Management and Budget. The Director of the Office of Management and Budget will:

1. Provide overall leadership and coordination of Federal information resources management within the executive branch;
2. Serve as the President's principal adviser on procurement and management of Federal telecommunications systems, and develop and establish policies for procurement and management of such systems;
3. Issue policies, procedures, and guidelines to assist agencies in achieving integrated, effective, and efficient information resources management;
4. Initiate and review proposals for changes in legislation, regulations, and agency procedures to improve Federal information resources management;
5. Review and approve or disapprove agency proposals for collection of information from the public, as defined by 5 CFR 1320.3;
6. Develop and maintain a Governmentwide strategic plan for information resources management.
7. Evaluate agencies' information resources management and identify cross-cutting information policy issues through the review of agency information programs, information collection budgets, information technology acquisition plans, fiscal budgets, and by other means;
8. Provide policy oversight for the Federal records management function conducted by the National Archives and Records Administration, coordinate records management policies and programs with other information activities, and review compliance by agencies with records management requirements;
9. Review agencies' policies, practices, and programs pertaining to the security, protection, sharing, and disclosure of information, in order to ensure compliance, with respect to privacy and security, with the Privacy Act, the Freedom of Information Act, the Computer Security Act, the GPEA, and related statutes;
10. Review proposed U. S. Government Position and Policy statements on international issues affecting Federal Government information activities, and advise the Secretary of State as to their consistency with Federal information resources management policy.
11. Coordinate the development and review by the Office of Information and Regulatory Affairs of policy associated with Federal procurement and acquisition of information technology with the Office of Federal Procurement Policy, and policies regarding management of financial management systems with the Office of Federal Financial Management.
12. Evaluate agency information resources management practices and programs and, as part of the budget process, oversee agency capital planning and investment control processes to analyze, track, and evaluate the risks and results of major capital investments in information systems;
13. Notify an agency if OMB believes that a major information system project requires outside assistance;
14. Provide guidance on the implementation of the Clinger-Cohen Act and on the management of information resources to the executive agencies, to the CIO Council, and to the Information Technology Resources Board; and
15. Designate one or more heads of executive agencies as executive agent for governmentwide acquisitions of information technology.

10. Oversight:

- a. The Director of OMB will use information technology planning reviews, fiscal budget reviews, information collection budget reviews, management reviews, and such other measures as the Director deems necessary to evaluate the adequacy and efficiency of each agency's information resources management and compliance with this Circular.
 - b. The Director of OMB may, consistent with statute and upon written request of an agency, grant a waiver from particular requirements of this Circular. Requests for waivers must detail the reasons why a particular waiver is sought, identify the duration of the waiver sought, and include a plan for the prompt and orderly transition to full compliance with the requirements of this Circular. Notice of each waiver request must be published promptly by the agency in the Federal Register, with a copy of the waiver request made available to the public on request.
11. **Effectiveness:** This Circular is effective upon issuance. Nothing in this Circular will be construed to confer a private right of action on any person.
 12. **Inquiries:** All questions or inquiries should be addressed to the Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, D.C. 20503. Telephone: (202) 395-3785.
 13. **Sunset Review Date:** OMB will review this Circular three years from the date of issuance to ascertain its effectiveness.

COMPUTER SECURITY ACT OF 1987
Public Law 100-235 (H.R. 145)
January 8, 1988

SECTION 1. SHORT TITLE

The Act may be cited as the "Computer Security Act of 1987".

SEC. 2 PURPOSE

(a) IN GENERAL.--The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use.

(b) SPECIFIC PURPOSES.--The purposes of this Act are--

(1) by amending the Act of March 3, 1901, to assign to the National Bureau of Standards responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate;

(2) to provide for promulgation of such standards and guidelines by amending section 111(d) of the Federal Property and Administrative Services Act of 1949;

(3) to require establishment of security plans by all operators of Federal computer systems that contain sensitive information; and

(4) to require mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information.

SEC. 3. ESTABLISHMENT OF COMPUTER STANDARDS PROGRAM.

The Act of March 3, 1901, (15 U.S.C. 271-278h), is amended--

(1) in section 2(f), by striking out "and" at the end of paragraph (18), by striking out the period at the end of paragraph (19) and inserting in lieu thereof: "; and", and by inserting after such paragraph the following:

"(20) the study of computer systems (as that term is defined in section 20(d) of this Act) and their use to control machinery and processes.";

(2) by redesignating section 20 as section 22, and by inserting after section 19 the following new sections: "SEC. 20. (a) The National Bureau of Standards shall--

"(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems;

"(2) except as described in paragraph (3) of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code.

"(3) have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except--

"(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code; and

"(B) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy,

The primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer-related fraud and misuse;

"(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under

section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1987; and

"(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to paragraphs (1), (2), and (3) of this subsection through research and liaison with other government and private agencies.

"(b) In fulfilling subsection (a) of this section, the National Bureau of Standards is authorized--

"(1) to assist the private sector, upon request, in using and applying the results of the programs and activities under this section;

"(2) to make recommendations, as appropriate, to the Administrator of General Services on policies and regulations proposed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(3) as requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(4) to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1987;

"(5) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to devise techniques for the cost effective security and privacy of sensitive information in Federal computer systems; and

"(6) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget)--

"(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

"(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a) (3) and (5) are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

"(c) For the purposes of--

"(1) developing standards and guidelines for the protection of sensitive information in Federal computer systems under subsections (a) (1) and (a) (3) , and

"(2) performing research and conducting studies under subsection (b)(5), the National Bureau of Standards shall draw upon computer system technical security guidelines developed by the National Security Agency to the extent that the National Bureau of Standards determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

"(d) As used in this section--

"(1) the term computer system'--

"(A) means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and

"(B) includes--

" (i) computers;

"(ii) ancillary equipment;

"(iii) software, firmware, and similar procedures;

"(iv) services, including support services; and

"(v) related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and

Administrative Services Act of 1949;

"(2) the term 'Federal computer system'--

"(A) means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function; and

"(B) includes automatic data processing equipment as that term is defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949;

"(3) the term 'operator of a Federal computer system' means a Federal agency, contractor of a Federal agency, or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal function;

"(4) the term 'sensitive information' means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; and

"(5) the term 'Federal agency' has the meaning given such term by section 3(b) of the Federal Property and Administrative Services Act of 1949.

"SEC. 21. (a) There is hereby established a Computer System Security and Privacy Advisory Board within the Department of Commerce. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:

"(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industries;

"(2) four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

"(3) four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

"(b) The duties of the Board shall be--

"(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy;

"(2) to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and

"(3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate Committees of the Congress.

"(c) The term of office of each member of the Board shall be four years, except that--

"(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

"(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

"(d) The Board shall not act in the absence of a quorum, which shall consist of seven members.

"(e) Members of the Board, other than full-time employees of the Federal Government while attending meetings of such committees or while otherwise performing duties at the request of the Board Chairman while away from their homes or a regular place of business, may be allowed travel expenses in accordance with subchapter I of chapter 57 of title 5, United States Code.

"(f) To provide the staff services necessary to assist the Board in carrying out its

functions, the Board may utilize personnel from the National Bureau of Standards or any other agency of the Federal Government with the consent of the head of the agency.

"(g) As used in this section, the terms 'computer system' and 'Federal computer system' have the meanings given in section 20(d) of this Act."; and

"(3) by adding at the end thereof the following new section:

"SEC. 23. This Act may be cited as the National Bureau of Standards Act."

SEC. 4 AMENDMENT TO BROOKS ACT.

Section 111(d) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759(d)) is amended to read as follows:

"(d)(1) The Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Bureau of Standards pursuant to section 20(a) (2) and (3) of the National Bureau of Standards Act, promulgate standards and guidelines pertaining to Federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to improve the efficiency of operation or security and privacy of Federal computer systems. The President may disapprove or modify such standards and guidelines if he determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may not be delegated. Notice of such disapproval or modification shall be submitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President.

"(2) The head of a Federal agency may employ standards for the cost effective security and privacy of sensitive information in a Federal computer system within or under the supervision of that agency that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

"(3) The standards determined to be compulsory and binding may be waived by the Secretary of Commerce in writing upon a determination that compliance would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or cause a major adverse financial impact on the operator which is not offset by government-wide savings. The Secretary may delegate to the head of one or more Federal agencies authority to waive such standards to the extent to which the Secretary determines such action to be necessary and desirable to allow for timely and effect implementation of Federal computer systems standards. The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of title 44, United States Code. Notice of each such waiver and delegation shall be transmitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register.

"(4) The Administrator shall revise the Federal information resources management regulations (41 CFR ch. 201) to be consistent with the standards and guidelines promulgated by the Secretary of Commerce under this subsection.

"(5) As used in this subsection, the terms 'Federal computer system' and 'operator of a Federal computer system' have the meanings given in section 20(d) of the National Bureau of Standards Act."

SEC. 5. FEDERAL COMPUTER SYSTEM SECURITY TRAINING.

(a) In General.--Each Federal agency shall 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 each Federal computer system within or under the supervision of that agency. Such training shall be--

(1) provided in accordance with the guidelines developed pursuant to section 20(a)(5) of the National Bureau of Standards Act (as added by section 3 of this Act), and in accordance with the regulations issued under subsection (c) of this section for Federal civilian employees; or

(2) provided by an alternative training program approved by the head of that agency on the basis of a determination that the alternative training program is at least as effective in accomplishing the objectives of such guidelines and regulations.

(b) TRAINING OBJECTIVES.--Training under this section shall be started within 60 days after the issuance of the regulations described in subsection (c). Such training

shall be designed--

(1) to enhance employees' awareness of the threats to and vulnerability of computer systems; and

(2) to encourage the use of improved computer security practices.

(c) REGULATIONS.--Within six months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall issue regulations prescribing the procedures and scope of the training to be provided Federal civilian employees under subsection (a) and the manner in which such training is to be carried out.

SEC. 6. ADDITIONAL RESPONSIBILITIES FOR COMPUTER SYSTEMS SECURITY AND PRIVACY.

(a) IDENTIFICATION OF SYSTEMS THAT CONTAIN SENSITIVE INFORMATION Within 6 months after the date of enactment of this Act, each Federal agency shall identify each Federal computer system, and system under development, which is within or under the supervision of that agency and which contains sensitive information.

(b) SECURITY PLAN.--Within one year after the date of enactment of this Act, each such agency shall, consistent with the standards, guidelines, policies, and regulations prescribed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949, establish a plan for the security and privacy of each Federal computer system identified by that agency pursuant to subsection (a) that is commensurate with the risk and magnitude or the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system. Copies of each such plan shall be transmitted to the National Bureau of Standards and the National Security Agency for advice and comment. A summary of such plan shall be included in the agency's five-year plan required by section 3505 of title 44, United States Code. Such plan shall be subject to disapproval by the Director of the Office of Management and Budget. Such plan shall be revised annually as necessary.

SEC. 7. DEFINITIONS.

As used in this Act, the terms "computer system", "Federal computer system", "operator of a Federal computer system", "sensitive information", and "Federal agency" have the meanings given in section 20(d) of the National Bureau of Standards Act (as added by section 3 of this Act).

SEC. 8. RULES OF CONSTRUCTION OF ACT.

Nothing in this Act, or in any amendment made by this Act, shall be construed--

(1) to constitute authority to withhold information sought pursuant to section 552 of title 5, United States Code; or

(2) to authorize any Federal agency to limit, restrict, regulate, or control the collection, maintenance, disclosure, use, transfer, or sale of any information (regardless of the medium in which the information may be maintained) that is--

(A) privately-owned information;

(B) disclosable under section 552 of title 5, United States Code, or other law requiring or authorizing the public disclosure of information; or

(C) public domain information.

Subtitle G—Government Information Security Reform

SEC. 1061. COORDINATION OF FEDERAL INFORMATION POLICY.

Chapter 35 of title 44, United States Code, is amended by inserting at the end the following new subchapter:

SUBCHAPTER II—INFORMATION SECURITY

§ 3531. Purposes

The purposes of this subchapter are the following:

- (1) To provide a comprehensive framework for establishing and ensuring the effectiveness of controls over information resources that support Federal operations and assets.
- (2)(A) To recognize the highly networked nature of the Federal computing environment including the need for Federal Government interoperability and, in the implementation of improved security management measures, assure that opportunities for interoperability are not adversely affected.
- (B) To provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities.
- “(3) To provide for development and maintenance of minimum controls required to protect Federal information and information systems.
- “(4) To provide a mechanism for improved oversight of Federal agency information security programs.

§ 3532. Definitions

- “(a) Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.
- “(b) In this subchapter:
- “(1) The term ‘information technology’ has the meaning given that term in section 5002 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401).
 - “(2) The term ‘mission critical system’ means any telecommunications or information system used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, that—
 - “(A) is defined as a national security system under section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452);
 - “(B) is protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be classified in the interest of national defense or foreign policy; or
 - “(C) processes any information, the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency.

§ 3533. Authority and functions of the Director

- (a)(1) The Director shall establish governmentwide policies for the management of programs that—
- “(A) support the cost-effective security of Federal information systems by promoting security as an integral component of each agency’s business operations; and
 - “(B) include information technology architectures as defined under section 5125 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1425).
- (2) Policies under this subsection shall—
- (A) be founded on a continuing risk management cycle that recognizes the need to—
 - “(i) identify, assess, and understand risk; and
 - “(ii) determine security needs commensurate with the level of risk;
 - (B) implement controls that adequately address the risk;
 - (C) promote continuing awareness of information security risk; and
 - (D) continually monitor and evaluate policy and control effectiveness of information security practices.
- (b) The authority under subsection (a) includes the authority to—
- (1) oversee and develop policies, principles, standards, and guidelines for the handling of Federal information and information resources to improve the efficiency and effectiveness of governmental operations, including principles, policies, and guidelines for the implementation of agency responsibilities under applicable law for ensuring the privacy, confidentiality, and security of Federal information;
 - (2) consistent with the standards and guidelines promulgated under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441) and sections 5 and 6 of the Computer Security Act of 1987 (40 U.S.C. 1441 note; Public Law 100–235; 101 Stat. 1729), require Federal agencies to identify and afford security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency;
 - (3) direct the heads of agencies to—
 - “(A) identify, use, and share best security practices;
 - “(B) develop an agencywide information security plan;
 - “(C) incorporate information security principles and practices throughout the life cycles of the agency’s information systems; and
 - “(D) ensure that the agency’s information security plan is practiced throughout all life cycles of

- the agency's information systems;
- (4) oversee the development and implementation of standards and guidelines relating to security controls for Federal computer systems by the Secretary of Commerce through the National Institute of Standards and Technology under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441) and section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3);
- (5) oversee and coordinate compliance with this section in a manner consistent with—
 - “(A) sections 552 and 552a of title 5;
 - “(B) sections 20 and 21 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3 and 278g-4);
 - “(C) section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);
 - “(D) sections 5 and 6 of the Computer Security Act of 1987 (40 U.S.C. 1441 note; Public Law 100-235; 101 Stat. 1729); and
 - “(E) related information management laws; and
- (6) take any authorized action under section 5113(b)(5) of the Clinger-Cohen Act of 1996 (40 U.S.C. 1413(b)(5)) that the Director considers appropriate, including any action involving the budgetary process or appropriations management process, to enforce accountability of the head of an agency for information resources management, including the requirements of this subchapter, and for the investments made by the agency in information technology, including—
 - “(A) recommending a reduction or an increase in any amount for information resources that the head of the agency proposes for the budget submitted to Congress under section 1105(a) of title 31;
 - “(B) reducing or otherwise adjusting apportionments and reapportionments of appropriations for information resources; and
 - “(C) using other authorized administrative controls over appropriations to restrict the availability of funds for information resources.
- (c) The authorities of the Director under this section (other than the authority described in subsection (b)(6))—
 - “(1) shall be delegated to the Secretary of Defense, the Director of Central Intelligence, and another agency head as designated by the President in the case of systems described under subparagraphs (A) and (B) of section 3532(b)(2);
 - “(2) shall be delegated to the Secretary of Defense in the case of systems described under subparagraph (C) of section 3532(b)(2) that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense; and
 - “(3) in the case of all other Federal information systems, may be delegated only to the Deputy Director for Management of the Office of Management and Budget.

§ 3534. Federal agency responsibilities

- (a) The head of each agency shall—
 - (1) be responsible for—
 - “(A) adequately ensuring the integrity, confidentiality, authenticity, availability, and nonrepudiation of information and information systems supporting agency operations and assets;
 - “(B) developing and implementing information security policies, procedures, and control techniques sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by or for the agency; and
 - “(C) ensuring that the agency's information security plan is practiced throughout the life cycle of each agency system;
 - (2) ensure that appropriate senior agency officials are responsible for—
 - “(A) assessing the information security risks associated with the operations and assets for programs and systems over which such officials have control;
 - “(B) determining the levels of information security appropriate to protect such operations and assets; and
 - “(C) periodically testing and evaluating information security controls and techniques;
 - (3) delegate to the agency Chief Information Officer established under section 3506, or a comparable official in an agency not covered by such section, the authority to administer all functions under this subchapter including—
 - “(A) designating a senior agency information security official who shall report to the Chief Information Officer or a comparable official;
 - “(B) developing and maintaining an agencywide information security program as required under subsection (b);
 - “(C) ensuring that the agency effectively implements and maintains information security policies, procedures, and control techniques;
 - “(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and
 - “(E) assisting senior agency officials concerning responsibilities under paragraph (2);
 - (4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and
 - (5) ensure that the agency Chief Information Officer, in coordination with senior agency officials, periodically—
 - (A)(i) evaluates the effectiveness of the agency information security program, including testing control techniques; and
 - (ii) implements appropriate remedial actions based on that evaluation; and
 - (B) reports to the agency head on—
 - “(i) the results of such tests and evaluations; and

“(ii) the progress of remedial actions.

(b)(1) Each agency shall develop and implement an agencywide information security program to provide information security for the operations and assets of the agency, including operations and assets provided or managed by another agency.

(2) Each program under this subsection shall include—

(A) periodic risk assessments that consider internal and external threats to—

“(i) the integrity, confidentiality, and availability of systems; and

“(ii) data supporting critical operations and assets;

(B) policies and procedures that—

“(i) are based on the risk assessments required under subparagraph (A) that cost-effectively reduce information security risks to an acceptable level; and

“(ii) ensure compliance with—

“(I) the requirements of this subchapter;

“(II) policies and procedures as may be prescribed by the Director; and

(III) any other applicable requirements;

(C) security awareness training to inform personnel of—

“(i) information security risks associated with the activities of personnel; and

“(ii) responsibilities of personnel in complying with agency policies and procedures designed to reduce such risks;

(D) periodic management testing and evaluation of the

effectiveness of information security policies and procedures;

(E) a process for ensuring remedial action to address any significant deficiencies; and

(F) procedures for detecting, reporting, and responding to security incidents, including—

“(i) mitigating risks associated with such incidents before substantial damage occurs;

“(ii) notifying and consulting with law enforcement officials and other offices and authorities;

“(iii) notifying and consulting with an office designated by the Administrator of General Services within the General Services Administration; and

“(iv) notifying and consulting with an office designated by the Secretary of Defense, the Director of Central Intelligence, and another agency head as designated by the President for incidents involving systems described under subparagraphs (A) and (B) of section 3532(b)(2).

(3) Each program under this subsection is subject to the approval of the Director and is required to be reviewed at least annually by agency program officials in consultation with the Chief Information Officer. In the case of systems described under subparagraphs (A) and (B) of section 3532(b)(2), the Director shall delegate approval authority under this paragraph to the Secretary of Defense, the Director of Central Intelligence, and another agency head as designated by the President.

(c)(1) Each agency shall examine the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to—

“(A) annual agency budgets;

“(B) information resources management under subchapter I of this chapter;

“(C) performance and results based management under the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.);

“(D) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 through 2805 of title 39; and

“(E) financial management under—

“(i) chapter 9 of title 31, United States Code, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101-576) (and the amendments made by that Act);

“(ii) the Federal Financial Management Improvement Act of 1996 (31 U.S.C. 3512 note) (and the amendments made by that Act); and

“(iii) the internal controls conducted under section 3512 of title 31.

(2) Any significant deficiency in a policy, procedure, or practice identified under paragraph (1) shall be reported as a material weakness in reporting required under the applicable provision of law under paragraph (1).

(d)(1) In addition to the requirements of subsection (c), each agency, in consultation with the Chief Information Officer, shall include as part of the performance plan required under section 1115 of title 31 a description of—

“(A) the time periods; and

“(B) the resources, including budget, staffing, and training, which are necessary to implement the program required under subsection (b)(1).

(2) The description under paragraph (1) shall be based on the risk assessment required under subsection (b)(2)(A).

§ 3535. Annual independent evaluation

(a)(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency.

(2) Each evaluation by an agency under this section shall include—

“(A) testing of the effectiveness of information security control techniques for an appropriate subset of the agency’s information systems; and

“(B) an assessment (made on the basis of the results of the testing) of the compliance with—

“(i) the requirements of this subchapter; and

- “(ii) re late d in formation security po licies, proce dures, standards, and guidelines.
- (3) The Inspector General or the independent evaluator performing an evaluation under this section may use an audit, evaluation, or report relating to programs or practices of the applicable agency.
- (b)(1)(A) Subject to subparagraph (B), for agencies with Inspectors General appointed under the Inspector General Act of 1978 (5 U.S.C. App.) or any other law, the annual evaluation required under this section or, in the case of systems described under subparagraphs (A) and (B) of section 3532(b)(2), an audit of the annual evaluation required under this section, shall be performed by the Inspector General or by an independent evaluator, as determined by the Inspector General of the agency.
 - (B) For systems described under subparagraphs (A) and (B) of section 3532(b)(2), the evaluation required under this section shall be performed only by an entity designated by the Secretary of Defense, the Director of Central Intelligence, or another agency head as designated by the President.
- (2) For any agency to which paragraph (1) does not apply, the head of the agency shall contract with an independent evaluator to perform the evaluation.
- (c) Each year, not later than the anniversary of the date of the enactment of this subchapter, the applicable agency head shall submit to the Director—
 - “(1) the results of each evaluation required under this section, other than an evaluation of a system described under subparagraph (A) or (B) of section 3532(b)(2); and
 - “(2) the results of each audit of an evaluation required under this section of a system described under subparagraph (A) or (B) of section 3532(b)(2).
- (d)(1) The Director shall submit to Congress each year a report summarizing the materials received from agencies pursuant to subsection (c) in that year.
 - (2) Evaluations and audits of evaluations of systems under the authority and control of the Director of Central Intelligence and evaluations and audits of evaluation of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available only to the appropriate oversight committees of Congress, in accordance with applicable laws.
- (e) Agencies and evaluators shall take appropriate actions to ensure the protection of information, the disclosure of which may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws.

§ 3536. Expiration

This subchapter shall not be in effect after the date that is two years after the date on which this subchapter takes effect..

SEC. 1062. RESPONSIBILITIES OF CERTAIN AGENCIES.

- (a) DEPARTMENT OF COMMERCE.—Notwithstanding section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and except as provided under subsection (b), the Secretary of Commerce, through the National Institute of Standards and Technology and with technical assistance from the National Security Agency, as required or when requested, shall—
 - (1) develop, issue, review, and update standards and guidance for the security of Federal information systems, including development of methods and techniques for security systems and validation programs;
 - (2) develop, issue, review, and update guidelines for training in computer security awareness and accepted computer security practices, with assistance from the Office of Personnel Management;
 - (3) provide agencies with guidance for security planning to assist in the development of applications and system security plans for such agencies;
 - (4) provide guidance and assistance to agencies concerning cost-effective controls when interconnecting with other systems; and
 - (5) evaluate information technologies to assess security vulnerabilities and alert Federal agencies of such vulnerabilities as soon as those vulnerabilities are known.
- (b) DEPARTMENT OF DEFENSE AND THE INTELLIGENCE COMMUNITY.—
 - (1) IN GENERAL.—Notwithstanding any other provision of this subtitle (including any amendment made by this subtitle)—
 - (A) the Secretary of Defense, the Director of Central Intelligence, and another agency head as designated by the President, shall, consistent with their respective authorities—
 - (i) develop and issue information security policies, standards, and guidelines for systems described under subparagraphs (A) and (B) of section 3532(b)(2) of title 44, United States Code (as added by section 1061 of this Act), that provide more stringent protection, to the maximum extent practicable, than the policies, principles, standards, and guidelines required under section 3533 of such title (as added by such section 1061); and
 - (ii) ensure the implementation of the information security policies, principles, standards, and guidelines described under clause (i); and
 - (B) the Secretary of Defense shall, consistent with his authority—
 - (i) develop and issue information security policies, standards, and guidelines for systems described under subparagraph (C) of section 3532(b)(2) of title 44, United States Code (as added by section 1061 of this Act), that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that provide more stringent protection, to the maximum extent practicable, than the policies, principles, standards, and guidelines required under section 3533 of such title (as added by such section 1061); and
 - (ii) ensure the implementation of the information security policies, principles, standards, and guidelines described under clause (i).
 - (2) MEASURES ADDRESSED.—The policies, principles, standards, and guidelines developed by the Secretary of Defense and the Director of Central Intelligence under paragraph (1) shall address the full range of information assurance measures needed to protect and defend Federal information and information systems by ensuring their integrity, confidentiality, authenticity, availability, and nonrepudiation.

- (c) DEPARTMENT OF JUSTICE.—The Attorney General shall review and update guidance to agencies on—
 - (1) legal remedies regarding security incidents and ways to report to and work with law enforcement agencies concerning such incidents; and
 - (2) lawful uses of security techniques and technologies.
- (d) GENERAL SERVICES ADMINISTRATION.—The Administrator of General Services shall—
 - (1) review and update General Services Administration guidance to agencies on addressing security considerations when acquiring information technology; and
 - (2) assist agencies in—
 - (A) fulfilling agency responsibilities under section 3534(b)(2)(F) of title 44, United States Code (as added by section 1061 of this Act); and
 - (B) the acquisition of cost-effective security products, services, and incident response capabilities.
- (e) OFFICE OF PERSONNEL MANAGEMENT.—The Director of the Office of Personnel Management shall—
 - (1) review and update Office of Personnel Management regulations concerning computer security training for Federal civilian employees;
 - (2) assist the Department of Commerce in updating and maintaining guidelines for training in computer security awareness and computer security best practices; and
 - (3) work with the National Science Foundation and other agencies on personnel and training initiatives (including scholarships and fellowships, as authorized by law) as necessary to ensure that the Federal Government—
 - (A) has adequate sources of continuing information security education and training available for employees; and
 - (B) has an adequate supply of qualified information security professionals to meet agency needs.
- (f) INFORMATION SECURITY POLICIES, PRINCIPLES, STANDARDS, AND GUIDELINES.—
 - (1) ADOPTION OF POLICIES, PRINCIPLES, STANDARDS, AND GUIDELINES OF OTHER AGENCIES.—

The policies, principles, standards, and guidelines developed under subsection (b) by the Secretary of Defense, the Director of Central Intelligence, and another agency head as designated by the President may be adopted, to the extent that such policies are consistent with policies and guidance developed by the Director of the Office of Management and Budget and the Secretary of Commerce—

 - (A) by the Director of the Office of Management and Budget, as appropriate, for application to the mission critical systems of all agencies; or
 - (B) by an agency head, as appropriate, for application to the mission critical systems of that agency.
 - (2) DEVELOPMENT OF MORE STRINGENT POLICIES, PRINCIPLES, STANDARDS, AND GUIDELINES.—

To the extent that such policies are consistent with policies and guidance developed by the Director of the Office of Management and Budget and the Secretary of Commerce, an agency may develop and implement information security policies, principles, standards, and guidelines that provide more stringent protection than those required under section 3533 of title 44, United States Code (as added by section 1061 of this Act), or subsection (a) of this section.
 - (g) ATOMIC ENERGY ACT OF 1954.—Nothing in this subtitle (including any amendment made by this subtitle) shall supersede any requirement made by, or under, the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.). Restricted Data or Formerly Restricted Data shall be handled, protected, classified, downgraded, and declassified in conformity with the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.).

SEC. 1063. RELATIONSHIP OF DEFENSE INFORMATION ASSURANCE PROGRAM TO GOVERNMENT-WIDE INFORMATION SECURITY PROGRAM.

- (a) CONSISTENCY OF REQUIREMENTS.—Subsection (b) of section 2224 of title 10, United States Code, is amended—
 - (1) by striking (b) OBJECTIVES OF THE PROGRAM.— and inserting (b) OBJECTIVES AND MINIMUM REQUIREMENTS.—(1);
 - and
 - (2) by adding at the end the following:
 - (2) The program shall at a minimum meet the requirements of sections 3534 and 3535 of title 44..
 - (b) ADDITION TO ANNUAL REPORT.—Subsection (e) of such section is amended by adding at the end the following new paragraph:
 - (7) A summary of the actions taken in the administration of sections 3534 and 3535 of title 44 within the Department of Defense..

SEC. 1064. TECHNICAL AND CONFORMING AMENDMENTS.

- (a) TABLE OF SECTIONS.—Chapter 35 of title 44, United States Code, is amended—
 - (1) in the table of sections—
 - (A) by inserting after the chapter heading the following:

SUBCHAPTER I—FEDERAL INFORMATION POLICY;

and

(B) by inserting after the item relating to section 3520 the following:

SUBCHAPTER II—INFORMATION SECURITY

Sec.
 3531. Purposes.
 3532. Definitions.
 3533. Authority and functions of the Director. 3534. Federal agency responsibilities.
 3535. Annual independent evaluation. 3536. Expiration.;

and

(2) by inserting before section 3501 the following:

SUBCHAPTER I—FEDERAL INFORMATION POLICY.

(b) REFERENCES TO CHAPTER 35.—Sections 3501 through 3520 of title 44, United States Code, are amended by striking chapter each place it appears and inserting subchapter, except in section 3507(i)(1) of such title.

SEC. 1065. EFFECTIVE DATE.

This subtitle and the amendments made by this subtitle shall take effect 30 days after the date of the enactment of this Act.

NIST Special Publication 800-53
Revision 2

Recommended Security Controls for Federal Information Systems

NIST

**National Institute of
Standards and Technology**

U.S. Department of Commerce

Ron Ross
Stu Katzke
Arnold Johnson
Marianne Swanson
Gary Stoneburner
George Rogers

I N F O R M A T I O N S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

December 2007



U.S. Department of Commerce

Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology

James M. Turner, Acting Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Authority

This document has been developed by the National Institute of Standards and Technology (NIST) to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, P.L. 107-347. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

NIST Special Publication 800-53, Revision 2, 188 pages

(December 2007)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There are references in this publication to documents currently under development by NIST in accordance with responsibilities assigned to NIST under the Federal Information Security Management Act of 2002. The methodologies in this document may be used even before the completion of such companion documents. Thus, until such time as each document is completed, current requirements, guidelines, and procedures (where they exist) remain operative. For planning and transition purposes, agencies may wish to closely follow the development of these new documents by NIST. Individuals are also encouraged to review the public draft documents and offer their comments to NIST. All NIST documents mentioned in this publication, other than the ones noted above, are available at <http://csrc.nist.gov/publications>.

Comments may be submitted to the Computer Security Division, Information Technology Laboratory, NIST via electronic mail at sec-cert@nist.gov or via regular mail at 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Compliance with NIST Standards and Guidelines

NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act (FISMA) of 2002 and in managing cost-effective programs to protect their information and information systems.

- Federal Information Processing Standards (FIPS) are developed by NIST in accordance with FISMA. FIPS are approved by the Secretary of Commerce and are compulsory and binding for federal agencies. Since FISMA requires that federal agencies comply with these standards, agencies may not waive their use.
- Guidance documents and recommendations are issued in the NIST Special Publication (SP) 800-series. Office of Management and Budget (OMB) policies (including OMB FISMA Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management) state that for other than national security programs and systems, agencies must follow NIST guidance.¹
- Other security-related publications, including interagency and internal reports (NISTIRs), and ITL Bulletins, provide technical and other information about NIST's activities. These publications are mandatory only when so specified by OMB.

Schedule for Compliance with NIST Standards and Guidelines

- For legacy information systems, agencies are expected to be in compliance with NIST security standards and guidelines within one year of the publication date unless otherwise directed by OMB or NIST.²
- For information systems under development, agencies are expected to be in compliance with NIST security standards and guidelines immediately upon deployment of the system.

¹ While agencies are required to follow NIST guidance in accordance with OMB policy, there is flexibility within NIST's guidance in how agencies apply the guidance. Unless otherwise specified by OMB, the 800-series guidance documents published by NIST generally allow agencies some latitude in their application. Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of *adequate security* for federal information systems. When assessing agency compliance with NIST guidance, auditors, evaluators, and/or assessors should consider the intent of the security concepts and principles articulated within the particular guidance document and how the agency applied the guidance in the context of its specific mission responsibilities, operational environments, and unique organizational conditions.

² The one-year compliance date for revisions to NIST Special Publications applies only to the new and/or updated material in the publications resulting from the periodic revision process. Agencies are expected to be in compliance with previous versions of NIST Special Publications within one year of the publication date of the previous versions.

Acknowledgments

The authors, Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner, and George Rogers, wish to thank their colleagues who reviewed drafts of this document and contributed to its development. A special note of thanks goes to Peggy Himes and Elizabeth Lennon for their superb technical editing and administrative support, to Murugiah Souppaya and the NIST information security operations group for their review of the security controls and insightful recommendations, and to Annabelle Lee for her contribution to earlier versions of the document. The authors also gratefully acknowledge and appreciate the many contributions from individuals in the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

A special acknowledgment is also given to the participants in the *Industrial Control System (ICS) Security Project* who have put forth significant effort in helping to augment the security controls in NIST Special Publication 800-53 for industrial controls systems. These participants include: Keith Stouffer (NIST), Stu Katzke (NIST), and Marshall Abrams (Mitre Corporation) from the ICS Security Project Development Team; federal agencies participating in the ICS workshops; and individuals and organizations from the public and private sector ICS community providing thoughtful and insightful comments on the proposed augmentations.

FEDERAL INFORMATION SECURITY MANAGEMENT ACT

IMPLEMENTING SECURITY STANDARDS AND GUIDELINES

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, is a mandatory, non-waiverable standard developed in response to the Federal Information Security Management Act of 2002. To comply with the federal standard, agencies must first determine the security category of their information system in accordance with the provisions of FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and then apply the appropriate set of baseline security controls in NIST Special Publication 800-53 (as amended), *Recommended Security Controls for Federal Information Systems*. Agencies have flexibility in applying the baseline security controls in accordance with the tailoring guidance provided in Special Publication 800-53. This allows agencies to adjust the security controls to more closely fit their mission requirements and operational environments.

The combination of FIPS 200 and NIST Special Publication 800-53 requires a foundational level of security for all federal information and information systems. The agency's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, or the Nation. The resulting set of security controls establishes a level of "security due diligence" for the federal agency and its contractors.

In addition to the security requirements established by FISMA, there may also be specific security requirements in different business areas within agencies that are governed by other laws, Executive Orders, directives, policies, regulations, or associated governing documents, (e.g., the Health Insurance Portability and Accountability Act of 1996, the Federal Financial Management Improvement Act of 1996, or OMB Circular A-127 on Financial Management Systems). These requirements may not be equivalent to the security requirements and implementing security controls required by FISMA or may enhance or further refine the security requirements and security controls. It is important that agency officials (including authorizing officials, chief information officers, senior agency information security officers, information system owners, information system security officers, and acquisition authorities) take steps to ensure that: (i) all appropriate security requirements are addressed in agency acquisitions of information systems and information system services; and (ii) all required security controls are implemented in agency information systems. See <http://csrc.nist.gov/sec-cert/ca-compliance.html> for additional information on FISMA compliance.

DEVELOPING COMMON INFORMATION SECURITY FOUNDATIONS

COLLABORATION AMONG PUBLIC AND PRIVATE SECTOR ENTITIES

In developing standards and guidelines required by the Federal Information Security Management Act (FISMA), NIST consults with other federal agencies and offices as well as the private sector to improve information security, avoid unnecessary and costly duplication of effort, and ensure that NIST standards and guidelines are complementary with standards and guidelines employed for the protection of national security systems. In addition to its comprehensive public review and vetting process, NIST is working with the Office of the Director of National Intelligence (ODNI), the Department of Defense (DOD), and the Committee on National Security Systems (CNSS) to establish a common foundation for information security across the federal government. The common foundation for information security will provide the Intelligence, Defense, and Civil sectors of the federal government and their support contractors, more uniform and consistent ways to manage the risk to organizational operations, organizational assets, individuals, other organizations, and the Nation from the operation and use of information systems. NIST is also working with public and private sector entities to establish specific mappings and relationships between the security standards and guidelines developed by NIST in the FISMA Implementation Project and the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27000-series standards.

Table of Contents

CHAPTER ONE INTRODUCTION	1
1.1 PURPOSE AND APPLICABILITY	2
1.2 TARGET AUDIENCE.....	3
1.3 RELATIONSHIP TO OTHER SECURITY CONTROL PUBLICATIONS.....	3
1.4 ORGANIZATIONAL RESPONSIBILITIES	4
1.5 ORGANIZATION OF THIS SPECIAL PUBLICATION.....	5
CHAPTER TWO THE FUNDAMENTALS	6
2.1 SECURITY CONTROL ORGANIZATION AND STRUCTURE	6
2.2 SECURITY CONTROL BASELINES.....	8
2.3 COMMON SECURITY CONTROLS	9
2.4 SECURITY CONTROLS IN EXTERNAL ENVIRONMENTS.....	11
2.5 SECURITY CONTROL ASSURANCE.....	13
2.6 REVISIONS AND EXTENSIONS	14
CHAPTER THREE THE PROCESS	15
3.1 MANAGING RISK	15
3.2 SECURITY CATEGORIZATION	17
3.3 SELECTING AND TAILORING THE INITIAL BASELINE	18
3.4 SUPPLEMENTING THE TAILORED BASELINE	21
3.5 UPDATING SECURITY CONTROLS	23
APPENDIX A REFERENCES	A-1
APPENDIX B GLOSSARY	B-1
APPENDIX C ACRONYMS	C-1
APPENDIX D MINIMUM SECURITY CONTROLS – SUMMARY	D-1
APPENDIX E MINIMUM ASSURANCE REQUIREMENTS	E-1
APPENDIX F SECURITY CONTROL CATALOG	F-1
APPENDIX G SECURITY CONTROL MAPPINGS	G-1
APPENDIX H STANDARDS AND GUIDANCE MAPPINGS	H-1
APPENDIX I INDUSTRIAL CONTROL SYSTEMS	I-1

CHAPTER ONE

INTRODUCTION

THE NEED FOR SECURITY CONTROLS TO PROTECT INFORMATION SYSTEMS

The selection and employment of appropriate *security controls* for an information system³ are important tasks that can have major implications on the operations⁴ and assets of an organization as well as the welfare of individuals. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. There are several important questions that should be answered by organizational officials when addressing the security considerations for their information systems:

- What security controls are needed to adequately protect the information systems that support the operations and assets of the organization in order for that organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals?
- Have the selected security controls been implemented or is there a realistic plan for their implementation?
- What is the desired or required level of assurance (i.e., grounds for confidence) that the selected security controls, as implemented, are effective⁵ in their application?

The answers to these questions are not given in isolation but rather in the context of an effective *information security program* for the organization that identifies, controls, and mitigates risks to its information and information systems.⁶ The security controls defined in Special Publication 800-53 (as amended) and recommended for use by organizations in protecting their information systems should be employed in conjunction with and as part of a well-defined and documented information security program. An effective information security program should include:

- Periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization;
- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level and address information security throughout the life cycle of each organizational information system;

³ An information system is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems such as industrial/process controls systems, telephone switching/private branch exchange (PBX) systems, and environmental control systems.

⁴ Organizational operations include mission, functions, image, and reputation.

⁵ Security control effectiveness addresses the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment.

⁶ The E-Government Act (P.L. 107-347), passed by the one hundred and seventh Congress and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for organizations to develop, document, and implement an organization-wide program to provide security for the information systems that support its operations and assets.

- Plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;
- Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks;
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;
- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization;
- Procedures for detecting, reporting, and responding to security incidents; and
- Plans and procedures for continuity of operations for information systems that support the operations and assets of the organization.

It is of paramount importance that responsible officials within the organization understand the risks and other factors that could adversely affect organizational operations, organizational assets, or individuals. Moreover, these officials must understand the current status of their security programs and the security controls planned or in place to protect their information systems in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level. The ultimate objective is to conduct the day-to-day operations of the organization and to accomplish the organization's stated mission(s) with what the Office of Management and Budget (OMB) Circular A-130 defines as *adequate security*, or security commensurate with risk, including the magnitude of harm to individuals, the organization, or its assets resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. The guidelines apply to all components⁷ of an information system that process, store, or transmit federal information. The guidelines have been developed to help achieve more secure information systems within the federal government by:

- Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems;
- Providing a recommendation for minimum security controls for information systems categorized in accordance with Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*;

⁷ Information system components include, but are not limited to, mainframes, servers, workstations, network components, operating systems, middleware, and applications. Network components can include, for example, such devices as firewalls, sensors (local or remote), switches, guards, routers, gateways, wireless access points, and network appliances. Servers can include, for example, database servers, authentication servers, electronic mail and web servers, proxy servers, domain name servers, and network time servers. Information system components are either purchased commercially off-the-shelf or are custom-developed and can be deployed in land-based, sea-based, airborne, and/or space-based information systems.

- Providing a stable, yet flexible catalog of security controls for information systems to meet current organizational protection needs and the demands of future protection needs based on changing requirements and technologies; and
- Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness.

The guidelines provided in this special publication are applicable to all federal information systems⁸ other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542.⁹ The guidelines have been broadly developed from a technical perspective to complement similar guidelines for national security systems. This publication is intended to provide guidance to federal agencies implementing FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. In addition to the agencies of the federal government, state, local, and tribal governments, and private sector organizations that compose the critical infrastructure of the United States, are encouraged to use these guidelines, as appropriate.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse federal audience of information system and information security professionals including: (i) individuals with information system and information security management and oversight responsibilities (e.g., chief information officers, senior agency information security officers, and authorizing officials); (ii) individuals with information system development responsibilities (e.g., program and project managers, mission/application owners, system designers, system and application programmers); (iii) individuals with information security implementation and operational responsibilities (e.g., information system owners, information owners, information system administrators, information system security officers,); and (iv) individuals with information system and information security assessment and monitoring responsibilities (e.g., auditors, inspectors general, evaluators, and certification agents). Commercial companies producing information technology products and systems, creating information security-related technologies, and providing information security services can also benefit from the information in this publication.

1.3 RELATIONSHIP TO OTHER SECURITY CONTROL PUBLICATIONS

To create the most technically sound and broadly applicable set of security controls for information systems, a variety of sources were considered during the development of this special publication. The sources included security controls from the defense, audit, financial, healthcare, and intelligence communities as well as controls defined by national and international standards organizations.¹⁰ The objective of NIST Special Publication 800-53 is to provide a set of security

⁸ A federal information system is an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

⁹ NIST Special Publication 800-59 provides guidance on identifying an information system as a national security system.

¹⁰ Security controls from the audit, defense, healthcare, intelligence, and standards communities are contained in the following publications: (i) Government Accountability Office, *Federal Information System Controls Audit Manual*; (ii) Department of Defense Instruction 8500.2, *Information Assurance Implementation*; (iii) Department of Health and Human Services Centers for Medicare and Medicaid Services, *Core Security Requirements*; (iv) Director of Central Intelligence Directive 6/3 Manual, *Protecting Sensitive Compartmented Information within Information Systems*; (v) NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*; and (vi) International Organization for Standardization/International Electrotechnical Commission 17799:2005, *Code of Practice for Information Security Management*.

controls that is sufficiently rich to satisfy the breadth and depth of security requirements¹¹ levied on information systems and that is consistent with and complementary to other established security standards.

The catalog of security controls provided in Special Publication 800-53 can be effectively used to demonstrate compliance with a variety of governmental, organizational, or institutional security requirements. It is the responsibility of organizations to select the appropriate security controls, to implement the controls correctly, and to demonstrate the effectiveness of the controls in satisfying their stated security requirements. The security controls in the catalog facilitate the development of assessment methods and procedures that can be used to demonstrate control effectiveness in a consistent and repeatable manner—thus contributing to the organization's confidence that there is ongoing compliance with its stated security requirements.¹²

1.4 ORGANIZATIONAL RESPONSIBILITIES

Organizations¹³ should use FIPS 199 to define security categories for their information systems. This publication associates recommended minimum security controls with FIPS 199 low-impact, moderate-impact, and high-impact security categories. For each information system, the recommendation for minimum security controls from Special Publication 800-53 (i.e., the baseline security controls defined in Appendix D, tailored in accordance with the tailoring guidance in Section 3.3) is intended to be used as a starting point for and input to the organization's risk assessment process.¹⁴ The risk assessment results are used to supplement the tailored baseline resulting in a set of agreed-upon controls documented in the security plan for the information system. While the FIPS 199 security categorization associates the operation of the information system with the potential impact on an organization's operations, assets, or individuals, the incorporation of refined threat and vulnerability information during the risk assessment facilitates supplementing the tailored baseline security controls to address organizational needs and tolerance for risk. The final, agreed-upon set of security controls should be documented with appropriate rationale in the security plan for the information system.¹⁵

The use of security controls from Special Publication 800-53 and the incorporation of tailored baseline controls as a starting point in the control selection process, facilitates a more consistent level of security across federal information systems. It also offers the needed flexibility to

¹¹ Security requirements are those requirements levied on an information system that are derived from laws, Executive Orders, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

¹² NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Second Public Draft), April 2006, provides guidance on assessment methods and procedures for security controls defined in this publication. Special Publication 800-53A can also be used to conduct self-assessments of information systems.

¹³ An organization typically exercises direct managerial, operational, and/or financial control over its information systems and the security provided to those systems, including the authority and capability to implement the appropriate security controls necessary to protect organizational operations, organizational assets, and individuals.

¹⁴ Risk assessments can be accomplished in a variety of ways depending on the specific needs of the organization. The assessment of risk is a process that should be incorporated into the system development life cycle. NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, provides guidance on the assessment and mitigation of risk as part of an overall risk management process.

¹⁵ NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*, provides guidance on documenting information system security controls. The general guidance in Special Publication 800-18 is augmented by Special Publication 800-53 with recommendations for information and rationale to be included in the system security plan.

appropriately modify the controls based on specific organizational policy and requirements, particular conditions and circumstances, known threat and vulnerability information, and tolerance for risk to the organization's operations, assets, or to individuals.

Building a more secure information system is a multifaceted undertaking that involves the use of: (i) well-defined system-level security requirements and security specifications; (ii) well-designed information technology products; (iii) sound systems/security engineering principles and practices to effectively integrate information technology products into the information system; (iv) appropriate methods for product/system testing and evaluation; and (v) comprehensive system security planning and life cycle management.¹⁶ From a systems engineering viewpoint, security is just one of many required capabilities for an organizational information system—capabilities that must be funded by the organization throughout the life cycle of the system. Realistically assessing the risks to an organization's operations and assets or to individuals by placing the information system into operation or continuing its operation is of utmost importance. Addressing the information system security requirements must be accomplished with full consideration of the risk tolerance of the organization in light of the potential impacts, cost, schedule, and performance issues associated with the acquisition, deployment, and operation of the system.

1.5 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the fundamental concepts associated with security control selection and specification including: (i) the structural components of security controls and how the controls are organized into families; (ii) minimum (baseline) security controls; (iii) the use of common security controls in support of organization-wide information security programs; (iv) security controls in external environments; (v) assurance in the effectiveness of security controls; and (vi) the commitment to maintain currency of the individual security controls and the control baselines.
- **Chapter Three** describes the process of selecting and specifying security controls for an information system including: (i) defining the organization's overall approach to managing risk; (ii) categorizing the system in accordance with FIPS 199; (iii) selecting and tailoring the initial set of minimum (baseline) security controls; (iv) supplementing the tailored security control baseline, as necessary, based upon risk assessment results; and (v) updating the controls as part of a comprehensive continuous monitoring process.
- **Supporting appendices** provide more detailed security control selection and specification-related information including: (i) general references; (ii) definitions and terms; (iii) acronyms; (iv) baseline security controls for low-impact, moderate-impact, and high-impact information systems; (v) minimum assurance requirements; (vi) a master catalog of security controls; (vii) mapping tables relating the security controls in this publication to other standards and control sets; (viii) crosswalks of NIST security standards and guidelines with associated security controls; and (ix) guidance on the application of security controls to industrial control systems.

¹⁶ Successful life cycle management depends on having qualified personnel to oversee and manage the information systems within an organization. The skills and knowledge of organizational personnel with information systems (and information security) responsibilities should be carefully evaluated (e.g., through performance, certification, etc.).

NIST Special Publication 800-53A

NIST

**National Institute of
Standards and Technology**

U.S. Department of Commerce

Guide for Assessing the Security Controls in Federal Information Systems

Building Effective Security Assessment Plans

Ron Ross
Arnold Johnson
Stu Katzke
Patricia Toth
Gary Stoneburner
George Rogers

I N F O R M A T I O N S E C U R I T Y

FINAL PUBLIC DRAFT

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

December 2007



U.S. Department of Commerce

Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology

James M. Turner, Acting Director

Notes to Reviewers

The final public draft of NIST Special Publication 800-53A contains some important changes to improve the efficiency and effectiveness of the document in supporting individuals and organizations conducting assessments of security controls in federal information systems. These changes have been driven by the extensive comments from the public and private sectors during the last public comment period. There were significant differences of opinion from the public respondents regarding preferences for the greater specificity in assessment procedures offered in the second public draft or the greater flexibility in assessment procedures offered in the third public draft. There were compelling arguments made for both approaches.

To address the needs of all of our customers, NIST chose to use a modified third public draft format to define the general assessment procedures for the security controls in NIST Special Publication 800-53, thus preserving the flexibility desired by organizations in creating their individualized security assessment plans. To address the concerns of those organizations that desired a greater level of specificity and a checklist approach in the assessment procedures, NIST initiated the *Assessment Case Development Project*, an inter-agency task force of experienced assessors, who are developing specific exemplary assessment cases for the assessment procedures in NIST Special Publication 800-53A. The assessment cases, described in Appendix J of this publication, provide an assessor's view of cost-effective and efficient techniques and methods for carrying out the more generic assessment procedures in Special Publication 800-53A to satisfy the stated assessment objectives. The assessment cases also address the level of effort expended in an assessment through the use of specific depth and coverage values incorporated into the assessment cases for security controls in low-, moderate-, and high-impact information systems.

The Assessment Case Development Project deliverables (i.e., the completed assessment cases) will be posted on the NIST web site as they are completed beginning in January 2008 and culminating in March 2008 with the final publication of Special Publication 800-53A. The assessment cases will *not* be part of this publication and will *not* be mandatory for use by federal agencies. Rather, assessment cases offer the opportunity for a community-wide effort to provide worked examples of assessor actions and activities that more cost-effectively address the assessment of security controls and provide a web-based delivery mechanism to get state-of-the-practice assessment information to assessors.

In addition to the assessment case initiative described above, the final public draft includes:

- Updated assessment procedures based on NIST Special Publication 800-53, Revision 2, (including industrial control system information);
- A reorganization and streamlining of the material in the Chapters One, Two, and Three to provide greater clarity in describing the components of an assessment procedure and how the components are used within the context of a security assessment plan;
- Minor modifications to the assessment method definitions in Appendix D;
- A streamlined assessment procedure format in Appendix F for expressing assessment objectives, assessment methods, and assessment objects;
- A specific assignment of (L) (M) (H) designators to assessment methods to indicate applicability to low-impact, moderate-impact, and high-impact information systems, respectively; and
- Relocating the Risk Management Framework to NIST Special Publication 800-39 (Initial Public Draft), *Managing Risk from Information Systems: An Organizational Perspective*.

Comments on this public draft will be accepted through **January 31, 2008**. Comments should be forwarded to the Computer Security Division, Information Technology Laboratory at NIST or submitted via email to sec-cert@nist.gov. The FISMA Implementation Project main website at <http://csrc.nist.gov/sec-cert> contains information on all of the FISMA-related security standards and guidelines and how the publications can be used to manage risk from information systems and build comprehensive information security programs.

-- RON ROSS
PROJECT LEADER, FISMA IMPLEMENTATION PROJECT

Draft

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Draft

Authority

This document has been developed by the National Institute of Standards and Technology (NIST) to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, P.L. 107-347. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in Circular A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by federal agencies. However, it may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

NIST Special Publication 800-53A, 396 pages

(December 2007) CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

THE PUBLIC COMMENT PERIOD FOR THIS DOCUMENT IS DECEMBER 20, 2007 TO JANUARY 31, 2008.
COMMENTS MAY BE SUBMITTED TO THE COMPUTER SECURITY DIVISION, INFORMATION TECHNOLOGY
LABORATORY, NIST VIA ELECTRONIC MAIL AT SEC-CERT@NIST.GOV OR VIA REGULAR MAIL AT
100 BUREAU DRIVE (MAIL STOP 8930) GAITHERSBURG, MD 20899-8930

Compliance with NIST Standards and Guidelines

NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act (FISMA) of 2002 and in managing cost-effective programs to protect their information and information systems.

- Federal Information Processing Standards (FIPS) are developed by NIST in accordance with FISMA. FIPS are approved by the Secretary of Commerce and are compulsory and binding for federal agencies. Since FISMA requires that federal agencies comply with these standards, agencies may not waive their use.
- Guidance documents and recommendations are issued in the NIST Special Publication (SP) 800-series. Office of Management and Budget (OMB) policies (including OMB FISMA Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management) state that for other than national security programs and systems, agencies must follow NIST guidance.¹
- Other security-related publications, including interagency and internal reports (NISTIRs) and ITL Bulletins, provide technical and other information about NIST's activities. These publications are mandatory only when so specified by OMB.

Schedule for Compliance with NIST Standards and Guidelines

- For legacy information systems, agencies are expected to be in compliance with NIST security standards and guidelines within one year of the publication date unless otherwise directed by OMB or NIST.²
- For information systems under development, agencies are expected to be in compliance with NIST security standards and guidelines immediately upon deployment of the system.

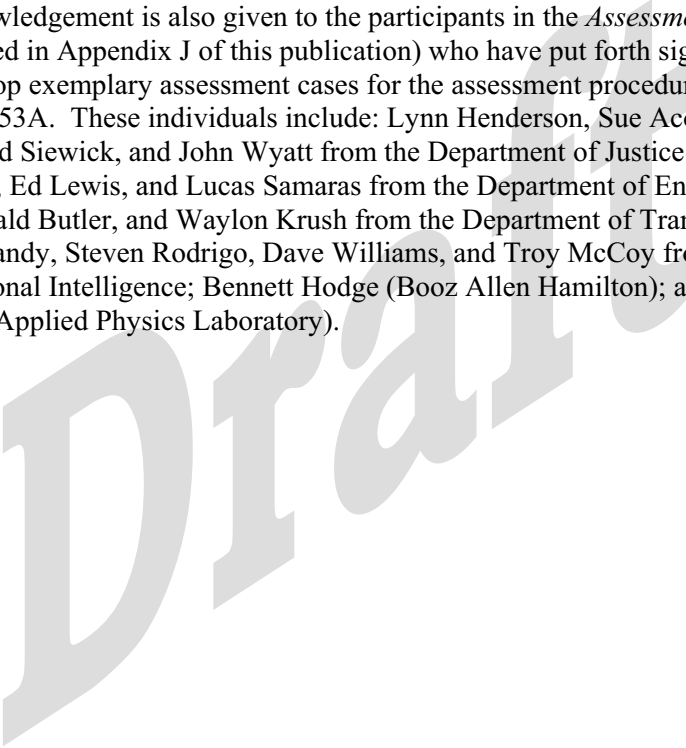
¹ While agencies are required to follow NIST guidance in accordance with OMB policy, there is flexibility within NIST's guidance in how agencies apply the guidance. Unless otherwise specified by OMB, the 800-series guidance documents published by NIST generally allow agencies some latitude in their application. Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of *adequate security* for federal information systems. When assessing agency compliance with NIST guidance, auditors, evaluators, and/or assessors should consider the intent of the security concepts and principles articulated within the particular guidance document and how the agency applied the guidance in the context of its specific mission responsibilities, operational environments, and unique organizational conditions.

² The one-year compliance date for revisions to NIST Special Publications applies only to the new and/or updated material in the publications resulting from the periodic revision process. Agencies are expected to be in compliance with previous versions of NIST Special Publications within one year of the publication date of the previous versions.

Acknowledgements

The authors, Ron Ross, Arnold Johnson, Stu Katzke, Patricia Toth, Gary Stoneburner, and George Rogers, wish to thank their colleagues who reviewed drafts of this document and contributed to its development. A special note of thanks is also extended to Peggy Himes and Elizabeth Lennon for their superb technical editing and administrative support. The authors also gratefully acknowledge and appreciate the many contributions from individuals in the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

A special acknowledgement is also given to the participants in the *Assessment Case Development Project* (described in Appendix J of this publication) who have put forth significant effort in helping to develop exemplary assessment cases for the assessment procedures in NIST Special Publication 800-53A. These individuals include: Lynn Henderson, Sue Acosta, Peter Crichlow, Ryan Higgins, Ed Siewick, and John Wyatt from the Department of Justice; Tony Bailey, Ja’Nelle Devore, Ed Lewis, and Lucas Samaras from the Department of Energy; Arvid Knutsen, Jim Harrell, Gerald Butler, and Waylon Krush from the Department of Transportation; Sharon Ehlers, Mike Grandy, Steven Rodrigo, Dave Williams, and Troy McCoy from the Office of the Director of National Intelligence; Bennett Hodge (Booz Allen Hamilton); and Gary Stoneburner (Johns Hopkins Applied Physics Laboratory).



FEDERAL INFORMATION SECURITY MANAGEMENT ACT

IMPLEMENTING SECURITY STANDARDS AND GUIDELINES

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, is a mandatory, non-waiverable standard developed in response to the Federal Information Security Management Act of 2002. To comply with the federal standard, agencies must first determine the security category of their information system in accordance with the provisions of FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and then apply the appropriate set of baseline security controls in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*. Agencies have flexibility in applying the baseline security controls in accordance with the tailoring guidance provided in Special Publication 800-53. This allows agencies to adjust the security controls to more closely fit their mission requirements and operational environments.

The combination of FIPS 200 and NIST Special Publication 800-53 requires a foundational level of security for all federal information and information systems (other than national security information and information systems). The agency's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, or the Nation. The resulting set of security controls establishes a level of "security due diligence" for the federal agency and its contractors.

In addition to the security requirements established by FISMA, there may also be specific security requirements in different business areas within agencies that are governed by other laws, Executive Orders, directives, policies, regulations, or associated governing documents, (e.g., the Health Insurance Portability and Accountability Act of 1996, the Federal Financial Management Improvement Act of 1996, or OMB Circular A-127 on Financial Management Systems). These requirements may not be equivalent to the security requirements and implementing security controls required by FISMA or may enhance or further refine the security requirements and security controls. It is important that agency officials (including authorizing officials, chief information officers, senior agency information security officers, information system owners, information system security officers, and acquisition authorities) take steps to ensure that: (i) all appropriate security requirements are addressed in agency acquisitions of information systems and information system services; and (ii) all required security controls are implemented in agency information systems. See <http://csrc.nist.gov/sec-cert/ca-compliance.html> for additional information on FISMA compliance.

DEVELOPING COMMON INFORMATION SECURITY FOUNDATIONS

COLLABORATION AMONG PUBLIC AND PRIVATE SECTOR ENTITIES

In developing standards and guidelines required by the Federal Information Security Management Act (FISMA), NIST consults with other federal agencies and offices as well as the private sector to improve information security, avoid unnecessary and costly duplication of effort, and ensure that NIST standards and guidelines are complementary with standards and guidelines employed for the protection of national security systems. In addition to its comprehensive public review and vetting process, NIST is working with the Office of the Director of National Intelligence (ODNI), the Department of Defense (DOD), and the Committee on National Security Systems (CNSS) to establish a common foundation for information security across the federal government. The common foundation for information security will provide the Intelligence, Defense, and Civil sectors of the federal government and their support contractors, more uniform and consistent ways to manage the risk to organizational operations, organizational assets, individuals, other organizations, and the Nation that results from the operation and use of information systems. In another collaboration initiative, NIST is working with public and private sector entities to establish specific mappings and relationships between the security standards and guidelines developed by NIST and the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27001, Information Security Management System (ISMS).

Draft

Preface

Security control assessments are not about checklists, simple pass-fail results, or generating paperwork to pass inspections or audits—rather, security controls assessments are the principal vehicle used to verify that the implementers and operators of information systems are meeting their stated security goals and objectives. NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, is written to facilitate security control assessments conducted within an effective risk management framework. The assessment results provide key organizational officials:

- Evidence about the effectiveness of the security controls in the organizational information system;
- An indication of the quality of the risk management processes employed within the organization; and
- Information about the strengths and weaknesses of an organization's information system which is supporting critical federal applications and missions in a global environment of sophisticated threats.

The findings produced by assessors are used primarily in determining the overall effectiveness of the security controls in an information system and in providing credible and meaningful inputs to the organization's security accreditation (information system authorization) process. A well-executed assessment helps to determine the validity of the security controls contained in the information system security plan (and subsequently employed in the information system) and to facilitate a cost-effective approach to correcting any deficiencies in the system in an orderly and disciplined manner consistent with the organization's mission requirements.

NIST Special Publication 800-53A is a companion guideline to NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*. Each publication provides guidance for implementing the steps in the NIST Risk Management Framework. Special Publication 800-53 covers the steps in the Risk Management Framework that address security control selection and supplementation (i.e., determining what security controls are needed to protect organizational operations and assets, individuals, other organizations, and the Nation) in accordance with the security requirements stated in FIPS 200.³ This includes: (i) selecting an initial set of baseline security controls based on a FIPS 199 impact analysis;⁴ (ii) tailoring the baseline controls; and (iii) supplementing the controls, as necessary, based on an organizational assessment of risk. Special Publication 800-53A covers both the security control assessment and continuous monitoring steps in the Risk Management Framework and provides guidance on the security assessment process. This guidance includes how to build effective security assessment plans and how to manage assessment results.

NIST Special Publication 800-53A has been developed with the intention of enabling organizations to tailor and supplement the basic assessment procedures provided. The concepts of tailoring and supplementation used in this document are similar to the concepts described in NIST Special Publication 800-53. Tailoring involves scoping the assessment procedures to match the characteristics of the information system under assessment. The tailoring process provides organizations with the flexibility needed to avoid overly constrained assessment approaches. Supplementation involves adding assessment procedures or assessment details to

³ FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*.

⁴ FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*.

adequately meet the organization's risk management needs (e.g., adding assessment objectives or adding organization-specific details such as system and platform-specific information for selected security controls employed in the hardware, software, and firmware). Supplementation decisions are left to the discretion of the organization in order to maximize flexibility in developing security assessment plans when applying the results of risk assessments in determining the extent, rigor, and level of intensity of the assessments.

While flexibility continues to be an important factor in developing security assessment plans, consistency of assessments is also an important consideration. A major design objective for NIST Special Publication 800-53A is to provide an assessment framework and initial starting point for assessment procedures that are essential for achieving such consistency. In addition to the assessment framework and initial starting point for assessment procedures, NIST initiated the *Assessment Case Development Project*. The purpose of the project is threefold: (i) to actively engage experienced assessors from multiple organizations in the development of exemplary sets of assessment cases corresponding to the assessment procedures in Special Publication 800-53A; (ii) to provide organizations and the assessors supporting those organizations with an exemplary set of assessment cases for each assessment procedure in the catalog of procedures in this publication; and (iii) to provide a vehicle for ongoing community-wide review and comment of the assessment cases to promote continuous improvement in the assessment process for more consistent, cost-effective security assessments of federal information systems. The Assessment Case Development Project is described in Appendix J.

In addition to the above project, NIST also initiated the Information Security Automation Program (ISAP) and Security Content Automation Protocol (SCAP) that support and complement the approach for achieving consistent, cost-effective security control assessments outlined in this publication. The primary purpose of the ISAP/SCAP is to improve the automated application, verification, and reporting of commercial information technology product-specific security configuration settings, thereby reducing vulnerabilities when products are not configured properly. The ultimate objective is to achieve a direct linkage, where appropriate, of the assessment procedures found in NIST Special Publication 800-53A to the SCAP automated testing of information system mechanisms and associated security configuration settings.⁵

Finally, it should be noted that for environments with credible threat information indicating sophisticated, well-resourced threat agents and possible attacks against high-value targets, additional assurances may be required. NIST Special Publication 800-53 indicates the need for explicit risk acceptance or additional assurances for moderate-impact and high-impact information systems whenever the organization is relying on one or more security controls to mitigate risks from more capable threat sources. In a similar manner, NIST Special Publication 800-53A recognizes that, for such controls, additional organizationally-derived assessment activities will likely be required. These additional assessment activities will include the assessment objectives associated with verifying the *Additional Requirements Enhancing Moderate-impact and High-impact Information Systems* in Appendix E of NIST Special Publication 800-53—that is, the security controls in the information system are developed in a manner that supports a high degree of confidence the controls are complete, consistent, and correct, resulting in a greater degree of trustworthiness and penetration resistance of the system.

⁵ SCAP will help in achieving test results that are more uniform and repeatable, automated test procedures that are more transparent, and greater efficiency for assessment teams. Additional details on the ISAP/SCAP initiative, as well as freely available SCAP reference data, can be found at the NIST website at <http://nvd.nist.gov>.

CAUTIONARY NOTES

Organizations should carefully consider the potential impacts of employing the procedures defined in this Special Publication when assessing the security controls in *operational* information systems. Certain assessment procedures, particularly those procedures that directly impact the operation of hardware, software, and/or firmware components of an information system, may inadvertently affect the routine processing, transmission, or storage of information supporting critical organizational missions or business functions. For example, a key information system component may be taken offline for assessment purposes or a component may suffer a fault or failure during the assessment process. Organizations should take necessary precautions during security control assessment periods to ensure that organizational missions and business functions continue to be supported by the information system and that only approved impacts to operational effectiveness are caused by the assessment.

Security controls from NIST Special Publication 800-53 have been restated in NIST Special Publication 800-53A for ease of reference by assessors in specifying assessment procedures for conducting assessments of security controls and should not be viewed as replacing or revising the security controls in Special Publication 800-53, which remains the definitive NIST recommendation for employing security controls in federal information systems.

Unless otherwise stated, all references to NIST publications in this document (i.e., Federal Information Processing Standards and Special Publications) are to the most recent version of the referenced publication.

Table of Contents

CHAPTER ONE INTRODUCTION	1
1.1 PURPOSE AND APPLICABILITY	1
1.2 TARGET AUDIENCE	3
1.3 RELATIONSHIP TO OTHER ASSESSMENT PROCESSES AND PUBLICATIONS	3
1.4 ORGANIZATION OF THIS SPECIAL PUBLICATION	4
CHAPTER TWO THE FUNDAMENTALS	6
2.1 ASSESSMENTS WITHIN THE SYSTEM DEVELOPMENT LIFE CYCLE	6
2.2 STRATEGY FOR CONDUCTING SECURITY CONTROL ASSESSMENTS.....	6
2.3 BUILDING AN EFFECTIVE ASSURANCE CASE	8
2.4 ASSESSMENT PROCEDURES	8
2.5 EXTENDED ASSESSMENT PROCEDURE	13
CHAPTER THREE THE PROCESS	14
3.1 PREPARING FOR SECURITY CONTROL ASSESSMENTS.....	14
3.2 DEVELOPING SECURITY ASSESSMENT PLANS	16
3.3 CONDUCTING SECURITY CONTROL ASSESSMENTS	23
3.4 ANALYZING SECURITY ASSESSMENT REPORT RESULTS	25
APPENDIX A REFERENCES	A-1
APPENDIX B GLOSSARY	B-1
APPENDIX C ACRONYMS	C-1
APPENDIX D ASSESSMENT METHOD DESCRIPTIONS	D-1
APPENDIX E ASSESSMENT EXPECTATIONS.....	E-1
APPENDIX F ASSESSMENT PROCEDURE CATALOG	F-1
APPENDIX G PENETRATION TESTING	G-1
APPENDIX H ASSESSMENT PROCEDURE WORK SHEET	H-1
APPENDIX I SECURITY ASSESSMENT REPORTS	I-1
APPENDIX J ASSESSMENT CASES	J-1

CHAPTER ONE

INTRODUCTION

THE NEED TO ASSESS SECURITY CONTROL EFFECTIVENESS IN INFORMATION SYSTEMS

Today's information systems⁶ are incredibly complex assemblages of technology (including hardware, software, and firmware), processes, and people, all working together to provide organizations with the capability to process, store, and transmit information on a timely basis to support various organizational missions and business functions. The degree to which organizations have come to depend upon these information systems to conduct routine and critical missions and business functions means that the protection of the underlying systems is paramount to the success of the organization. The selection of appropriate security controls for an information system is an important task that can have major implications on the operations and assets of an organization as well as the welfare of individuals.⁷ Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity (including non-repudiation and authenticity), and availability of the system and its information. Once employed within an information system, security controls are assessed to provide the information necessary to determine their overall effectiveness; that is, the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Understanding the overall effectiveness of the security controls implemented in the information system is essential in determining the risk to the organization's operations and assets, to individuals, to other organizations, and to the Nation resulting from the use of the system.

1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide guidelines for building effective security assessment plans and a comprehensive set of procedures for assessing the effectiveness of security controls employed in information systems supporting the executive agencies of the federal government. The guidelines apply to the security controls defined in NIST Special Publication 800-53 (as amended), *Recommended Security Controls for Federal Information Systems*, and any additional security controls developed by the organization. The guidelines have been developed to help achieve more secure information systems within the federal government by:

- Enabling more consistent, comparable, and repeatable assessments of security controls;
- Facilitating more cost-effective assessments of security controls contributing to the determination of overall control effectiveness;
- Promoting a better understanding of the risks to organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems; and
- Creating more complete, reliable, and trustworthy information for organizational officials—to support security accreditation decisions, information sharing, and FISMA compliance.

⁶ An information system is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

⁷ When selecting security controls for an information system, the organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts.

The guidelines provided in this special publication are applicable to all federal information systems other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542. The guidelines have been broadly developed from a technical perspective to complement similar guidelines for national security systems and may be used for such systems with the approval of the Director of National Intelligence (DNI), the Secretary of Defense (SECDEF), or the Chairman of the Committee on National Security Systems (CNSS), or their designees. State, local, and tribal governments, as well as private sector organizations that compose the critical infrastructure of the United States, are also encouraged to consider the use of these guidelines, as appropriate.

Organizations should use as a minimum, NIST Special Publication 800-53A in conjunction with an approved information system security plan in developing a viable security assessment plan for producing and compiling the information necessary to determine the effectiveness of the security controls employed in the information system. This publication has been developed with the intention of enabling organizations to tailor and supplement the basic assessment procedures provided. The assessment procedures should be used as a starting point for and as input to the security assessment plan. In developing effective security assessment plans, organizations should take into consideration existing information about the security controls to be assessed (e.g., results from organizational assessments of risk, platform-specific dependencies in the hardware, software, or firmware,⁸ and any assessment procedures needed as a result of organization-specific controls not included in NIST Special Publication 800-53).

The selection of appropriate assessment procedures for a particular information system depends on three factors:

- The security categorization of the information system in accordance with FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*;
- The security controls identified in the approved information system security plan, including those from NIST Special Publication 800-53 (as amended) and any organization-specific controls;⁹ and
- The level of assurance that the organization must have in determining the effectiveness of the security controls in the information system.

The extent of security control assessments should always be risk-driven. Organizations should determine the most cost-effective implementation of this key element in the organization's information security program by applying the results of risk assessments, considering the maturity and quality level of the organization's risk management processes, and taking advantage of the flexibility in NIST Special Publication 800-53A. The use of Special Publication 800-53A as a starting point in the process of defining procedures for assessing the security controls in information systems, promotes a more consistent level of security within the organization and offers the needed flexibility to customize the assessment based on organizational policies and

⁸ For example, detailed test scripts may need to be developed for the specific operating system, network component, middleware, or application employed within the information system to adequately assess certain characteristics of a particular security control. Such test scripts are at a lower level of detail than provided by the assessment procedures contained in Appendix F (Assessment Procedures Catalog) and are therefore beyond the scope of this publication.

⁹ The set of agreed-upon security controls for the information system are documented in the system security plan after the initial selection and supplementation of the controls as described in NIST Special Publication 800-53. The security plan is approved by appropriate organizational officials prior to the start of the security control assessment.

requirements, known threat and vulnerability information, operational considerations, information system and platform dependencies, and tolerance for risk.¹⁰ Ultimately, organizations should view assessment as an information gathering activity, not a security producing activity.¹¹ Therefore, organizations should make the final determination on the extent of security control assessments, to include the level of effort and resources expended during those assessments, on the basis of what will most cost-effectively confirm or determine whether the information system security requirements have been met.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse group of information system and information security professionals including:

- Individuals with information system and security control assessment and monitoring responsibilities (e.g., system evaluators, assessors/assessment teams, certification agents/certification teams, independent verification and validation assessors, auditors, inspectors general, information system owners);
- Individuals with information system and security management and oversight responsibilities (e.g., authorizing officials, senior agency information security officers, information security managers);
- Individuals with information security implementation and operational responsibilities (e.g., information system owners, mission/information owners, and information system security officers); and
- Individuals with information system development and integration responsibilities (e.g., program managers, information technology product developers, information system developers, systems integrators).

1.3 RELATIONSHIP TO OTHER ASSESSMENT PROCESSES AND PUBLICATIONS

NIST Special Publication 800-53A has been designed to be used with NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*. In particular, the assessment procedures contained in this publication and the guidelines provided for developing security assessment plans for organizational information systems directly support the security certification and continuous monitoring phases in the four-phase certification and accreditation process. The primary objective of the security certification phase is to help determine if the security controls in the information system are effective in their application (i.e., implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system). The security assessment procedures defined in this publication provide a foundational level of assessment to support the security certification process. As the information system moves into the continuous monitoring phase (subsequent to system authorization during the security accreditation phase), organizations can select an appropriate subset of the assessment procedures from the security assessment plan to assess the

¹⁰ In this publication, the term *risk* is used to mean risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation.

¹¹ The information produced during security control assessments can be used by an organization to: (i) identify potential problems or shortfalls in the organization's implementation of the Risk Management Framework; (ii) identify information system weaknesses and deficiencies; (iii) prioritize risk mitigation decisions and associated risk mitigation activities; (iv) confirm that identified weaknesses and deficiencies in the system have been addressed; (v) support information system authorization (security accreditation) decisions; and (vi) support budgetary decisions and the capital investment process.

security controls on an ongoing basis. The procedures selected for the follow-on assessments that occur during the continuous monitoring phase are based on the organization's risk assessment, the plan of action and milestones for the information system, and organizational security policies, any of which may indicate the need for greater emphasis on assessment of selected security controls.

Organizations are encouraged, whenever possible, to take advantage of the assessment results and associated assessment-related documentation and evidence available on information system components from previous assessments including independent third-party testing, evaluation, and validation.¹² Product testing, evaluation, and validation are routinely conducted today on cryptographic modules and general-purpose information technology products such as operating systems, database systems, firewalls, intrusion detection devices, web browsers, web applications, smart cards, biometrics devices, personal identity verification devices, web applications, network devices, and hardware platforms using national and international standards. If an information system component product is identified as providing support for the implementation of a particular security control in NIST Special Publication 800-53, then any available evidence produced during the product testing, evaluation, and validation processes (e.g., security specifications, analyses and test results, validation reports, and validation certificates)¹³ should be used to the extent that it is applicable. This evidence should be combined with the assessment-related evidence obtained from the application of the assessment procedures in this publication, to cost-effectively produce the information necessary to determine whether the security controls are effective or ineffective in their application.

1.4 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the fundamental concepts associated with security control assessments including: (i) the integration of assessments into the system development life cycle; (ii) the importance of an organization-wide strategy for conducting security control assessments; (iii) the development of effective assurance cases; (iv) the format and content of assessment procedures; and (v) the use of an extended assessment procedure to help increase the grounds for confidence in the effectiveness of the security controls being assessed.
- **Chapter Three** describes the process of assessing the security controls in organizational information systems including: (i) the activities carried out by organizations and assessors to prepare for security control assessments; (ii) the development of security assessment plans; (iii) the conduct of security control assessments and the analysis, documentation, and reporting of assessment results; and (iv) post-assessment report analysis and follow-on activities carried out by organizations.

¹² Assessment results can be obtained from many activities that occur routinely during the System Development Life Cycle processes within organizations. For example, assessment results are produced during the testing and evaluation of new information system components during system upgrades or system integration activities. Organizations should take advantage of previous assessment results whenever possible, to reduce the overall cost of assessments and to make the assessment process more efficient.

¹³ Organizations should review the component product's available information to determine: (i) what security controls are implemented by the product; (ii) if those security controls meet intended control requirements of the information system under assessment; (iii) if the configuration of the product and the environment in which the product operates are consistent with the environmental and product configuration as stated by the vendor/developer; and (iv) if the assurance requirements stated in the developer/vendor specification satisfies the assurance requirements for assessing those controls. Meeting the above criteria provides a sound rationale that the product is suitable and meets the intended security control requirements of the information system under assessment.

- **Supporting appendices** provide detailed assessment-related information including: (i) general references; (ii) definitions and terms; (iii) acronyms; (iv) a description of assessment methods; (v) assessment expectations for low-impact, moderate-impact, and high-impact information systems; (vi) a master catalog of assessment procedures that can be used to develop plans for assessing security controls; (vii) penetration testing guidelines; (viii) an assessment procedure work sheet; (ix) a sample format for security assessment reports; and (x) the use of exemplary assessment cases.

Draft

SECTION 515 PRE-DISSEMINATION REVIEW & DOCUMENTATION GUIDELINES

Background

Section 515 of the Treasury and General Government Appropriations Act for Fiscal Year 2001 (Public Law 106-554, aka the Data Quality Act or Information Quality Act) directed the Office of Management and Budget (OMB) to issue government-wide guidelines that “provide policy and procedural guidance to federal agencies for ensuring and maximizing the quality, objectivity, utility, and integrity of information (including statistical information) disseminated by federal agencies.” OMB complied by issuing guidelines which direct each federal agency to 1) issue its own guidelines; 2) establish administrative mechanisms allowing affected persons to seek and obtain correction of information that does not comply with the OMB 515 Guidelines or the agency guidelines; and 3) report periodically to OMB on the number and nature of complaints received by the agency and how the complaints were handled. The OMB Guidelines can be found at: <http://www.whitehouse.gov/omb/fedreg/reproducible2.pdf>

The Department of Commerce Guidelines can be found at: <http://www.osec.doc.gov/cio/oipr/iqg.htm>

The NOAA Section 515 Information Quality Guidelines, created with input and reviews from each of the components of NOAA Fisheries, went into effect on October 1, 2002. **The NOAA Information Quality Guidelines are posted on the NOAA home page under “Information Quality.”** <http://www.noaanews.noaa.gov/stories/iq.htm>

The guidelines apply to a wide variety of government information products and all types of media, including printed, electronic, broadcast or other. The guidelines define “Information” as, “any communication or representation of knowledge such as facts or data, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.” For example, this definition includes information that an agency disseminates from a web page. The guidelines define “Dissemination” as, “agency initiated or sponsored distribution of information to the public.” Explicitly **not** included within this term is distribution limited to “government employees or agency contractors or grantees; intra- or inter-agency use or sharing of government information; and responses to requests for agency records under the Freedom of Information Act, the Privacy Act, the Federal Advisory Committee Act or other similar law.” It also does not include distribution limited to correspondence with individuals or persons, press releases, archival records, public filings, subpoenas or adjudicative processes. (See the NOAA IQ Guidelines, pgs 5-6).

To assist in Data Quality Act compliance, NOAA Fisheries has established a series of actions that should be completed for each new information product subject to the Data Quality Act. (See “Information Generation and Compliance Documentation” and “Pre-Dissemination Review” below.) **In addition to the information contained in this document, familiarity with the NOAA Section 515 Information Quality Guidelines (<http://www.noaanews.noaa.gov/stories/iq.htm>) is crucial for NOAA Fisheries employees who engage in the generation and dissemination of information.**

Information Generation and Compliance Documentation

- The fundamental step in the process is to create a Sec. 515 Information Quality file for each new information product. To aid in this process, a Section 515 Pre-Dissemination Review and Documentation form has been created. These guidelines are intended to serve as a supplement to the Pre-Dissemination Review and Documentation Form. The basic steps to the documentation process are outlined below.
- Complete general information (e.g., author/responsible office, title/description) section of the form.
- Determine the information category (i.e., original data; synthesized products; interpreted products; hydrometeorological, hazardous chemical spill, and space weather warnings, forecasts, and advisories; experimental products; natural resource plans; corporate and general information). **For most information products, you will only need to check one box.** More complex documents may be an “aggregate” of different categories of information products.
- Generate the information in a way that meets each of the applicable standards for the appropriate information category. See the NOAA Information Quality Guidelines.
- Document how the standards for **utility, integrity and objectivity** are met for each information product, describing what measures were taken to meet each of the applicable standards. Use the 2 page Pre-Dissemination Review & Documentation Form to document compliance with the Utility and Integrity standards contained in NOAA’s Information Quality Guidelines. The Utility and Integrity standards pertain to all categories of information disseminated by NOAA. Use these guidelines (pgs 4-11) to document compliance with the applicable objectivity standards for your information product and attach that documentation to the Pre-Dissemination Review & Documentation Form.
- Maintain the Sec. 515 Information Quality file in a readily accessible place. [Pre-Dissemination Review](#)
- Before information is disseminated, it must be reviewed for compliance with the NOAA Sec. 515 Information Quality Guidelines. This is accomplished by reviewing the information and the Sec. 515 Information Quality file.
- The Pre-Dissemination Review should be conducted during the normal course of clearing the information product for release. The person conducting the Pre-Dissemination Review will sign and date the Pre-Dissemination Review & Documentation Form. The reviewing official must be at least one level above the person generating the information product.
- The Pre-Dissemination Review form and the supporting information quality documentation must accompany the information product through the clearance process and be maintained on file.

Completing the Section 515 Pre-Dissemination Review & Documentation Form

Using the Section 515 Pre-Dissemination Review & Documentation Form and these guidelines, document how the information product meets the

following standards for **Utility, Integrity and Objectivity**. **Please note:** Use the Pre-Dissemination Review & Documentation Form to document how the information product complies with the Utility and Integrity standards that pertain to all categories of information products. The Utility and Integrity standards are presented here for your convenience. Use these guidelines to explain how the information product meets the applicable Objectivity standards for the information product and attach that documentation to the Pre-Dissemination Review & Documentation Form.

I. Utility of Information Product

Utility means that disseminated information is useful to its intended users. "Useful" means that the content of the information is helpful, beneficial, or serviceable to its intended users, or that the information supports the usefulness of other disseminated information by making it more accessible or easier to read, see, understand, obtain or use.

- A. Is the information helpful, beneficial or serviceable to the intended user? Explain.
- B. Who are the intended users of the data or information product? (e.g., the American public; other federal agencies; state and local governments; recreational concerns; national and international organizations). Is this data or information product an improvement over previously available information? Is it more detailed or current? Is it more useful or accessible to the public? Has it been improved based on comments or interactions with users?
- C. What media are used in the dissemination of the information? Printed publications? CD-ROM? Internet?
Is the product made available in a standard data format?
Does it use consistent attribute naming and unit conventions to ensure that the information is accessible to a broad range of users with a variety of operating systems and data needs?

II. Integrity of Information Product

Integrity refers to security - the protection of information from unauthorized access or revision, to ensure that the information is not compromised through corruption or falsification. Prior to dissemination, NOAA information, independent of the specific intended distribution mechanism, is safeguarded from improper access, modification, or destruction, to a degree commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information. **Please note: all electronic information disseminated by NOAA adheres to the standards set forth in paragraph A below. If the information product is disseminated electronically, simply circle paragraph II(A) on the form.** You may also contact your IT Manager for further information.

Explain (circle) how the information product meets the following standards for integrity:

- A. 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.
- B. If information is confidential, it is safeguarded pursuant to the Privacy Act and Titles 13, 15, and 22 of the U. S. Code (confidentiality of census, business and financial information).
- C. Other/Discussion
(e.g., 50 CFR 600, Subpart E, Confidentiality of Statistics of the Magnuson-Stevens Fishery Conservation and Management Act; NOAA Administrative Order 216-100, Protection of Confidential Fisheries Statistics; 50 CFR 229.11, Confidentiality of information collected under the Marine Mammal Protection Act.)

III. Objectivity of Information Product

(1) Indicate which one of the following categories of information products apply for this product (check one):

- Original Data - go to Section A
- Synthesized Products - go to Section B
- Interpreted Products - go to Section C
- Hydrometeorological, Hazardous Chemical Spill, and Space Weather Warnings, Forecasts, and Advisories - go to Section D
- Experimental Products - go to Section E
- Natural Resource Plans - go to Section F
- Corporate and General Information - go to Section G

(2) Describe how this information product meets the applicable objectivity standards.

General Standard: Information is presented in an accurate, clear, complete, and unbiased manner, and in proper context. The substance of the information is accurate, reliable, and unbiased; in the scientific, financial or statistical context, original and supporting data are generated and the analytical results are developed using sound, commonly accepted scientific and research methods. "Accurate" means that information is within an acceptable degree of imprecision or error appropriate to the particular kind of information at issue and otherwise meets commonly accepted scientific, financial and statistical standards.

If the information is "influential," that is, it is expected to have a genuinely clear and substantial impact on major public policy and private sector decisions, it is noted as such and it is presented with the highest degree of transparency. If influential information constitutes an assessment of risks to human health, safety or the environment, indicate whether the risk assessment was qualitative or quantitative, and describe which SDWA-adapted quality standards at page 9 of NOAA's Section 515 Information Quality Guidelines were applied to the information product.

Use of third party information in the product (information not collected or generated by NOAA) is only done when the information is of known quality and consistent with NOAA's Section 515 Guidelines; any limitations, assumptions, collection methods, or uncertainties concerning the information are taken into account and disclosed.

Specific Standards: Specific objectivity standards for categories of information products disseminated by NOAA are listed below. Document how the general and specific objectivity standards for the particular information product were met.

A. Original Data

Original Data are data in their most basic useful form. These are data from individual times and locations that have not been summarized or processed to higher levels of analysis. While these data are often derived from other direct measurements (e.g., spectral signatures from a chemical analyzer, electronic signals from current meters), they represent properties of the environment. These data can be disseminated in both real time and retrospectively. Examples of original data include buoy data, survey data (e.g., living marine resource and hydrographic surveys), biological and chemical properties, weather observations, and satellite data.

Objectivity of original data is achieved using sound quality control techniques.

Detail how the data collection methods, systems, instruments, training, and/or tools are appropriate to meet the requirements of the intended users.

Were the methods, systems, instruments, etc., validated before use?

Were standard operating procedures (SOPs) followed for time series data collections? If not, document the valid scientific reasons for the deviation.

Document the quality control techniques used, for example:

- Gross error checks for data that fall outside of physically realistic ranges (e.g., a minimum, maximum or maximum change)
- Comparisons made with other independent sources of the same measurement
- Examination of individual time series and statistical summaries
- Application of sensor drift coefficients determined by a comparison of pre- and post-deployment calibrations
- Visual inspection of data

Describe any evolution and/or improvements in survey techniques, instrument performance and/or data processing.

Have metadata record descriptions and explanations of the methods and quality controls to which original data are subjected been included in the disseminated product? If not, they must be made available upon request.

B. Synthesized Products

Synthesized Products are those that have been developed through analysis of original data. This includes analysis through statistical methods; model interpolations, extrapolations, and simulations; and combinations of multiple sets of original data.

While some scientific evaluation and judgment is needed, the methods of analysis are well documented and relatively routine.

Examples of synthesized products include summaries of fisheries landings statistics, weather statistics, model outputs, data display through Geographical Information System techniques, and satellite-derived maps.

The objectivity of synthesized products is achieved by using data of known quality, applying sound analytical techniques, and reviewing the products or processes used to create them before dissemination. For synthesized products, please document the following:

Identify data sources (preferred option) or be prepared to make them available upon request.

Are the data used of known quality or from sources acceptable to the relevant scientific and technical communities?

Are the methods used to create the synthesized product published in standard methods manuals or generally accepted by the relevant scientific and technical communities? Are the methods documented in readily accessible formats by the disseminating office?

Describe the review process used to ensure the validity of the synthesized product or the procedures used to create them, e.g., statistical procedures, models, or other analysis tools.

If the synthesized product is unique or not regularly produced, was this product reviewed by internal and/or external experts?

If this is a routinely produced synthesized product, was the process for developing the product reviewed by internal and/or external experts?

Does the synthesized product include information about the methods used to create the product? If not, the methods must be made available upon request.

C. Interpreted Products

Interpreted Products are those that have been developed through interpretation of original data and synthesized products. In many cases, this information incorporates additional contextual and/or normative data, standards, or information that puts original data and synthesized products into larger spatial, temporal, or issue contexts. This information is subject to scientific interpretation, evaluation, and judgment. Examples of interpreted products include journal articles, scientific papers, technical reports, and production of and contributions to integrated assessments.

Objectivity of interpreted products is achieved by using data of known quality or from sources acceptable to the relevant scientific and technical communities and reliable supporting products, applying sound analytical techniques, presenting the information in the proper context, and reviewing the products before dissemination.

Are all data and information sources identified or properly referenced?

Are the methods used to create the interpreted product generally accepted by the relevant scientific and technical communities?

Is information concerning the quality and limitations of the interpreted product provided to help the user assess the suitability of the product for the user's application?

Describe the review process used to ensure that the product is valid, complete, unbiased, objective and relevant. For example, peer reviews, ranging from internal peer review by staff who were not involved in the development of the product to formal, independent, external peer review. The review should be conducted at a level commensurate with the importance of the interpreted product.

Does the interpreted product include a description of the methods used to create the product? If not, they must be made available upon

request.

D. Hydrometeorological, Hazardous Chemical Spill, and Space Weather

Warnings, Forecasts, and Advisories

Hydrometeorological, Hazardous Chemical Spill, and Space Weather Warnings, Forecasts, and Advisories are time-critical interpretations of original data and synthesized products, prepared under tight time constraints and covering relatively short, discrete time periods. As such, these warnings, forecasts, and advisories represent the best possible information in given circumstances. They are subject to scientific interpretation, evaluation, and judgment. Some products in this category, such as weather forecasts, are routinely prepared. Other products, such as tornado warnings, hazardous chemical spill trajectories, and solar flare alerts, are of an urgent nature and are prepared for unique circumstances.

Objectivity of information in this category is achieved by using reliable data collection methods and sound analytical techniques and systems to ensure the highest possible level of accuracy given the time critical nature of the products.

What is the source of the data or information used in the product? Are the data used of known quality or from sources acceptable to the relevant scientific and technical communities? Are the sources included in the information product? If not, they must be made available upon request. Are the methods used to create the product generally accepted by the relevant scientific and technical communities?

Please note if individual best judgment was used due to the time-critical nature of the product.

What mechanisms were used to evaluate the accuracy of the information product? Statistical analysis may be carried out for a subset of products for verification purposes.

E. Experimental Products

Experimental products are products that are experimental (in the sense that their quality has not yet been fully determined) in nature, or are products that are based in part on experimental capabilities or algorithms. Experimental products fall into two classes.

They are either (1) disseminated for experimental use, evaluation or feedback, or (2) used in cases where, in the view of qualified scientists who are operating in an urgent situation in which the timely flow of vital information is crucial to human health, safety, or the environment, the danger to human health, safety, or the environment will be lessened if every tool available is used. Examples of experimental products include imagery or data from non-NOAA sources, algorithms currently being tested and evaluated, experimental climate forecasts, and satellite imagery processed with developmental algorithms for urgent needs (e.g., wildfire detection).

Objectivity of experimental products is achieved by using the best science and supporting studies available, in accordance with sound and objective scientific practices, evaluated in the relevant scientific and technical communities, and peer-reviewed where feasible.

Describe the science and/or supporting studies used, the evaluation techniques used, and note any peer-review of the experimental product. Were the results of initial tests or evaluations made available where possible? Describe the review, by the appropriate NOAA unit, of the experimental products and capabilities documentation, along with any tests or evaluations.

Are explicit limitations provided concerning the quality of the experimental product? Is the degree of uncertainty indicated?

Describe the testing process used, e.g., the experimental product or capabilities are used only after careful testing, evaluation, and review by NOAA experts, and then are approved for provisional use only by selected field offices or other NOAA components. This process is repeated as needed to ensure an acceptable and reliable level of quality.

F. Natural Resource Plans

Natural Resource Plans are information products that are prescribed by law and have content, structure, and public review processes (where applicable) that will be based upon published standards, e.g., statutory or regulatory guidelines. Examples of such published standards include the National Standard Guidelines (50 CFR Part 600, Subpart D), Essential Fish Habitat Guidelines, and Operational Guidelines - Fishery Management Plan Process, all under the Magnuson-Stevens Fishery Conservation and Management Act; and the National Marine Sanctuary Management Plan Handbook (16 U.S.C. section 1434) under the National Marine Sanctuary Act. These Natural Resource Plans are a composite of several types of information (e.g., scientific, management, stakeholder input, and agency policy) from a variety of internal and external sources. Examples of Natural Resources Plans include fishery, protected resource, and sanctuary management plans and regulations, and natural resource restoration plans.

Objectivity of Natural Resource Plans will be achieved by adhering to published standards, using information of known quality or from sources acceptable to the relevant scientific and technical communities, presenting the information in the proper context, and reviewing the products before dissemination.

What published standard(s) governs the creation of the Natural Resource Plan? Does the Plan adhere to the published standards? (See the NOAA Sec. 515 Information Quality Guidelines, Section II(F) for links to the published standards for the Plans disseminated by NOAA.)

Was the Plan developed using the best information available? Please explain.

Have clear distinctions been drawn between policy choices and the supporting science upon which they are based? Have all supporting materials, information, data and analyses used within the Plan been properly referenced to ensure transparency?

Describe the review process of the Plan by technically qualified individuals to ensure that the Plan is valid, complete, unbiased, objective and relevant. For example, internal review by staff who were not involved in the development of the Plan to formal, independent, external peer review. The level of review should be commensurate with the importance of the Plan and the constraints imposed by legally enforceable deadlines.

G. Corporate and General Information

Corporate or general information includes all non-scientific, non-financial, non-statistical information. Examples include program and organizational descriptions, brochures, pamphlets, education and outreach materials, newsletters, and other general descriptions of NOAA operations and capabilities.

Corporate and general information disseminated by NOAA must be presented in a clear, complete, and unbiased manner, and in a context that enhances usability to the intended audience. To the extent possible, identify the sources of the disseminated information, consistent with confidentiality, privacy and security considerations and protections, and taking into account timely presentation, the medium of dissemination, and the importance of the information, balanced against the resources required and the time available.

Information disseminated by NOAA is reliable and accurate to an acceptable degree of error as determined by factors such as the importance of the information, the intended use, time sensitivity, expected degree of permanence, relation to the primary mission(s) of the disseminating office, and the context of the dissemination, balanced against the resources required and the time available.

For non-scientific, non-statistical information, has the information product been reasonably determined to be factually correct in the view of the disseminating office as of the time of dissemination?

Describe the review process for the information product. Review can be accomplished in a number of ways, including but not limited to combinations of the following:

- Active personal review of information by supervisory and management layers, either by reviewing each individual dissemination, or selected samples, or by any other reasonable method.
- Use of quality check lists, charts, statistics, or other means of tracking quality, completeness, and usefulness.
- Process design and monitoring to ensure that the process itself imposes checks on information quality .
- Review during information preparation.
- Use of management controls.
- Any other method, which serves to enhance the accuracy, reliability and objectivity of the information.

SUPPLEMENTARY INFORMATION: The Ocean.US Office, operating by interagency agreement under the statutory authority of the National Oceanographic Partnership Program (NOPP, 10 U.S.C. 7901 *et seq.*), serves as the national agent for integrating ocean observing activities (<http://www.ocean.us>). Ocean.US is also the focal point for relating U.S. ocean observing system elements to associated international efforts, such as the Global Earth Observing System of Systems (GEOSS) and the Intergovernmental Oceanographic Commission (IOC) sponsored Global Ocean Observing System (GOOS). The U.S. IOOS represents the U.S. contribution to the ocean components of these international partnership efforts. Key to the realization of the U.S. IOOS is the establishment of an integrated DMAC infrastructure. This infrastructure will enable users to discover, retrieve, and use data from Federal and State government, government-sponsored, other public, private, and commercial coastal and ocean observing activities regardless of source or location. In 2005 Ocean.US established an IOOS DMAC Steering Team drawn from government, industry, academia, public, and non-profit communities to: (a) Coordinate and oversee the evolution of DMAC standards; (b) identify and provide recommendations regarding gaps in needed standards; and, (c) help ensure that the DMAC standards process is conducted in an open, objective, and balanced manner. That team adopted a standards process in May 2006 that includes these public comment periods as a critical input to any decisions on a particular standard.

Review to Date of the Proposed Standards

Proposed standards have been reviewed by members of the DMAC Steering Team and its Expert Teams for non-technical and technical criteria. Their designation as 'proposed' indicates the standard has potential merit for application in IOOS and should be evaluated further based on actual use in pilot projects and demonstrations and based on public comments on experience using the standard in IOOS applications.

Authority: 10 U.S.C. 7901 *et seq.*

Dated: January 17, 2008.

Elizabeth R. Scheffler,

Associate Assistant Administrator for Management, Ocean Services and Coastal Zone Management.

[FR Doc. E8-1723 Filed 1-30-08; 8:45 am]

BILLING CODE 3510-22-P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

RIN 0648-XF16

Vessel Monitoring Systems; Specification of Requirements for Mobile Transmitting Unit Type Approval

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

ACTION: Revision of type approval requirements for mobile transmitting units.

SUMMARY: This document provides notice of type approval requirements for Mobile Transmitting Units (MTU) to be authorized for use on any vessel participating in the NOAA Vessel Monitoring System (VMS) program. Vessels participating in VMS program must acquire an NMFS-approved MTU to comply with VMS standards set forth in NMFS rules requiring the use of VMS.

ADDRESSES: To obtain copies of the list of NMFS-approved VMS MTU and VMS communications service providers, or to obtain information regarding the status of VMS systems being evaluated by NOAA, write to NOAA Fisheries, Office for Law Enforcement (OLE), 8484 Georgia Avenue, Suite 415, Silver Spring, MD 20910.

FOR FURTHER INFORMATION CONTACT: For current listing information contact the VMS Support Center by phone: 888-210-9228, or by fax: 301-427-0049 or for questions regarding VMS installation and status of evaluations contact Jonathan Pinkerton, National VMS Program Manager by phone: 301 427 2300 or by fax: 301-427-0049.

SUPPLEMENTARY INFORMATION: This notice supersedes all previous notices on MTU type approval requirements. Previously installed MTU approved under prior notices will continue to be approved for the remainder of their service life. New installations of a previously approved MTU occurring 120 days or more after the publication date of this notice must comply with all of the requirements herein. All new requests for type approval must comply with all of the requirements herein.

Background

The Department of Commerce, National Oceanic and Atmospheric Administration, National Marine Fisheries Service, Office for Law Enforcement (OLE) maintains MTU

specification requirements as an OLE National Directive. This notice sets prerequisite standards for the purpose of type approval that must be met by an MTU and any associated software before it is authorized for use in the NOAA VMS program. Vessels participating in VMS program must acquire an NMFS-approved MTU to comply with the specific VMS standards set forth in NMFS rules requiring the use of VMS. The MTU is a transceiver or communications device, including antennae, dedicated message terminal and display, and an input device such as a keyboard installed on fishing vessels participating in the VMS requirement. The MTU allows OLE to determine the geographic position of the vessel during specified intervals or events. In addition, it enables mobile communications services between OLE and the vessel when using an NMFS-accepted Mobile Communication Service Provider (MCSP). (Note: Standards for the MCSP are written in the complementary directive titled Mobile Communication Service Provider Specification of Requirements.)

Goal

OLE seeks to deploy an "open system," whereby the fishing industry participants may select from a variety of suppliers that qualify and have been approved to participate in VMS program. Fishermen must comply with applicable Federal fishery regulations regarding VMS and therefore may be cited for a violation and held accountable for monitoring anomalies not attributable to faults in the MCSP or MTU. Therefore, type approval is essential to establish and maintain uniformly high system integrity. By this directive, OLE seeks to approve reliable, robust, and secure MTU products and thereby create and maintain a VMS meeting the requirement of high integrity. Specific VMS programs are created to support particular NMFS rules requiring the use of VMS, which typically are designed to manage or protect fish and other marine species within designated areas.

Process

Based on a request for type approval from an MTU supplier and certification of certain minimal standards, OLE will conduct a thorough evaluation and then issue a statement accepting or denying the type approval of the particular MTU. An MTU must meet the minimal national VMS standards, as required by this directive, and the requirements of the specific fisheries for which approval is sought. MTU supplier requesters are encouraged to review the national VMS

standards and NMFS rules requiring the use of VMS prior to submitting a request for approval. Upon successful demonstration of compliance with the requirements set forth in this directive, NMFS will issue an MTU type approval within a particular communications Class applicable to one or more VMS operations targeting particular NMFS rules requiring the use of VMS. OLE will maintain a current list of type approved MTU(s), and will forward lists of type approved MTU(s) to the respective regional Fisheries Management Council(s), post the information on the OLE website and provide it by fax upon request.

NMFS approval will not necessarily result in agency procurement of the MTU. Instead, OLE will request that the MTU supplier provide a fact sheet to the fishing industry. The fact sheet will allow fishermen to make purchase decisions that are compatible with the VMS standards and their individual needs. Purchasing strategies are determined on a per implementation basis.

Initiation

OLE will initiate the MTU type approval process upon written request from the supplier, subject to the demonstration of compliance with this directive and the availability of test units. The requestor for type approval may include the manufacturer, or an OEM/labeler, distributor, and/or reseller acting as a representative of the manufacturer. The evaluation may include consideration if that MTU has already passed a comparable type approval process to qualify for use in a foreign fisheries management effort. If applicable, the supplier should provide the MTU's identifying characteristics, the details of the foreign VMS requirement specifications, the MTU's level of compliance with them, and appropriate contact details of the approving authorities. NMFS also will consider approving an MTU OEM (original equipment manufacturer) model built from an equivalent MTU that already has received agency type approval under this directive.

Interoperability

A supplier of an MTU seeking type approval within a particular communications class for VMS shall demonstrate that it meets the standards when using at least one qualified MCSP within that same class. The standards in this directive are intended to ensure that type approval for a particular MTU will permit its interoperability with all qualified MCSPs within its same class. A class refers to the medium, protocol,

and frequency of the mobile communications technology. Some examples of existing classes include Inmarsat-C and Qualcomm/OmniTracs. To best promote interoperability within a class, MTU and MCSP acceptance standards are outlined in separate directives. However, concurrent with the approval process for an MTU, the approval for a same-class MCSP must be either in place or pending. Data received by OLE from the MTU via an approved MCSP must be in a format compatible with OLE tracking software.

Submission

A supplier of an MTU requesting type approval shall begin by certifying that the MTU meets the minimum national VMS standards as required by this directive. Suppliers must describe in detail the extent to which its MTU complies with each of the requirements for the VMS implementation of interest as stated within this directive. The supplier, or requestor for type approval, must provide OLE with two MTUs for each fishery for which application is made for a minimum of 90-days for testing and evaluation. The supplier must also provide thorough MTU documentation, including fact sheets, installation guides, operator manuals, user handbooks, the applicable interfacing software, and technical support. OLE shall review the submissions against the criteria of this directive. Next, OLE shall perform field test and sea trials. For this, OLE will either coordinate test conditions with volunteer and/or contract fishing vessels, or contract a third-party to accomplish this task. The tests may involve demonstrating every aspect of MTU operation, including installation of a registered MTU, location tracking, messaging, and maintenance procedures.

Submit requests for type approval, along with hard and soft copies of support material to: U.S. Department of Commerce; National Oceanic and Atmospheric Administration; National Marine Fisheries Service; Office for Law Enforcement; Attention: Vessel Monitoring System Program; 8484 Georgia Ave. Suite 415; Silver Spring, MD 20910 USA; voice 301-427-2300; fax 301-427-0049.

Litigation Support

Due to the use of VMS for law enforcement, all technical aspects of a supplier's submission are subject to being admitted as evidence in a court of law, if needed. The reliability of all technologies utilized in the MTU may be analyzed in court for, inter alia, testing procedures, error rates, peer

review, and general industry acceptance. Further, the supplier may be required to provide technical and expert support for a litigation to support the MTU capabilities to establish OLE's case against violators. If the technologies have previously been subject to such scrutiny in a court of law, the supplier should describe the evidence and any court finding on the reliability of the technology. Additionally, to maintain the integrity of VMS for fisheries management, the supplier will be required to sign a non-disclosure agreement limiting the release of certain information that might compromise the effectiveness of the VMS operations, such as, but not limited to, details of anti-tampering safeguards. The supplier shall include a statement confirming its agreement with these conditions.

Change Control

Once an MTU is approved, it is the supplier's responsibility to notify OLE of any substantive change in the original submission, such as changes to firmware versions, and customer support contacts. OLE reserves the right to reconsider and revoke the MTU approval if as a result of a change to the MTU or VMS requirement the unit no longer satisfies the requirement.

Any modification to the functionality of an approved MTU including but not limited to firmware, software, services, or passwords unless expressly authorized by NMFS OLE will invalidate the type approval of the unit and render it out of compliance with NMFS rules requiring the use of VMS. Any addition, deletion or change of the firmware, software, services, or passwords of an MTU unless expressly authorized by NMFS OLE will also invalidate the type approval of the unit and render it out of compliance with NMFS rules requiring the use of VMS. Fishermen that are determined to be out of compliance with Federal Fisheries VMS regulations may be cited for violations and held accountable for monitoring anomalies not attributable to faults in the MCSP or MTU.

Requester

Requesters must respond to each of the items listed in sections 1 through 6 of this document. The response should indicate how the requestor complies with the requirement referred to in the item. Items that the requestor does not currently comply with must be responded to by explaining how the requestor will comply with the requirement prior to approval.

Section 1. Identifiers

- 1.1. Specify the identifying characteristics of the MTU:
 - 1.1.1. Communications Class.
 - 1.1.2. Manufacturer.
 - 1.1.3. Brand Name.
 - 1.1.4. Model Name.
 - 1.1.5. Model Number.
 - 1.1.6. Software Version Number and Date.
 - 1.1.7. Firmware Version Number and Date.
 - 1.1.8. Hardware Version Number and Date.
 - 1.1.9. Antenna Type.
 - 1.1.10. Antenna Model Number and Date.
 - 1.1.11. Monitor or terminal Model Number and Date.
 - 1.1.12. MCSP Providing Communications Services.
- 1.2. For the following responsibilities, name the business entities who act on behalf of the manufacturer and supplier applying for type approval. Include the address, phone, contacts, email, and designated geographic territory where applicable.
 - 1.2.1. Manufacturer.
 - 1.2.2. Label or use MTU for an OEM. This includes re-labeling OEM MTUs or reselling. Reselling includes value-added reselling. The MTU that is type approved is the final, value-added product and not the original manufacturer's MTU, if enhancements or modifications have been made. For example, if a transceiver is contained within an enclosure, it is the new enclosure including the transceiver that is being type approved.
 - 1.2.3. Distribute.
 - 1.2.4. Sell.
 - 1.2.5. Bench configures the MTU at the warehouse or point of supply.
 - 1.2.6. Install MTU onboard the vessel.
 - 1.2.7. Offer limited warranty.
 - 1.2.8. Offer maintenance and service agreement.
 - 1.2.9. Repair.
 - 1.2.10. Train.
 - 1.2.11. Advertise.

Section 2. Messaging

The MTU must provide the following messaging functionality:

- 2.1. Transmit mandatory, automatically generated position reports.
- 2.2. Onboard visible or audible alarms for malfunctioning of the MTU.
- 2.3. Ability to disable non-essential alarms in non-Global Maritime Distress and Safety System (GMDSS) installations.
- 2.4. Ability to provide comprehensive and transparent communications, which function uniformly within the entire

geographic coverage area for that communications class.

- 2.5. Two-way communications between MCSP and MTU.
- 2.6. The ability to send and receive free-form Internet email text messages and electronic forms.
- 2.7. All messages should be relayed so that OLE automatically receives no less than 97 percent of all messages within 15 minutes or less of the MTU timestamp and be transparent to the geographic region.

Section 3. Position Data Formats and Transmission

- 3.1. The MTU must provide position information as required by the applicable VMS rule in addition to:
 - 3.1.1. Position fixes latitude and longitude, including the hemisphere of each.
 - 3.1.2. The position fix precision must be to the decimal minute hundredths.
 - 3.1.3. Accuracy of the reported position must be within 100 meters, unless otherwise indicated by an existing regulation or VMS requirement.
 - 3.1.4. Communications between MTU and MCSP must be secure from tampering or interception, including the reading of passwords and data. Therefore, the MTU must have mechanisms to prevent to the extent possible:
 - 3.1.4.1. Interception and "sniffing" during transmission from the MTU to MCSP via either wireless or terrestrial facilities.
 - 3.1.4.2. Spoofing, whereby one MTU is fraudulently identifying itself as another MTU.
 - 3.1.4.3. Modification of MTU identification.
 - 3.1.4.4. Interference with GMDSS or other safety/distress functions.
 - 3.1.4.5. Introduction of viruses that may corrupt, disturb, or disrupt messages, transmission, or the VMS system.
 - 3.1.4.6. Introduction of software modifications through the use of input/output devices. Item such as CDDVD readers or writers should be removed, physically disabled, or rendered inaccessible, ports and connections not directly used for connecting to the VMS device or authorized peripherals should be removed or permanently sealed.
 - 3.2. MTU shall provide the ability to meet minimum reporting requirements and intervals as required for specific NMFS rules requiring the use of VMS.
 - 3.2.1. Provide automatically generated position reporting, for vessels managed individually or grouped by fleet, such that OLE automatically receives no less than 97 percent of the position reports sent at defined intervals within 15

minutes or less of the MTU timestamp and be transparent to the geographic region.

- 3.2.2. Have the ability to store 100 position fixes in local, non-volatile memory.
- 3.2.3. Allow for defining variable reporting intervals between 5 minutes and 24 hours.
- 3.2.4. MTU must be able to change reporting intervals remotely, and only by authorized users.
- 3.3. An MTU must be able to transmit automatically generated position reports, which contain the following:
 - 3.3.1. Unique identification of an MTU within the communications class.
 - 3.3.2. Date (year/month/day with century in the year) and time (GMT) stamp of the position fix.
 - 3.4. In addition to automatically generated position reports, specially identified position reports shall be generated upon:
 - 3.4.1. Antenna disconnection
 - 3.4.2. Loss of the positioning reference signals.
 - 3.4.3. Loss of the mobile communications signals.
 - 3.4.4. Security events, power-up, power-down, and other status data.
 - 3.4.5. The vessel crossing a pre-defined geographic boundary.
 - 3.4.6. MTU status information such as configuration of programming and reporting intervals.
 - 3.4.7. When an MTU is powered up, it must automatically re-establish its position reporting function without manual intervention.

Section 4. Text Messaging

- 4.1.1. Text messaging from vessel to shore with a minimum supported message length of 1kb.
- 4.1.2. User interface must support an 'address book' capability and a function permitting a "reply" to a received message without re-entry of the senders e-mail address.
 - 4.1.3. A confirmation of delivery function is required such that a user can ascertain whether a specific message was successfully transmitted via the satellite system to the MCSP e-mail server(s).
 - 4.1.4. Onward delivery to NMFS must be reliable and make use of features such as SMTP retries and delivery confirmation to ensure a reliable transport path exists for text messages sent from the vessel to NMFS.
 - 4.1.5. The user interface must provide the ability to review by date order, or by recipient, messages that were previously sent. The terminal must support a minimum message history of 20 messages - commonly referred to as an "Outbox" or "Sent" messages display.

4.1.6. Text messaging from shore to vessel with a minimum supported message length of 1kb.

4.1.7. The user interface must provide the ability to review by date order, or by sender, all messages received. The terminal must support a minimum message history of 20 messages—commonly referred to as an “Inbox”.

4.1.8. Negative delivery notifications must be sent to the originator where delivery to the terminal could not be completed for any reason. Such Non Delivery Notification must include sufficient information to uniquely identify the message that failed and the cause of failure (i.e., mobile number invalid, mobile switched off etc.).

4.2. Electronic Forms

Pre-formatted messages are required for the collection of validated data for specific fisheries programs (i.e., declaration systems, catch effort reporting). This capability is referred to as Electronic Forms. The E-MTU must support a minimum of 20 Forms, selectable by the user from a menu. Forms must be able to be updated over the air. Copies of forms currently used by NMFS are available upon request. From time to time NMFS will provide all E-MTU approved vendors with updates defining new forms or modifying existing forms. Such notice will be at least 60 (sixty) days prior to the implementation date for the new or changed form. Vendors will be responsible for translating the requirements into MTU specific forms definitions and transmitting the same to all VMS terminals supplied to fishing vessels. All forms software provided with the E-MTU must be capable of supporting the requirements described in this specification. Additional capabilities beyond those stated here are acceptable, provided that the minimum requirements are satisfied.

4.2.1. A form is defined as: (a) 1–40 characters describing the form, (b) Delivery address (i.e., e-mail or other network identifier), (c) Form number as defined by NMFS to uniquely identify the form, (d) Form version number (numeric with one decimal place; i.e., 1.2), and (e) a collection of 1–30 fields and associated logic rules.

4.2.2. Each field (within a form) is defined by the following elements. Except where noted, all elements of the field definition are mandatory: (a) Label (0 to 40 characters, alpha numeric), (b) Context Help Text (0 to 200 characters, alpha numeric), (c) Type (Either; enumeration, numeric, alpha, alphanumeric or Boolean), (d) Default Value, (e) Optional/Mandatory/Hidden/Logic indicator, (f) Min/Max values (for numeric fields only) in range 0.000 to

999,999, (g) Decimal places (for numeric fields only) 0–3, and (h) Min/Max characters (for alpha/alphanumeric fields only).

4.2.3. Up to 100 code/value/help text pairs (enumerations only) must be provided, where codes are defined as 1–20 alphanumeric characters, values are 1–80 alphanumeric characters and help text is 0–200 characters. Such fields are typically used to permit a user to select from a range of options (i.e., geographic areas, gear types, fish species). Codes are used to compress the form data for efficient transmission. Help text would typically be displayed only when the user selects a specific value from the enumeration.

4.2.4. Form Validation: Each field must be defined as; Optional, Mandatory or Logic Driven. Mandatory fields must be entered by the user before the form is complete, optional fields that do not require data entry, and logic driven fields have their attributes determined by earlier form selections. Specifically; it must be possible for selection of an enumeration to change the optional/mandatory setting, min/max values, or the permitted enumeration values on a later field within the same form.

4.2.5. State Information: The capability to populate a form based on the last values used must be available. This provides the user with an easy mechanism to “modify” or “update” a prior submission - without unnecessary re-entry of data. The user must be able to review a minimum of 20 past form submissions and ascertain for each form when the form was transmitted and whether delivery was successfully completed to the vendor’s processing center. In the case of a transmission failure, the user must be provided with details of the cause and have the opportunity to retry the form submission.

4.2.6. Inclusion of VMS Position Report: In addition to the manually entered fields, the forms package must permit the inclusion of VMS position report fields such as latitude, longitude, date and time. Such fields must be obtained from the GPS function of the MTU and transmitted along with the manually entered form data within the same transaction.

4.2.7. Delivery Format for Form Data: It is preferred that form data be transferred from the terminal to NMFS using the same transport as for either text messages or VMS position reports (the selected option to be at the election of the E-MTU vendor). Currently supported protocols for transfer are; FTP, SMTP, XML and HTTP Post. The SMTP protocol is not permitted for the

transmission of data sent to the OLE. The field coding within the data must follow either CSV or XML formatting rules. For CSV format the form must contain an identifier and the version number, and then the fields in the order defined on the form. In the CSV format strings that may contain “,” (comma) characters must be quoted. XML representations must use the field label to define the XML element that contains each field value.

Section 5. Customer Service

The MTU supplier or its designated entities shall provide customer service that is professional, courteous, and responsive. It should provide MTU diagnostic and troubleshooting support to OLE and the fishermen. No services shall be billed to any NOAA or any OLE office without being specifically contracted for in writing by an authorized entity. Services shall include:

5.1. Service level, warranty, and maintenance agreements. Clarify constraints, if any, on the geographic territory, personnel availability, and escalation procedures for problem resolution covered by such services.

5.2. Facilities and procedures in place to assist the fisherman in maintaining and repairing their MTU on a 24 hour basis, including timely responses to requests, and general system service turnaround time.

5.3. Help in the determination and isolation of the cause of communications anomalies.

5.4. Assist in the resolution of communications anomalies that are traced to the MTU.

5.5. All services will be considered to be free of charge unless specifically listed in service or purchase agreements.

Section 6. Other Information

6.1. The MTU must have the durability and reliability necessary to provide acceptable service in a marine environment where the unit may be subjected to saltwater (spray) in smaller vessels, and in larger vessels where the unit may be maintained in a wheelhouse. The unit, cabling and antenna must be resistant to moisture and shock associate with the marine environments.

6.2. The MTU must comply with any additional requirements specified in the regulations for the VMS implementation for which application is made. The requestor must review the applicable NMFS rules requiring the use of VMS and respond here to any specific requirements listed therein.

6.3. All personally identifying information provided by vessels owners

or other authorized personnel for the purchase or activation of MTU or E-MTU, or for the participation in any NMFS VMS-approved fishery must be protected from unauthorized disclosure. Personally identifying information includes, but is not limited to, names, addresses, telephone numbers, social security account numbers, credit card numbers, vessel names, federal, state, and local documentation numbers, e-mail addresses, and crew lists. Any information sent electronically to the OLE must be transmitted by a secure means that prevents interception, spoofing, or viewing by unauthorized individuals. Any release of such information must be requested and approved in writing by the vessel owner, authorized personnel, or the OLE. Inadvertent or intentional unauthorized release of personally identifying information will be grounds for reconsideration and possible revocation of the type approval for any MTU supplied by the offending provider.

Dated: January 25, 2008.

Samuel D. Rauch III

Deputy Assistant Administrator for Regulatory Programs, National Marine Fisheries Service.

[FR Doc. E8-1662 Filed 1-30-08; 8:45 am]

BILLING CODE 3510-22-S

DEPARTMENT OF COMMERCE

Patent and Trademark Office

Submission for OMB Review; Comment Request

The United States Patent and Trademark Office (USPTO) will submit to the Office of Management and Budget (OMB) for clearance the following proposal for collection of information under the provisions of the Paperwork Reduction Act (44 U.S.C. Chapter 35).

Agency: United States Patent and Trademark Office (USPTO).

Title: Post Registration (Trademark Processing).

Form Number(s): PTO-1583, PTO/TM/1583, PTO-1597, PTO-1963, PTO-4.16, PTO/TM/4.16.

Agency Approval Number: 0651-0055.

Type of Request: Revision of a currently approved collection.

Burden: 21,097 hours annually, including 1,349 hours per year for Section 7 Requests.

Number of Respondents: 133,587 responses per year, including 3,800 responses per year for Section 7 Requests.

Avg. Hours Per Response: The USPTO estimates that the public will require

approximately 20 to 23 minutes (0.33 to 0.38 hours) to supply the information required for a Section 7 Request, depending upon the amount and type of information requested in a particular case.

Needs and Uses: This collection of information is required by the Trademark Act, 15 U.S.C. 1051 *et seq.*, which provides for the Federal registration of trademarks, service marks, collective trademarks and service marks, collective membership marks, and certification marks. Individuals and businesses that use or intend to use such marks in commerce may file an application to register their marks with the United States Patent and Trademark Office (USPTO). Such individuals and businesses may also submit various communications to the USPTO, including requests to correct or amend their registrations.

The USPTO is proposing to add one form to this information collection for Section 7 Requests (PTO-1597). Registrants may use a Section 7 Request to request a correction or amendment to the information appearing on the certificate of registration. Requests for changes that would result in a material alteration of the registration are not permitted under Section 7. Registrants may submit the proposed new form to the USPTO electronically through the USPTO Web site or submit the required information for the Section 7 Request to the USPTO on paper.

Affected Public: Individuals or households, businesses or other for-profits, and not-for-profit institutions.

Frequency: On occasion.

Respondent's Obligation: Required to obtain or retain benefits.

OMB Desk Officer: David Rostker, (202) 395-3897.

Copies of the above information collection proposal can be obtained by any of the following methods:

- **E-mail:** Susan.Fawcett@uspto.gov.

Include "0651-0055 copy request" in the subject line of the message.

- **Fax:** 571-273-0112, marked to the attention of Susan Fawcett.

- **Mail:** Susan K. Fawcett, Records Officer, Office of the Chief Information Officer, Customer Information Services Group, Public Information Services Division, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450.

Written comments and recommendations for the proposed information collection should be sent on or before March 3, 2008 to David Rostker, OMB Desk Officer, Room 10202, New Executive Office Building, 725 17th Street, NW., Washington, DC 20503.

Dated: January 24, 2008.

Susan K. Fawcett,

Records Officer, USPTO, Office of the Chief Information Officer, Customer Information Services Group, Public Information Services Division.

[FR Doc. E8-1727 Filed 1-30-08; 8:45 am]

BILLING CODE 3510-16-P

COMMODITY FUTURES TRADING COMMISSION

Sunshine Act Meetings

TIME AND DATE: 1 p.m., Wednesday, March 5, 2008.

PLACE: 1155 21st St., NW., Washington, DC, 9th Floor Commission Conference Room.

STATUS: Closed.

MATTERS TO BE CONSIDERED: Rule Enforcement Review.

CONTACT PERSON FOR MORE INFORMATION: Sauntia S. Warfield, 202-418-5084.

David A. Stawick,

Secretary of the Commission.

[FR Doc. 08-456 Filed 1-29-08; 1:03 pm]

BILLING CODE 6351-01-P

DEPARTMENT OF DEFENSE

Office of the Secretary

[DoD-2008-OS-0004]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary, DoD.

ACTION: Notice to amend two systems of records.

SUMMARY: The Office of the Secretary of Defense is amending two systems of records notices in its existing inventory of record systems subject to the Privacy Act of 1974, (5 U.S.C. 552a), as amended.

DATES: This proposed action will be effective without further notice on March 3, 2008, unless comments are received which result in a contrary determination.

ADDRESSES: Send comments to the OSD Privacy Act Coordinator, Records Management Section, Washington Headquarters Services, 1155 Defense Pentagon, Washington, DC 20301-1155.

FOR FURTHER INFORMATION CONTACT: Ms. Cindy Allard at (703) 588-2386.

SUPPLEMENTARY INFORMATION: The Office of the Secretary of Defense systems of records notices subject to the Privacy Act of 1974, (5 U.S.C. 552a), as amended, have been published in the

II. Method of Collection

Paper applications.

III. Data

OMB Number: 0648-0012.

Form Number: NOAA Form 88-1.

Type of Review: Regular submission.

Affected Public: Individuals or households and business or other for-profit organizations.

Estimated Number of Respondents: 1,735.

Estimated Time per Response: 8 hours.

Estimated Total Annual Burden Hours: 13,880.

Estimated Total Annual Cost to Public: \$8,050.

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: December 4, 2007.

Gwellnar Banks,

Management Analyst, Office of the Chief Information Officer.

[FR Doc. E7-23858 Filed 12-7-07; 8:45 am]

BILLING CODE 3510-22-P

DEPARTMENT OF COMMERCE**National Oceanic and Atmospheric Administration****Proposed Information Collection; Comment Request; Vessel Monitoring System Requirement for American Samoa Pelagic Longline Fishery**

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 February 8, 2008.

ADDRESSES: Direct all written comments to Diana Hynek, Departmental Paperwork Clearance Officer, Department of Commerce, Room 6625, 14th and Constitution Avenue, NW., Washington, DC 20230 (or via the Internet at 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.

SUPPLEMENTARY INFORMATION:**I. Abstract**

The commercial fishing vessels active in the American Samoa-based pelagic longline fishery that are greater than 50 feet in length overall must allow the National Marine Fisheries Service (NMFS) to install Vessel Monitoring System (VMS) units on their vessels when directed to do so by NMFS enforcement personnel. VMS units automatically send periodic reports on the position of the vessel. NMFS uses the reports to monitor the vessel's location and activities while enforcing longline fishing area closures. NMFS provide the funds for the units and messaging.

II. Method of Collection

The only information collected is vessel position reports, which are automatically transmitted via the VMS.

III. Data

OMB Number: 0648-0519.

Form Number: None.

Type of Review: Regular submission.

Affected Public: Business or other for-profits organizations.

Estimated Number of Respondents: 40.

Estimated Time per Response: 4 hours to install a VMS; 2 hours per year to maintain a VMS; 24 seconds a day to transmit hourly automated position reports from a vessel.

Estimated Total Annual Burden Hours: 193.

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: December 4, 2007.

Gwellnar Banks,

Management Analyst, Office of the Chief Information Officer.

[FR Doc. E7-23862 Filed 12-7-07; 8:45 am]

BILLING CODE 3510-22-P

DEPARTMENT OF COMMERCE**National Oceanic and Atmospheric Administration****Meeting: Climate Change Science Program (CCSP) Product Development Committee (CPDC) for Synthesis and Assessment Product 5.3**

AGENCY: Office of Oceanic and Atmospheric Research (OAR), National Oceanic and Atmospheric Administration (NOAA), Department of Commerce (DOC).

ACTION: Notice of open meeting.

SUMMARY: The Climate Change Science Program (CCSP) Product Development Committee for Synthesis and Assessment Product 5.3 (CPDC-S&A 5.3) was established by a Decision Memorandum dated October 12, 2006. CPDC-S&A 5.3 is the Federal Advisory Committee charged with responsibility to develop a draft Synthesis and Assessment Product that addresses CCSP Topic 5.3: "Decision Support Experiments and Evaluations Using Seasonal to Interannual Forecasts and Observational Data".

Place: The meeting will be held at the Southwest Center, 1052 North Highland Ave, University of Arizona, Tucson, Arizona 85721.

Time and Date: The meeting will convene at 9 a.m. on Thursday, January 10, 2008 and adjourn the afternoon of January 11, 2008. Meeting information will be available online on the CPDC-S&A 5.3 Web site (<http://www.fxsp0/climate.noaa.gov/>)