presence of cracks penetrating through the outer wall as shown in Fig. 2.

(d) Inspect coupling V-Band clamp for cracks by spreading the band segments and checking for failed spot welds and for indication of exhaust flanges bottoming in coupling V-Band (see Figure 1) and clamp bolt for bending, overstress, thread damage and cracks (see Figure 1).

(e) Inspect turbochargers and tailpipe flanges for cracks and distortion (see Figure 1). Remove all carbon deposits from mating flanges before reassembly.

(f) Inspect mating area of turbocharger exhaust flange to exhaust tailpipe connection for proper mating of surfaces.

(g) Inspect engine mount for indication of overheat, warpage, and corrosion, or rust. Repair as required.

(h) If during inspection required by paragraph (c), an internal crack is found that either exceeds the limit shown in Figure 2, View 1 or 2, or a crack penetrates the outer wall of a turbine housing as shown in Figure 2, View 3, the existing turbine housing must be removed from service and replaced with a serviceable turbine housing prior to the next flight.

(i) If during the inspections required by paragraphs (d) through (g), cracked, distored, or otherwise damaged parts, components, or assemblies are found, before further flight repair or replace with serviceable parts, components, and assemblies of the same part number.

(j) The inspections required by this AD may be discontinued when the turbine housing is replaced with a Roto-Master part number 600510-04 (TCM P/N 643931).

(k) Special flight permits may be issued in accordance with FAR 21.197 and 21.199 to operate aircraft to a base for the accomplishment of inspections required by this AD.

(l) Alternative inspections, modifications or other actions which provide an equivalent level of safety may be used when approved by the Manager, Western Aircraft Certification Field Office, FAA Northwest Mountain Region, Hawthorne, California.

Note.—Roto-Master, Inc. Service Letter Number 27, Rev. A dated September 24, 1982 refers to the above procedures.

(Secs. 313(a), 601, and 603 of the Federal Aviation Act of 1958, as amended (49 U.S.C. 1354(a), 1421, and 1423); sec. 6(c) Department of Transportation Act (49 U.S.C. 1655(c)); and sec. 1189 Federal Aviation Regulation (14 CFR 11.89))

Note.—The FAA has determined that this regulation is an emergency regulation that is not major under Section 8 of Executive Order 12291. It is impracticable for the agency to follow the procedures of Order 12291 with respect to this rule since the rule must be issued immediately to correct an unsafe condition in aircraft. It has been further determined that this document involves an emergency regulation under DOT Regulatory Policies and Procedures (44 FR 11034; February 26, 1979). If this action is subsequently determined to involve a significant regulation, a final regulatory evaluation or analysis, as appropriate, will be prepared and placed in the regulatory docket (otherwise, an evaluation is not required). A copy of it, when filed, may be obtained by contacting the person identified above under the caption **"FOR FURTHER INFORMATION CONTACT."**

Issued in Burlington, Massachusetts, on December 8, 1982.

Robert E. Whittington,

Director, New England Region.

[FR Doc. 82-34230 Filed 12-30-82; 8:45 am]

BILLING CODE 4910-13-M

CONSUMER PRODUCT SAFETY COMMISSION

16 CFR Part 1030

Revisions to Financial Interest Reporting Requirements

AGENCY: Consumer Product Safety Commission.

ACTION: Final rule.

SUMMARY: The Consumer Product Safety Commission is revising its regulations pertaining to the submission of Confidential Statements of Employment and Financial Interests by updating the list of positions whose incumbents are required to submit statements, and clarifying the requirement for annual reporting. This is being done to reflect recent changes in the Commission's organizational structure, and to include certain data processing and contract personnel.

EFFECTIVE DATE: January 3, 1983.

FOR FURTHER INFORMATION CONTACT: Joseph F. Rosenthal, Office of General Counsel, Consumer Product Safety Commission, Washington, D.C. 20207, Telephone (301) 492-6980.

SUPPLEMENTARY INFORMATION: Subpart F of Part 1030 of Title 16 of the Code of Federal Regulations contains the Commission's regulations regarding the submission of Confidential Statement of Employment and Financial Interests (CPSC Form 219). The statements are used to ascertain possible employee conflicts of interest. Submission of these forms by employees in positions such that their individual decisions could have an economic impact on private enterprises is mandated by Executive Order 11222 and regulations promulgated by the Office of Personnel Management. The actual list of such positions has been located in an Appendix at the end of Part 1030, printed several pages from Subpart F in the Code of Federal Regulations.

The list of positions required to submit Confidential Statements of Employment and Financial Interests has been revised to reflect recent changes in the Commission's organizational structure, and has been made a section of Subpart F itself so that it will be physically contiguous to the applicable regulations. Only minor substantive changes have been made in the grades required to report, but the list has been simplified by omitting position classification schedule numbers, and by defining the reporting positions in certain organizations as Merit Pay positions. Merit Pay employees are those in grades 13–15 with managerial or supervisory authority.

The list has also been revised in two other respects. All contract specialists at grade 7 and above in the Directorate for Administration are now required to report because their role in supervising contracts and selecting contractors makes them susceptible to conflicts of interest. Also, certain data processing positions at grade 7 and above which are sufficiently sensitive, under Office of Personnel Management regulations, to require background checks have been added to the list because they have the opportunity to manipulate critical data which underlies the Commission's decision making processes.

Section 1031.602 has been revised to give the Ethics Counselor the primary responsibility for determining which positions should be subject to the reporting requirement. Previously, the Executive Director had this responsibility.

Section 1030.604 has been revised to indicate that senior employees subject to the financial reporting requirements of the Ethics in Government Act are not also subject to the reporting requirements of Subpart F.

Sections 1030.605 and 1060.606 have been simplified and combined to specifically indicate when submissions are due, and to inform employees that they may be subject to disciplinary action for failing to report as required.

Since this rule relates solely to internal agency management, pursuant to 5 U.S.C. 553 the Commission finds that notice and other public procedures with respect to this rule are impractical and contrary to the public interest, and good cause is found for making this rule effective less than 30 days after publication in the **Federal Register.** Further, this action is not a rule as defined in the Regulatory Flexibility Act, 5 U.S.C. 601–612, and thus is exempt from the provisions of that act.

List of Subjects in 16 CFR Part 1030

Government employees and conflict of interest

PART 1030—[AMENDED]

Accordingly, Part 1030 of Title 16 of the Code of Federal Regulations is amended as shown.

1. The authority citation for Part 1030 is as follows:

Authority: E.O. 11222, 30 FR 6469, 3 CFR 1964–1965 Comp., p. 306; 5 CFR Part 735; Pub. L. 95–521, 92 Stat. 1824, as amended by Pub. L. 96–19, 93 Stat. 37 (5 U.S.C. App.).

§ 1030.601 [Amended]

2. Section 1030.601 is amended by removing the words "Appendix E" and inserting, in their place, "§ 1030.611".

3. Section 1030.602 is revised to read as follows:

§ 1030.602 Inclusion or removal of positions.

The Ethics Counselor shall, in accordance with the criteria in § 1030.601 and after consultation with the Executive Director, identify positions to be added to or removed from the listing in § 1030.611.

4. Section 1030.604 is revised to read as follows:

§ 1030.604 Employees not required to submit statements.

(a) Employees in positions that meet the criteria of § 1030.601, as listed in § 1030.611, may be excluded from the reporting requirement when the Ethics Counselor determines that:

(1) The duties of a position are at such a level of responsibility that the submission of a statement of employment and financial interests by the incumbent is not necessary because of the degree of supervision and review over the incumbent; or

(2) The duties of a position are such that the likelihood of the incumbent's involvement in a conflict of interest situation is remote.

(b) Exclusions under this provision must be documented in writing and retained by the Ethics Counselor.

(c) Employees subject to the more detailed financial reporting requirements of Title II of the Ethics in Government Act of 1978 (Pub. L. 95–521, 5 U.S.C. Appendix), are excluded from the reporting requirements of this subpart.

5. Section 1030.605 is revised to read as follows:

§ 1030.605 Submission of statements.

(a) An employee required to submit a statement of employment and financial interests under this Subpart shall submit that statement to the Ethics Counselor not later than:

(1) Thirty days after appointment or assignment to a position covered by section 1030.611; and

(2) By June 30 of each succeeding year.

(b) Employees failing to submit a statement in accordance with this section may be subject to disciplinary action.

(c) Notwithstanding the filing of the statements required by this section, each employee shall at all times avoid acquiring a financial interest that could result, or taking an action that would result, in a violation of the conflict-of-interest provisions of 18 U.S.C. 208 or this part.

§ 1030.606 [Removed]

6. Section 1030.606 is removed.

7. A new § 1030.611 is added, to read as follows:

§ 1030.611 Positions requiring submission of statement of employment and finanical interests.

(a) *Commissioners' staffs.* All positions grade 13 and above.

(b) *Office of the General Counsel.* All positions grade 11 and above.

(c) *Office of Congressional Relations.* All positions grade 15 and above.

(d) *Office of Public Affairs.* All positions grade 14 and above.

(e) *Office of the Secretary.* All positions grade 13 and above.

(f) *Office of Internal Audit.* All positions grade 14 and above.

(g) *Office of Equal Employment Opportunity and Minority Enterprise.* All positions grade 15 and above.

(h) *Office of the Executive Director.* All Merit Pay positions.

(i) *Office of Program Management.* All Merit Pay positions.

(j) *Office of Budget, Program Planning and Evaluation.* All positions grade 15 and above.

(k) *Office of Outreach Coordination.* All positions grade 13 and above.

(l) *Directorate for Epidemiology.* All Merit Pay positions and all Physiologists grade 11 and above, all Engineering Psychologists grade 11 and above, all Statisticians grade 11 and above, and all Program Analysts grade 12 and above.

(m) *Directorate for Economics.* All positions grade 12 and above.

(n) *Directorate for Engineering Sciences.* All Merit Pay positions.

(o) *Directorate for Health Sciences.* All positions grade 11 and above.

(p) *Directorate for Compliance and Administrative Litigation.* All positions grade 11 and above.

(q) *Directorate for Administration.* All Merit Pay positions and all Contract Specialists grade 7 and above.

(r) *Regional Offices.* All investigative positions grade 5 and above; all other positions grade 13 and above.

(s) *Computer-related positions.* All CPSC computer-related positions grade 9 and above classifiable as ADP–I or ADP–II under Chapter 732 of the Federal Personnel Manual, regardless of organizational unit.

Appendix E—[Removed]

8. Appendix E is removed.

Dated: December 23, 1982.

Sadye E. Dunn,

Secretary, Consumer Product Safety Commission.

[FR Doc. 82-35324 Filed 12-30-82; 8:45 am]

BILLING CODE 6355-01-M

---

16 CFR Parts 1500 and 1507

Additions of Cross-Reference Notations to Certain Regulations

AGENCY: Consumer Product Safety Commission.

ACTION: Addition of cross-reference notations.

SUMMARY: The Commission is adding to certain regulations under the Federal Hazardous Substances Act cross references to separate provisions that relate to the regulations. The purpose of the cross references is to help users of the Code of Federal Regulations be aware of all relevant provisions on a particular subject.

DATE: The notations are effective on January 3, 1983.

FOR FURTHER INFORMATION CONTACT: Christine Nelson or Paul Galvydis (on fireworks provisions), Directorate for Compliance and Administrative Litigation, Consumer Product Safety Commission, Washington, D.C. 20207; telephone (301) 492–6400.

SUPPLEMENTARY INFORMATION: A number of regulations issued under the Federal Hazardous Substances Act ban, or require labeling for, certain household products. These regulations are codified in the Code of Federal Regulations (CFR) at Chapter II, Subchapter C, Part 1500 of Title 16.

Other provisions in the CFR exempt some of these household products from the banning and labeling regulations cited above, and still other provisions clarify or relate to the regulations. Because the related provisions appear separately in the CFR, a person interested in an affected product might refer to an applicable regulation without realizing that an exemption or clarification also exists. Therefore, the Commission is adding to the regulations bracketed notations that reference a user of the CFR to related provisions.

The new notations are merely nonsubstantive cross references, and not rules or amendments. Therefore,

neither the general notice of proposed rulemaking nor the delayed effective date requirements of the Administrative Procedure Act apply. 5 U.S.C. 553.

List of Subjects

Consumer protection, Labeling.

Pursuant to section 10(a) of the Federal Hazardous Substances Act, 15 U.S.C. 1269(a), the following cross-reference notations are added to the following sections of Title 16, Chapter II, Subchapter C of the Code of Federal Regulations (in each case the notation shall be inserted at the end of the listed Part, section, or paragraph):

Regulation	Notation
1500.14(b)(7)	[See also 1500.17(a) (3), (8) and (9); 1500.83(a)(27); 1500.85(a)(2); and Part 1507].
1500.17(a)(3)	[See also 1500.14(b)(7); 1500.17(a) (8) and (9); 1500.83(a)(27); 1500.85(a)(2); and Part 1507].
1500.17(a)(8)	[See also 1500.17(a) (3) and (9)].
1500.17(a)(9)	[See also 1500.17(a) (3) and (8)].
1500.18(a)(1)	[But see 1500.86(a)(1)].
1500.18(a)(3)	[But see 1500.86(a)(2)] [See also 1500.48 and 1500.49].
1500.18(a)(4)	[But see 1500.86(a)(3)].
1500.18(a)(6)	[But see 1500.86(a)(4)].
1500.18(a)(7)	[But see 1500.86(a)(5)].
1500.83(a)(27)	[See also 1500.14(b)(7); 1500.17(a) (3), (8) and (9); 1500.85(a)(2); and Part 1507].
1500.85(a)(2)	[See also 1500.14(b)(7); 1500.17(a) (3), (8) and (9); and Part 1507].
Part 1507	[See also 1500.14(b)(7); 1500.17(a) (3), (8) and (9); 1500.83(a)(27) and 1500.85(a)(2)].

Effective date: The notations shall be effective on January 3, 1983.

15 U.S.C. 1269(a)

Dated: December 23, 1982.

Sadye E. Dunn,

Secretary, Consumer Product Safety Commission.

[FR Doc. 83-35322 Filed 12-30-82; 8:45 am]

BILLING CODE 6355-01-M

DEPARTMENT OF THE TREASURY

Office of the Secretary

31 CFR Part 2

National Security Information

AGENCY: Treasury.

ACTION: Final rule.

SUMMARY: This regulation supersedes the Department's regulation at 31 CFR Part 2 which was published at 43 FR 60448, December 28, 1978. This regulation implements Executive Order No. 12356, 47 FR 14874, April 6, 1982, (hereinafter referred to as the Order), and the Information Security Oversight Office Directive, 47 FR 27836, June 25, 1982, (hereinafter referred to as the Directive), which prescribe a uniform system for the classification, downgrading, declassification and safeguarding of national security information. The Order will facilitate the public's access to information about the affairs of government when disclosure would not damage national security. The Order also expressly prohibits the use of the classification system to conceal violations of law, prevent embarrassment, or delay the release of information that does not require protection.

EFFECTIVE DATE: August 1, 1982.

FOR FURTHER INFORMATION CONTACT: Dennis E. Southern, Office of Physical Security, Office of Administrative Programs, Department of the Treasury, Washington, D.C. 20220 (202) 376-0823.

SUPPLEMENTARY INFORMATION: The sections in this regulation follow the format of the Directive. This regulation has been submitted to the Information Security Oversight Office in accordance with § 5.2(b)(3) of the Order.

The Department of the Treasury has determined that this regulation is not a major regulation for purposes of Executive Order 12291, February 17, 1981. Accordingly, a regulatory impact analysis is not required. Additionally, as this regulation is a rule of "agency organization, procedure or practice," notice and public procedure respecting this regulation is not deemed necessary or appropriate under 5 U.S.C. 553(b)(A). Because this regulation is being issued without notice of proposed rulemaking, the provisions of the Regulatory Flexibility Act, 5 U.S.C. 601-612, do not apply.

List of Subjects in 31 CFR Part 2

Archives and records, Authority delegations, Classified information, Executive orders, Freedom of information, Information, Intelligence, National defense, National security information, Presidential documents, Security information, Security measures.

Title 31 of the Code of Federal Regulations, Part 2, is revised to read as follows:

PART 2—NATIONAL SECURITY INFORMATION

Subpart A—Original Classification

Subpart B—Derivative Classification

Subpart C—Downgrading and Declassification

Subpart D—Safeguarding

Subpart E—Implementation and Review

Subpart F—General Provisions

Authority: Executive Order 12356.

Subpart A—Original Classification

§ 2.1 Classification levels.

(a) National security information (hereinafter also referred to as "classified information") shall be classified at one of the following three levels:

(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

(b) *Limitations [1.1(b)]*[1]. Markings other than "Top Secret," and "Confidential," such as "For Official Use Only" or "Limited Official Use," shall not be used to identify national security information. No other term or phrase shall be used in conjunction with these markings, such as "Secret Sensitive" or "Agency Confidential," to identify national security information. The terms "Top Secret," "Secret," and "Confidenatial" should not be used to identify non-classified Executive Branch information.

(c) *Reasonable Doubt [1.1(c)]*. When there is reasonable doubt the need to classify information, the information shall be safeguarded as if it were "Confidential" information in accordance with Subpart D, of this regulation, pending a determination about its classification. Upon a determination of a need for classification, the information that is classified shall be marked as provided in § 2.7. When there is reasonable doubt about the appropriate classification level, the information shall be safeguarded at the higher level in accordance with Subpart D, pending a determination of its classification level. Upon a determination of its classification level, the information shall be marked as provided in § 2.7.

§ 2.2 Classification authority.

(a) The authority to originally classify national security information as Top Secret, Secret or Confidential within the Department of the Treasury may be exercised by the Deputy Secretary, the Under Secretary (Monetary Affairs), the Under Secretary (Tax and Economic Affairs), the General Counsel, the Assistant Secretary (International Affairs), the Treasurer of the United States, the Fiscal Assistant Secretary, the Assistant Secretary (Administration), the Assistant Secretary (Legislative Affairs), the Assistant Secretary (Enforcement and Operations), the two Executive Assistants to the Secretary, the Executive Assistant to the Deputy Secretary, the Executive Secretary, the Special Assistant to the Secretary (National Security) and the Deputy (Security Affairs and Crisis Management) to the Assistant Secretary (Enforcement and Operations). The authority inheres in the office and may be exercised by a person acting in that office. These officials, with the exception of the Assistant Secretary (Administration), are not authorized to delegate authority to classify information as Top Secret, but may delegate authority to classify information as Secret and Confidential.

(b) The authority to originally classify national security information as Secret or Confidential within the Department of the Treasury may be exercised by the the Assistant Secretary (Tax Policy); Commissioner, Internal Revenue Service; the Director, Bureau of Alcohol, Tobacco and Firearms; the Commissioner, U.S. Customs Service; the Director, Bureau of Engraving and Printing; and the Director, U.S. Secret Service. This authority is not redelegable.

(c) The authority to originally classify national security information as Confidential within the Department of the Treasury may be exercised by the Assistant Secretary (Domestic Finance); the Assistant Secretary (Economic Policy); the Assistant Secretary (Public Affairs); the Inspector General; the Comptroller of the Currency; the Commissioner, Bureau of Government Financial Operations; the Commissioner, Bureau of the Public Debt; and the Director, Bureau of the Mint. Officials authorized to classify information as Confidential cannot redelegate such authority.

§ 2.3 Listing classification authorities.

Delegations of original Top Secret, Secret and Confidential classification authority shall be in writing and shall be reported in writing to the Assistant Secretary (Administration). These delegations shall be limited to the minimum number absolutely required for efficient administration. Periodic reviews of such delegations shall be made to ensure that the officials so designated have demonstrated a continuing need to exercise such authority.

§ 2.4 Record requirements.

The Assistant Secretary (Administration) shall maintain a listing by name, position title and authorized classification level of the officials in the Office of the Secretary who are authorized under this regulation to originally classify information as Top Secret, Secret or Confidential. Officials within the Office of the Secretary with Top Secret classification authority shall report in writing on TD F 71–01.14 (Report of Authorized Classifiers) to the Assistant Secretary (Administration) the names, position titles and authorized classification levels of the officials designated by them in writing to have original Top Secret, Secret and Confidential classification authority. The head of each bureau shall maintain a similar listing of the officials in his/her bureau authorized to apply original Secret and Confidential classification and shall furnish a copy of TD F 71–01.14 to the Assistant Secretary (Administration). This listing shall be compiled as of October 1, 1983, and updated no less than annually.

§ 2.5 Classification categories.

(a) *Classification in Context of Related Information [1.3(b)]*. Certain information which would otherwise be unclassified may require classification when combined or associated with other unclassified or classified information. Classification on this basis shall be supported by a written explanation that, at a minimum, shall be maintained with the file or referenced on the record copy of the information.

(b) *Unofficial Publication or Disclosure [1.3.(d)]*. Following an inadvertent or unauthorized publication or disclosure of information identical or similar to information that has been classified in accordance with the Order or predecessor orders, the agency of primary interest shall determine the degree of damage to the national security, the need for continued classification, and, in coordination with the agency in which the disclosure occurred, what action must be taken to prevent similar occurrences.

§ 2.6 Duration of classification.

(a) *Information Not Marked for Declassification [1.4]*. Information classified under predecessor orders that is not subject to automatic declassification shall remain classified until reviewed for declassification.

(b) *Authority to Extend Automatic Declassification Determinations [1.4(b)]*. The authority to extend the classification of information subject to automatic declassification under predecessor orders is limited to those officials who have classification authority over the information and are designated in writing to have original classification authority at the level of the information to remain classified. Any decision to extend this classification on other than a document-by-document basis shall be reported to the Assistant Secretary (Administration) who shall, in turn, report this fact to the Director of the Information Security Oversight Office.

§ 2.7 Identification and markings [1.5 (a), (b) and (c)].

A uniform information security system requires that standard markings be applied to classified information. Except in extraordinary circumstances as provided in § 1.5(a) of the Order, or as

[1] Bracketed references are to related sections of Executive Order 12356.

indicated herein, the marking of paper documents created after the effective date of the Order shall not deviate from the following prescribed formats. These markings shall also be affixed to material other than paper documents, including film, tape, etc., or the originator shall provide holders or recipients of the information with written instructions for protecting the information.

(a) *Classification Level.* The markiings "Top Secret," "Secret," and "Confidential" are used to indicate: information that requires protection as classified information under the Order; the highest level of classification contained in a document; and the classification level of each page and, in abbreviated form, each portion of a document.

(1) *Overall Marketing.* The highest level of classification of information in a document shall be marked in such a way as to distinguish it clearly from the informational text. These markings shall appear at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first and last pages, and on the outside of the back cover (if any).

(2) *Page Marking.* Each interior page of a classified document shall be marked at the top and bottom either according to the highest classification of the content of the page, including the designation "UNCLASSIFIED" when it is applicable, or with the highest overall classification of the document.

(3) *Portion Marking.* The Secretary of the Treasury may waive the portion marking requirement for specified classes of documents or information only upon a written determination that:

(i) There will be minimal circulation of the specified documents or information and minimal potential usage of these documents or information as a source for derivative classification determinations; or

(ii) There is some other basis to conclude that the potential benefits of portion marking are clearly outweighed by the increased administrative burdens.

(b) Unless the portion marking requirement has been waived as authorized, each portion of a document, including subjects and titles, shall be marked by placing a parenthetical designation immediately preceding the text to which it applies. The symbols "(TS)" for Top Secret, "(S)" for Secret, "(C)" for Confidential, and "(U)" for Unclassified shall be used for this purpose. If the application of parenthetical designations is not practicable, the document shall contain a statement sufficient to identify the information that is classified and the level of such classification, as well as the information that is not classified. If all portions of a document are classified at the same level, this fact may be indicated by a statement to that effect. If a subject or title requires classification, an unclassified identifier may be applied to facilitate reference.

(c) *Classification Authority.* If the original classifier is other than the signer or approver of the document, the identity shall be shown as follows: "CLASSIFIED BY (identification of original classification authority)".

(d) *Bureau and Office of Origin.* If the identity of the originating bureau and office is not apparent on the face of a document, it shall be placed below the "CLASSIFIED BY" line.

(e) *Downgrading and Declassification Instructions.* Downgrading and, as applicable, declassification instructions shall be shown as follows:

(1) For information to be declassified automatically on a specific date:

Classified by———
Office———
Declassify on (date) ———

(2) For information to be declassified automatically upon occurrence of a specific event:

Classified by———
Office———
Declassify on (description of event) ———

(3) For information not to be declassified automatically:

Classified by———
Office———
Declassify on Originating Agency's Determination Required or "OADR"———

(4) For information to be downgraded automatically on a specific date or upon occurrence of a specific event:

Classified by———
Office———
Downgrade to ———
on (date or description of event) ———

(f) *Special Markings.*—(1) *Transmittal Documents [1.5(c)].* A transmittal document shall indicate on its face and on the last page, if any, the highest classification of any information transmitted by it. It shall also include the following or similar instruction:

(i) For an unclassified transmittal document:

Unclassified When Classified Enclosure(s) Removed

(ii) For a classified transmittal document:

Upon Removal of Attachment(s) This Document is (classification level of the transmittal document standing alone)——

(2) *Restricted Data or Formerly Restricted Data [6.2(a)].* Restricted Data or Formerly Restricted Data information shall be marked in accordance with regulations issued under the Atomic Energy Act of 1954, as amended.

(3) *Intelligence Sources or Methods [1.5(c)].* Documents that contain information relating to intelligence sources or methods shall include the following marking unless otherwise proscribed by the Director of Central Intelligence:

"WARNING NOTICE—INTELLIGENCE SOURCES OR METHODS INVOLVED"

(4) *Foreign Government Information (FGI) [1.5(c)].* Documents that contain FGI shall include either the marking "FOREIGN GOVERNMENT INFORMATION," or a marking that otherwise indicates that the information is foreign government information. If the information is foreign government information that must be concealed, the marking shall not be used and the document shall be marked as if it were wholly of U.S. origin. However, such a marking must be supported by a written explanation that, at a minimum, shall be maintained with the file or referenced on the original record copy of the document or information.

(5) *National Security Information [4.1(c)].* Classified information furnished outside the Executive Branch shall show the following marking:

NATIONAL SECURITY INFORMATION

Unauthorized Disclosure Subject to Administrative and Criminal Sanctions

(6) *Computer Output [1.5(c)].* Documents that are generated as computer output may be marked automatically by systems software. If automatic marking is not practicable, such documents must be marked manually.

(g) *Electrically Transmitted Information (messages) [1.5(c)].* Classified information that is transmitted electrically shall be marked as follows:

(1) The highest level of classification shall appear before the first line of text;

(2) A "CLASSIFIED BY" line is not required;

(3) The duration of classification shall appear as follows:

(i) For information to be declassified automatically on a specific date: "DECL: (date)"

(ii) For information to be declassified upon occurrence of a specific event: "DECL: (description of event)"

(iii) For information not to be automatically declassified which

requires the originating agency's determination (see also § 2.7(e)(3)): "DECL: OADR"

(iv) For information to be automatically downgraded: "DNG (abbreviation of classification level to which the information is to be downgraded and date or description of event on which downgrading is to occur)"

(4) Portion marking shall be as prescribed in § 2.7(a)(3);

(5) Special markings as prescribed in § 2.7(f) (2), (3) and (4) shall appear after the marking for the highest level of classification. These include:

(i) Restricted Data or Formerly Restricted Data: Electrically transmitted information containing Restricted Data or Formerly Restricted Data shall be marked in accordance with regulations issued under the Atomic Energy Act of 1954, as amended;

(ii) Information concerning intelligence sources or methods: "WNINTEL," unless proscribed by the Director of Central Intelligence;

(iii) *Foreign Government Information:* "FGI," or a marking that otherwise indicates that the information is foreign government information. If the information is foreign government information that must be concealed, the marking shall not be used and the document shall be marked as if it were wholly of U.S. origin. However, such a marking must be supported by a written explanation that, at a minimum, shall be maintained with the file or referenced on the original or record copy of the document or information.

(6) Paper copies of electrically transmitted messages shall be marked as provided in § 2.7(a) (1) and(2).

(h) *Changes in Classification Markings [4.1(b)].* When a change is made in the duration of classified information, all holders of record shall be promptly notified. If practicable, holders of record shall also be notified of a change in the level of classification. Holders shall alter the markings to conform to the change, citing the authority for it. If the remarking of large quantities of information is unduly burdensome, the holder may attach a change of classification notice to the storage unit in lieu of the marking action otherwise required. Items withdrawn from the collection for purposes other than transfer for storage shall be marked promptly in accordance with the change notice.

§ 2.8 Limitations on classification [1.6(c)].

Before reclassifying information as provided in § 1.6(c) of the Order, the authorized official shall consider the following factors, which shall be addressed in a report to the Assistant Secretary (Administration) who shall in turn forward a report to the Director of the Information Security Oversight Office:

(a) The elasped time following disclosure;

(b) The nature and extent of disclosure;

(c) The ability to bring the fact of reclassification to the attention of persons to whom the information was disclosed;

(d) The ability to prevent further disclosure; and

(e) The ability to retrieve the information voluntarily from persons not authorized access in its reclassified state.

Subpart B—Derivative Classification

§ 2.9 Use of derivative classification [2.1].

The application of derivative classification markings is a responsibility of those who incorporate, paraphrase, restate, or generate in new form information that is already classified, and of those who apply markings in accordance with instructions from an authorized original classifier or in accordance with an authorized classification guide. If a person who applies derivative classification markings believes that the paraphrasing, restating or summarizing of classified information has changed the level of or removed the basis for classification, that person must consult an appropriate official of the originating agency or office of origin who has the authority to upgrade, downgrade or declassify the information for a determination. A sample marking documents is set forth in § 2.11.

§ 2.10 Classification guides.

(a) *General [2.2(a)].* A classification guide is a reference manual which assists document drafters and document classifiers in determining what types or categories of material have already been classified. The classification guide shall, at a minimum:

(1) Identify or categorize the elements of information to be protected;

(2) State which classification level applies to each element or category of information; and

(3) Prescribe declassification instructions for each element or category of information in terms of (i) a period of time, (ii) the occurrence of an event, or (iii) a notation that the information shall not be declassified automatically without the approval of the originating agency.

(b) *Review and Record Requirements [2.2(a)].* (1) Each classification guide shall be kept current and shall be reviewed at least once every two years and updated as necessary. Each office within the Office of the Secretary and the respective offices of each Treasury bureau possessing original classification authority for national security information shall maintain a list of all classification guides in current use by them. A copy of each such classification guide in current use shall be furnished to the Assistant Secretary (Administration).

(2) Each office that prepares and maintains a classification guide shall also maintain a record, copy to the Assistant Secretary (Administration), of individuals authorized to apply derivative classification markings in accordance with a classification guide. This record shall be maintained on TD F 71-01.18 (Report of Authorized Derivative Classifiers).

(c) *Waivers [2.2(c)].* Any authorized official desiring a waiver of the requirement to issue a classification guide shall submit in writing to the Assistant Secretary (Administration) a request for approval of such a waiver. Any request for such a waiver shall contain, at a minimum, an evaluation of the following factors:

(1) The ability to segregate and describe the elements of information;

(2) The practicality of producing or disseminating the guide because of the nature of the information;

(3) The anitcipated usage of the guide as a basis for derivative classification; and

(4) The availability of alternative sources for derivatively classifying the information in a uniform manner.

§ 2.11 Derivative identification and markings [1.5(c) and 2.1(b)].

Documents classified derivatively on the basis of source documents or classification guides shall bear all markings prescribed in § 2.7(a) through (f), as are applicable. Information for these markings shall be taken from the source document or instructions in the appropriate classification guide.

(a) *Classification Authority.* The authority for classification shall be shown as follows:

Derivatively Class by _____
Office _____
Derived from _____
Declassify on _____

If a document is classified on the basis of more than one source document or classification guide, the authority for classification shall be shown on the "DERIVED FROM" line as follows:

"CLASSIFIED BY MULTIPLE SOURCES"

In these cases, the derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document. A document derivatively classified on the basis of a source document that is marked "CLASSIFIED BY MULTIPLE SOURCES" shall cite the source document on its "DERIVED FROM" line rather than the term "MULTIPLE SOURCES."

(b) *Downgrading and Declassification Instructions.* Dates or events for automatic downgrading or declassification, or the notation "ORIGINATING AGENCY's DETERMINATION REQUIRED" to indicate that the document is not to be downgraded or declassified automatically, shall be carried forward from the source document, or as directed by a classification guide, and shown on a "DOWNGRADE TO" or "DECLASSIFY ON" line as follows:

"DOWNGRADE TO _____
ON (date; description of event; or 'ORIGINATING AGENCY'S DETERMINATION REQUIRED' (OADR))" "DECLASSIFY ON: *(date; description of* _____
event; or 'ORIGINATING AGENCY'S DETERMINATION REQUIRED' (OADR))"

Subpart C—Downgrading and Declassification

§ 2.12 Listing of downgrading and declassification authorities [3.1(b)].

Downgrading and declassification authority may be exercised by the official authorizing the original classification, if that official is still serving in the same position; a successor in that capacity; a supervisory official of either; or officials delegated such authority in writing by the Secretary or the Assistant Secretary (Administration). A listing of officials delegated such authority in writing shall be maintained on TD F 71-01.11 (Report of Authorized Downgrading and Declassification Authorities). Current listings of these officials shall be maintained by Treasury bureaus and offices within the Office of the Secretary. Copies of these listings shall be provided to the Assistant Secretary (Administration). If possible, these listings shall be unclassified.

§ 2.13 Declassification policy [3.1].

In making determinations under § 3.1(a) of the Order, officials shall respect the intent of the Order to protect foreign government information and confidential foreign sources.

§ 2.14 Downgrading and declassification markings.

Whenever a change is made in the original classification or in the dates of downgrading or declassification of any classified information, it shall be promptly and conspicuously marked to indicate the change, the authority for the action, the date of the action, and the identity of the person taking the action. Earlier classification markings shall be cancelled when practicable.

§ 2.15 Systematic review for declassification [3.3].

(a) *Permanent Records.* Systematic review is applicable only to those classified records and presidential papers or records that the Archivist of the United States, acting under the Federal Records Act, has determined to be of sufficient historical or other value to warrant permanent retention.

(b) *Non-Permanent Classified Records.* Non-permanent classified records shall be disposed of in accordance with schedules approved by the Administrator of General Services under the Records Disposal Act. These schedules shall provide for the continued retention of records subject to an ongoing mandatory declassification review request.

(c) *Systematic Declassification Review Guidelines [3.3(a)].* The Department, by February 1, 1983, shall:

(1) Issue guidelines for systematic declassification review, in consultation with the Archivist and the Director of the Information Security Oversight Office, to assist the Archivist in the conduct of systematic reviews;

(2) Designate experienced personnel to assist the Archivist in the systematic review process;

(3) Review and update systematic review guidelines at least every five years unless earlier review is requested by the Archivist.

(d) *Foreign Government Systematic Declassification Review Guidelines [3.3(a)].* By February 1, 1983, the Director of the Information Security Oversight Office shall issue, in consultation with the Archivist, the Department and other agencies having declassification authority over the information, guidelines for the systematic declassification review of foreign government information. These guidelines shall be reviewed and updated every five years unless earlier review is requested by the Archivist.

(e) *Special Procedures.* The Department shall be bound by the special procedures for systematic review of classified cryptologic records and classified records pertaining to intelligence activities (including special activities), or intelligence sources or methods issued by the Secretary of Defense and the Director of Central Intelligence, respectively.

§ 2.16 Procedures for mandatory declassification review [3.4].

(a) Except as provided by § 3.4(b) of the Order, all information classified by the Department under the Order or predecessor orders shall be subject to declassification review by the Department, if:

(1) The request is made by a United States citizen or permanent resident alien, a Federal agency, or a state or local government;

(2) The request describes the document or material containing the information with sufficient specificity to enable the Department to locate it with a reasonable amount of effort; and

(3) The requester provides substantial proof as to their U.S. citizenship or status as a permanent resident alien, e.g., a copy of a birth certificate, a certificate of naturalization, official passport or some other means of identity which would sufficiently describe the requester's status.

(b) *Processing.*—(1) *Initial Requests for Classified Records Originated by the Department.* Requests for mandatory declassification review shall be directed to the Office of Physical Security, Office of Administrative Programs. Upon each request for declassification, pursuant to § 3.4 of the Order, the following procedures shall apply:

(i) The Office of Physical Security, Office of Administrative Programs, shall acknowledge in writing receipt of the request.

(ii) A valid mandatory declassification review request need not identify the requested information by date or title of the responsive records, but must be of sufficient particularity to allow Treasury personnel to locate the records containing the information sought with a reasonable amount of effort. Whenever a request does not reasonably describe the information sought, the requester shall be notified that unless additional information is provided or the scope of the request is narrowed, no further action will be undertaken.

(iii) The Office of Physical Security, Office of Administrative Programs, shall determine the appropriate office to take action on the request and shall forward the request to that office.

(iv) Department responses to mandatory declassification review requests shall be governed by the amount of search and review time required to process the request. In responding to mandatory declassification review requests, the appropriate offical shall make a prompt declassification determination. The Office of Physical Security, Office of Administrative Programs, shall notify

the requester if additional time is needed to process the request. The Department shall make a final determination within one year from the date of receipt except in unusual circumstances. When information cannot be declassified in its entirety, reasonable efforts, consistent with other applicable laws, will be made to release those declassified portions of the requested information which constitute a coherent segment. Upon the denial or partial denial of an initial request, the Department shall also notify the requester of the right of an administrative appeal which must be filed with the Assistant Secretary (Administration) within 60 days of receipt of the denial.

(v) When the Department receives a mandatory declassification review request for records in its possession that were originated by another agency, the Office of Physical Security, Office of Administrative Programs, shall forward the request to that agency. The Office of Physical Security, Office of Administrative Programs, shall include a copy of the records requested together with the Department's recommendations for action. Upon receipt, the originating agency shall process the request in accordance with § 2001.32(a)(2)(i) of the Directive. Upon request, the originating agency shall communicate its declassification determination to Treasury.

(vi) When another agency forwards to the Department a request for information in that agency's custody that has been classified by Treasury, the Office of Physical Security, Office of Administrative Programs, shall:

(A) Advise the other agency as to whether they can notify the requester of the referral;

(B) Review the classified information in coordination with other agencies that have a direct interest in the subject matter; and

(C) Respond to the requester in accordance with the procedures in § 2.16(b)(1)(iv). If requested, Treasury's determination shall be communicated to the referring agency.

(vii) Appeals of denials of a request for declassification shall be referred to the Assistant Secretary (Administration) who shall normally make a determination within 30 working days following the receipt of an appeal. If additional time is required to make a determination, the Assistant Secretary (Administration) shall notify the requester of the additional time needed and provide the requester with the reason for the extension. The Assistant Secretary (Administration) shall notify the requester in writing of the final determination and of the reasons for any denial.

(viii) Except as provided in this paragraph, the Department shall process mandatory declassification review requests for classified records containing foreign government information in accordance with § 2.16(a). The agency that initially received or classified the foreign government information shall be responsible for making a declassification determination after consultation with concerned agencies. If upon receipt of the request, the Department determines that Treasury is not the agency that received or classified the foreign government information, it shall refer the request to the appropriate agency for action. Consultation with the foreign originator through appropriate channels may be necessary prior to final action on the request.

(ix) Mandatory declassification review requests for cryptologic information and information concerning intelligence activities (including special activities) or intelligence sources or methods shall be processed solely in accordance with special procedures issued by the Secretary of Defense and the Director of Central Intelligence, respectively.

(x) The fees to be charged for mandatory declassification review requests shall be for search, review and duplication. The fee charges for services of Treasury personnel involved in locating and reviewing records shall be at the rate of a GS-10, Step 1, for each hour or fraction thereof, except that no charge shall be imposed for search and/or review consuming less than one hour.

(A) Photocopies per page up to 8½" by 14" shall be $0.10 except that no charge will be imposed for reproducing 10 pages or less when search and/or review time requires less than one hour.

(B) When it is estimated that the costs associated with the mandatory declassification review request will exceed $100.00, the requester will be notified and requested to agree, in writing, to pay the actual charges. In the event the requester does not agree to pay the actual charges, the requester shall advise how to proceed with the mandatory declassification review request. Failure of a requester to pay charges after billing will result in future requests not being honored.

(C) A requester's initial request shall be accompanied by a statement that the requester is agreeable to paying fees for search, review and copying.

(D) Payment of fees shall be made by check or money order payable to the Treasurer of the United States.

§ 2.17 Assistance to the Department of State [3.3(b)].

The Secretary of the Treasury and other agency heads should assist the Department of State in its preparation of the *Foreign Relations of the United States* (FRUS) series by facilitating access to appropriate classified material in their custody and by expediting declassification review of documents proposed for inclusion in the FRUS.

§ 2.18 FOIA and Privacy Act Requests [3.4].

The Department of the Treasury shall process requests for declassification that are submitted under the provisions of the Freedom of Information Act, as amended, or the Privacy Act of 1974, in accordance with the provisions of those Acts.

Subpart D—Safeguarding

§ 2.19 General [4.1].

Information classified pursuant to this Order or predecessor orders shall be afforded a level of protection against unauthorized disclosure commensurate with its level of classification.

§ 2.20 General restrictions on access [4.1].

(a) *Determination of Need-To-Know.* Classified information shall be made available to a person only when the possessor of the classified information establishes in each instance, except as provided in § 4.3 of the Order, that access is essential to the accomplishment of official Government duties or contractual obligations.

(b) *Determination of Trustworthiness.* A person is eligible for access to classified information only after a showing of trustworthiness as determined by the Secretary of the Treasury based upon appropriate investigations in accordance with applicable standards and criteria.

§ 2.21 Access by Historical Researchers and Former Presidential Appointees [4.3].

(a) The requirement for access to classified information may be granted only as is essential to the accomplishment of authorized and lawful Government purposes and may be waived for persons who:

(1) Are engaged in historical research projects, or

(2) Previously have occupied policy-making positions to which they were appointed by the President.

(b) Access to classified information may be granted to historical researchers and to former Presidential appointees upon a determination of trustworthiness; a written determination that such access

is consistent with the interests of national security; the requestor's written agreement to safeguard classified information; and the requestor's written consent to have his notes and manuscripts reviewed in order to ensure that no classified information is contained therein. By the terms of § 4.3(b)(3) of the Order, former Presidential appointees not engaged in historical research may only be granted access to classified documents which they "originated, reviewed, signed or received while serving as a Presidential appointee."

(c) If the access requested by historical researchers and former Presidential appointees requires the rendering of services for which fair and equitable fees may be charged pursuant to Title 5 of the Independent Offices Appropriations Act, 31 U.S.C. 483a, the requestor shall be so notified and the fees may be imposed.

§ 2.22 Dissemination [4.1(d)].

Except as otherwise provided by Section 102 of the National Security Act of 1947, 61 Stat. 495, 50 U.S.C. 403 (1970 and Suppl V 1975), classified information originating in another agency may not be disseminated outside the Department without the consent of the originating agency.

§ 2.23 Standards for Security Equipment [4.1(b) and 5.1(b)].

The Administrator of General Services shall, in coordination with agencies originating classified information, establish and publish uniform standards, specifications, and supply schedules for security equipment designed to provide secure storage for and to destroy classified information. Any agency may establish more stringent standards for its own use. Whenever new security equipment is procured, it shall be in conformance with the standards and specifications referred to above and shall, to the maximum extent practicable, be of the type available through the Federal Supply System.

§ 2.24 Accountability procedures [4.1(b)].

(a) *Top Secret Control Officers.* Each Treasury bureau and the Office of the Secretary shall designate a primary and alternate Top Secret Control Officer. Top Secret Control Officers so designated shall:

(1) Maintain current accountability records of Top Secret information received within their bureau or office.

(2) Ensure that Top Secret information is properly stored and that Top Secret information under their control is personally destroyed, when required.

(3) Ensure that reproduction prohibitions of Top Secret information are strictly adhered to.

(4) Conduct annual physical inventories of such information. An inventory shall be conducted in the presence of an individual with an appropriate security clearance. The inventory shall be completed annually and signed by the Top Secret Control Officer and the witnessing individual.

(5) Ensure that Top Secret documents are downgraded, declassified, retired or destroyed as required by regulations or markings.

(6) Attach a TD F 71-01.7 (Top Secret Document Record) to the first page or cover of each copy of Top Secret information. The Top Secret Document Record shall be completed by the Top Secret Control Officer which shall serve as a permanent record.

(7) Ensure that all persons having access to Top Secret information sign the Top Secret Document Record. This also includes persons to whom oral disclosure was made.

(8) Maintain receipts concerning the transfer and destruction of Top Secret information. Record such actions on the Top Secret Document Record which shall be retained for a minimum of three years.

(9) As received, number in sequence each Top Secret document in a calendar year series (i.e. 82-001). This number shall be posted on the document and on all forms required for control of Top Secret information.

(10) Attach and properly execute TD F 71-01.5 (Classified Document Record of Transmittal) when a Top Secret document is transmitted internally or externally.

(11) Verify, prior to releasing Top Secret information, that the recipient is cleared for access to such information.

(12) Report in writing all Top Secret documents unacccounted for to the Assistant Secretary (Administration) who shall take appropriate action as promulgated by this regulation.

(13) Assure that no individual within the bureau or office transmits Top Secret information to another individual or office without the knowledge and consent of the Top Secret Control Officer.

(14) Ensure that Top Secret Document cover sheets (TD F 71-01.1) are affixed to such information while in use.

(15) Notify bureau of office employees of the designated control point for all incoming and outgoing Top Secret information.

(b) *Top Secret Control Officer Listings.* In order for the Office of Physical Security, Office of Administrative Programs, to maintain a current listing of Top Secret Control Officers within the Department, each Treasury bureau and the Office of the Secretary shall submit in writing to the Office of Physical Security, Office of Administrative Programs, the identities of the office(s) and names of the officials designated as their primary and alternate Top Secret Control Officers. Any changes in these designations shall be reported to the Office of Physical Security, Office of Administrative Programs, within thirty days.

(c) *Top Secret Document Record.* A TD F 71-01.7 shall be attached to the first page or cover of the original and each copy of Top Secret information. The Top Secret Document Record, which shall be completed by the Top Secret Control Officer, shall identify the Top Secret information attached, and shall serve as a permanent record of the information. All persons, including stenographic and clerical personnel, having access to the information attached to the Top Secret Document Record must list their name and date the TD F 71-01.7 prior to accepting responsibility for its custody. The TD F 71-01.7 shall indicate those individuals to whom only oral disclosure is made. The Top Secret Document Record shall remain attached to the Top Secret information until it is either transferred to another U.S. Government agency, downgraded, declassified or destroyed. Whenever any one of these actions is taken, the Top Secret Control Officer shall record the action on the Top Secret Document Record and retain it for a minimum of three years after which time it may be destroyed.

(d) *Classified Document Record of Transmittal.* TD F 71-01.5 shall be the exclusive classified document accountability record for use within the Department of the Treasury. No other logs or records shall be required except for the use of TD F 71-01.7 for Top Secret information. TD F 71-01.5 shall be used for single or multiple document receipting and for internal and external routing. The inclusion of classified information on TD F 71-01.5 should be avoided. In the event the subject title is classified, a recognizable short title shall be used, e.g., first letter of each word in the subject title. Several items may be transmitted to the same addressee with one TD F 71-01.5. The TD F 71-01.5 may be destroyed three years after the date of the final disposition of the document.

(1) *Top Secret Information.* Top Secret information shall be subject to a continuous receipt system regardless of how brief the period of custody. TD F 71-01.5 shall be used for this purpose. Top Secret accountability records shall

be maintained by Top Secret Control Officers separately from the accountability records of other classified information.

(2) *Secret Information.* Receipt on TD F 71-01.5 shall be required for transmission of Secret information between bureaus, offices and separate agencies. Responsible office heads shall determine administrative procedures required for the internal control within their respective offices. The volume of classified information handled and personnel resources available must be considered in determining the level of adequate security measures while at the same time maintaining efficiency.

(3) *Confidential Information.* Receipts for Confidential information shall not be required unless the originator indicates that receipting is necessary.

§ 2.25 Storage [4.1(b)].

Classified information shall be stored only in facilities or under conditions designed to prevent unauthorized persons from gaining access to it.

(a) *Minimum Requirements for Physical Barriers.*—(1) *Top Secret.* Top Secret information shall be stored in a GSA-approved security container with an approved, built-in, three-position, dial-type changeable combination lock or in other types of storage facilities that meet the standards for Top Secret established under the provisions of § 2.23. In addition, the designated security officer in each Treasury bureau or the Office of the Secretary shall prescribe those supplementary controls deemed necessary to restrict unauthorized access to areas in which such information is stored. Any vault used for the storage of sensitive compartmented information shall be configured to the specifications of the Director of Central Intelligence.

(2) *Secret and Confidential.* Secret and Confidential information shall be stored in a manner and under the conditions prescribed for Top Secret information, or in a container, vault, or alarmed area that meets the standards for Secret or Confidential information established under the provisions of § 2.23. Secret and Confidential information may also be stored in a safe-type filing cabinet having a built-in, three-position, dial-type changeable combination lock, or a steel filing cabinet equipped with a steel lock bar secured by a GSA-approved three-position changeable combination padlock. The designated security officer in each Treasury bureau or the Office of the Secretary shall prescribe those supplementary controls deemed necessary to restrict unauthorized access to areas in which such information is stored. Access to bulky Secret and Confidential material in weapons storage areas, strong rooms, closed areas or similar facilities shall be controlled in accordance with requirements established by the Department. At a minimum, such requirements shall prescribe the use of key-operated, high-security padlocks approved by the General Services Administration.

(b) *Combinations.*—(1) *Equipment in Service.* Combinations to dial-type locks shall be changed only by persons having an appropriate security clearance, and shall be changed whenever such equipment is placed in use; whenever a person knowing the combination no longer requires access to it; whenever a combination has been subjected to possible compromise; whenever the equipment is taken out of service; or at least once every year. Knowledge of combinations shall be limited to the minimum number of persons necessary for operating purposes. Records of combinations shall be classified no lower than the highest level of classified information that is protected by the lock.

(2) *Equipment Out of Service.* When security equipment is taken out of service, it shall be inspected to ensure that no classified information remains, and any built-in combination lock shall be reset to the standard combination 50-25-50. Combination padlocks shall be reset to the standard combination 10-20-30 or the designated security officer in each Treasury bureau or the Office of the Secretary shall prescribe such supplementary controls deemed necessary to fulfill their individual needs.

(3) *Safe or Cabinet Security Record.* Each piece of equipment used for the storage of classified information will have attached conspicuously to the outside a General Services Administration Optional Form 62 (Safe or Cabinet Security Record) on which an authorized person will record the date and time each day that they initially unlock and finally lock the security equipment, followed by their initials.

On each normal workday regardless of whether the security equipment was opened on that particular day, the security equipment shall be checked by authorized personnel to assure that no surreptitious attempt has been made to penetrate the equipment and the "Checked By" column of the Optional Form 62 shall be annotated to reflect the date and time of the action followed by that person's initials. Security equipment used for the storage of classified information that has been opened on a particular day shall not be left unattended at the end of that day until it has been locked by an authorized person and checked by a second person. In addition, reversible "Open-Closed" signs, available through normal supply channels, shall be used on such equipment and the tops of such equipment shall be kept free of all extraneous matter.

(4) *Safe Combination Records.* Combinations to equipment containing classified information shall be recorded on Treasury Form No. 4032 (Security Container Information). Such forms shall be completed in their entirety. Part 1 of the Form shall be posted on the interior of the top or locking drawer of the safekeeping equipment concerned. The names, addresses and home telephone numbers of personnel responsible for the combination and the classified information stored therein must be posted on Part 1 of the Form. Part II shall be properly completed, inserted in the envelope (Part III) provided and forwarded to the designated central repository for safe combinations. Parts II and III shall show the appropriate classification marking.

(c) *Keys.* The designated security officer in each Treasury bureau and the Office of the Secretary shall establish administrative procedures for the control and accountability of keys and locks whenever key-operated, high-security padlocks are utilized. The level of protection provided such keys shall be equivalent to that afforded the classified information being protected by the padlock.

(d) *Classified Document Cover Sheets.* In order to alert personnel to the fact that a document or folder is classified and to protect it from unauthorized scrutiny, classified document cover sheets, available through normal supply channels, will be used to cover classified documents when in use. Classified document cover sheets will be removed before classified information is filed to conserve filing space and also prior to transmission except when the transmission is made internally within a headquarters by courier, messenger or by personal contact.

§ 2.26 Transmittal [4.1(b)].

(a) *Preparation and Receipting.* Classified information to be transmitted outside of a Treasury facility shall be enclosed in opaque inner and outer covers. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee. The outer cover shall be sealed and addressed with no identification of the classification of its contents. A receipt

shall be attached to or enclosed in the inner cover, except that Confidential information shall require a receipt only if the sender deems it necessary. The receipt shall identify the sender, addressee, and the document, but shall contain no classified information. It shall be immediately signed by the recipient and returned to the sender. Within a Treasury facility, such information may be transmitted between offices by direct contact of the officials concerned in a single sealed opaque envelope with no security classification category being shown on the outside of the envelope. Classified information shall never be delivered to unoccupied rooms or offices.

(b) *Transmittal of Top Secret.* The transmittal of Top Secret information outside of a facility shall be by specifically designated personnel, by State Department diplomatic pouch, by a messenger-courier system authorized for the purpose, or over authorized secure communications circuits.

(c) *Transmittal of Secret.* The transmittal of Secret information shall be effected in the following manner:

(1) *The 50 States, District of Columbia, and Puerto Rico.* Secret information may be transmitted within and between the 50 States, the District of Columbia, and the Commonwealth of Puerto Rico by one of the means authorized for Top Secret information, by the U.S. Postal Service registered mail, or by protective services provided by U.S. air or surface commercial carriers under such conditions as may be prescribed by the head of the agency concerned.

(2) *Other Areas.* Secret information may be transmitted from, to, or within areas other than those specified in § 2.25(c)(1) by one of the means established for Top Secret Information, or by U.S. registered mail through Military Postal Service facilities provided that the information does not at any time pass out of U.S. citizen control and does not pass through a foreign postal system. Transmittal outside such areas may also be accomplished under escort of appropriately cleared personnel aboard U.S. Government owned and U.S. Government contract vehicles or aircraft, ships the United States Navy, civil service manned U.S. Naval ships, and ships of U.S. Registry. Operators of vehicles, captains or masters of vessels, and pilots of aircraft who are U.S. citizens and who are appropriately cleared may be designated as escorts.

(d) *Transmittal of Confidential.* Confidential information shall be transmitted within and between the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories or possessions by one of the means established for higher classifications, or by the U.S. Postal Service certified or registered mail. Outside these areas, Confidential information shall be transmitted only as is authorized for higher classifications.

(e) *Hand Carrying of Classified Information in Travel Status.*—(1) *General Provisions.* Personnel in travel status shall physically transport classified information across international boundaries only when essential. Whenever possible, and when time permits, the most desirable way to transmit classified information to the location being visited would be by other authorized means. The physical transportation of classified information on non-U.S. flag aircraft should be avoided if possible. See TD 71-10.A entitled "Screening of Airline Passengers Carrying U.S. Classified Information or Material".

(2) *Specific Safeguards.* If it is determined that the transportation of classified information by an individual in travel status is in the best interest of the U.S. Government, the following specific safeguards shall be provided for:

(i) Classified information shall be in the physical possession of the individual and shall have adequate safeguards at all times if proper storage at a U.S. Government facility is not available. Under no circumstances shall classified information be stored in a hotel safe or room, locked in automobiles, private residences, train compartments, or any vehicular detachable storage compartments.

(ii) An inventory of all Top Secret classified information, including teletype messages, shall be made prior to departure and a copy of same shall be retained by the traveller's office until the traveller's return at which time all Top Secret classified information shall be accounted for. These same procedures are recommended for information classified Secret.

(iii) Classified information shall not be displayed or used in any manner in public conveyances or rooms.

(iv) In order to avoid unnecessary delays in the screening process prior to boarding commercial air carriers, it is advisable that the individual shall have in his/her possession a written Department of the Treasury authorization to transport classified information. This courier authorization, along with official travel orders, shall in most instances, permit the individual to exempt the classified information from inspection. If difficulty is encountered, the individual should tactfully refuse to exhibit or disclose the classified information to inspection and should insist on the assistance of the local U.S. diplomatic representative at the port of entry or departure.

(v) Upon completion of the visit, the individual shall have the information returned to his/her office by approved means. All Top Secret classified information, including teletype messages, taken for the purpose of the visit shall be accounted for. It is recommended that Secret information also be accounted for. If any Top Secret or Secret classified items are left with the office being visited for its retention and use, the individual shall obtain a receipt.

§ 2.27 Telecommunications transmissions.

Classified information shall not be communicated by telecommunications transmission, except as may be authorized by this regulation with respect to the transmission of classified information over authorized secure communications circuits or systems.

§ 2.28 Special access programs [1.2(a) and 4.2(a)].

The Department may create or continue a special access program if:

(a) Normal management and safeguarding procedures do not limit access sufficiently; and

(b) The number of persons with access is limited to the minimum necessary to meet the objective of providing extra protection for the information.

§ 2.29 Reproduction controls [4.1(b)].

(a) Top Secret documents, except for the controlled initial distribution of information processed or received electrically, shall not be reproduced without the consent of the originator.

(b) Unless restricted by the originating agency, Secret and Confidential documents may be reproduced to the extent required by operational needs.

(c) Reproduced copies of classified documents shall be subject to the same accountability and controls as the original documents.

(d) Paragraphs (a) and (b) of this section shall not restrict the reproduction of documents to facilitate review for declassification.

§ 2.30 Loss or possible compromise [4.1(b)].

(a) *Report of Loss or Compromise.* Any Treasury employee who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to their designated security officer who shall take

appropriate action. In turn, the Office of Physical Security, Office of Administrative Programs, shall be notified by the affected bureau of such reported loss or possible compromise. The Office of Physical Security shall also notify the originating department and any other interested department.

(b) *Inquiry.* The Office of Physical Security, Office of Administrative Programs, shall notify the Assistant Secretary (Administration) who shall then direct an immediate inquiry to be conducted for the purpose of taking corrective measures and assessing damages. Based on the results of the initial inquiry, it may be deemed appropriate to notify the Inspector General who shall determine whether the Office of the Inspector General or a Treasury bureau will conduct any additional investigation. Upon completion of the investigation by the Inspector General, the Inspector General shall recommend to the Assistant Secretary (Administration) and concurrently the Office of Physical Security, Office of Administrative Programs, the appropriate administrative, disciplinary, or legal action to be taken.

§ 2.31 Responsibilities of holders [4.1(b)].

Any person having access to and possession of classified information is responsible for protecting it from persons not authorized access. This includes securing it in approved equipment or facilities whenever it is not under the direct supervision of authorized persons and meeting accountability requirements prescribed by the Department.

§ 2.32 Inspections [4.1(b)].

Individuals charged with the custody of classified information shall conduct the necessary inspections within their areas to ensure adherence to procedural safeguards prescribed to protect classified information. Security officers shall ensure that periodic inspections are made to determine whether procedural safeguards prescribed by this regulation are in effect at all times.

§ 2.33 Security violations.

General. Any individual, at any level of employment, determined to have been responsible for the unauthorized release or disclosure or potential release or disclosure of classified national security information, whether it be knowingly, willfully or through negligence, shall be notified on TD F 71-21.1 (Record of Security Violation) that his/her action is in violation of this regulation, the Order, the Directive, and Executive Order No. 10450, as amended. TD 71-21.A entitled "Administration of Security Violations" sets forth provisions concerning security violations which shall apply to each Treasury employee and all persons under contract or subcontract to the Department of the Treasury authorized access to classified national security information.

(a) Repeated abuse of the classification process, either by unnecessary or over-classification, or repeated failure, neglect or disregard of established requirements for safeguarding classified information by any employee shall be grounds for appropriate adverse or disciplinary action. Such actions may include, but are not limited to, a letter or warning, a letter of reprimand, suspension without pay, or dismissal, as appropriate in the particular case, under applicable personnel rules, regulations and procedures. Where a violation of criminal statutes may be involved, any such case shall be promptly referred to the Department of Justice.

(b) After an affirmative adjudication of a security violation, and as the occasion demands, reports of accountable security violations shall be placed in the employee's personnel security file, and as appropriate, in the employee's official personnel folder. The security official of the bureau or office concerned shall recommend to the respective management official or bureau head that disciplinary action be taken when such action is indicated.

§ 2.34 Disposition and destruction [4.1(b)].

Classified information no longer needed in current working files or for reference or record purposes shall be processed for appropriate disposition in accordance with the provisions of Chapters 21 and 33 of Title 44, United States Code, which govern disposition of Federal records. Classified information approved for destruction shall be destroyed by burning, mulching, or shredding in the presence of designated or authorized individuals. The method of destruction must preclude recognition or reconstruction of the classified information.

(a) *Approval of Use of Mulching and Shredding Equipment.* Prior to obtaining mulching or shredding equipment, the Office of Physical Security, Office of Administrative Programs, shall approve the use of such equipment.

(b) *Destruction by Burning.* Any classified information to be destroyed by burning shall be torn and placed in containers designated as burnbags and shall be clearly and distinctly labeled "Burn." Burnbags awaiting destruction shall be protected by security safeguards commensurate with the classification or control designation of the information involved.

(c) *Records of Destruction.* Appropriate accountability records shall be maintained on TD F 71-01.17 (Classified Document Certificate of Destruction) to reflect the destruction of all Top Secret information. The TD F 71-01.17 shall also be executed for the destruction of information classified Secret or Confidential as deemed necessary by the originator or as required by special regulations.

(d) *Destruction of Nonrecord Classified Information.* Nonrecord classified information such as extra copies and duplicates, including shorthand notes, preliminary drafts, used carbon paper and other material of similar temporary nature, shall also be destroyed by burning, mulching, or shredding as soon as it has served its purpose, but no records of such destruction need be maintained

Subpart E—Implementation and Review

§ 2.35 Departmental administration.

(a) The Assistant Secretary (Administration) shall:

(1) Enforce the Order, the Directive and this regulation, and establish, coordinate and maintain active training, orientation and inspection programs for employees concerned with classified information.

(2) Review suggestions and complaints regarding the administration of this regulation.

(b) The Office of Physical Security, Office of Administrative Programs, shall:

(1) Review all bureau implementing regulations prior to publication and shall require any regulation to be changed, if it is not consistent with the Order, the Directive or this regulation.

(2) Have the authority to conduct on-site reviews of bureau physical security programs and the information security programs as they pertain to each Treasury bureau and to require such reports, information and assistance as may be necessary.

§ 2.36 Bureau administration.

Each Treasury bureau and the Office of the Secretary shall designate a security officer or an official to direct, coordinate and administer its information security programs and physical security programs which shall include active oversight to ensure effective implementation of the Order, the Directive, this regulation and any bureau implementing regulation.

§ 2.37 Emergency planning [4.1(b)].

Each Treasury bureau and the Office of the Secretary shall develop plans for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, or enemy action. These plans shall include the disposition of classified information located in foreign countries.

§ 2.38 Emergency authority [4.1(b)].

The Secretary of the Treasury and other officials delegated original classification authority by the President may prescribe by regulation special provisions for the dissemination, transmittal, destruction, and safeguarding of national security information during combat or other emergency situations which pose an imminent threat to national security information.

§ 2.39 Security education [5.3(a)].

Each Treasury bureau that creates or handles national security information, including the Office of the Secretary, is required to establish a security education program. The program shall be sufficient to familiarize all necessary personnel with the provisions of the Order, the Directive, this regulation and any other implementing directives and regulations to impress upon them their individual security responsibilities. The program shall also provide for initial, refresher, and termination briefings.

(a) *Briefing of Employees.* All new employees concerned with classified information shall be afforded a security briefing regarding the Order, the Directive and this regulation. Employees concerned with sensitive compartmented information shall be required to read and sign a security agreement. All new employees afforded a security briefing shall be provided with copies of applicable laws and pertinent security regulations setting forth the procedures for the protection and disclosure of classified information. All employees given a security briefing shall be required to sign a TD F 71-01.16 (Physical Security Orientation Acknowledgment).

Supbart F—General Provisions

§ 2.40 Definitions [6.1].

(a) *Original Classification Authority.* The authority vested in an Executive Branch official to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security.

(b) *Originating Agency.* The agency responsible for the initial determination that particular information is classified.

(c) *Multiple Sources.* The term used to indicate that a document is derivatively classified when it contains classified information derived from other than one source.

(d) *Portion.* A segment of a document for purposes of expressing a unified theme; ordinarily a paragraph.

(e) *Special Access Program.* Any program imposing "need-to-know" or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. Such a program may include, but is not limited to, special clearance, adjudication, or investigative requirements, special designations of officials authorized to determine "need-to-know," or special lists of persons determined to have a "need-to-know".

(f) *Intelligence Activity.* An activity that an agency within the Intelligence Community is authorized to conduct pursuant to Executive Order No. 12333.

(g) *Special Activity.* An activity conducted in support of national foreign policy objectives abroad which is planned and executed so that the role of the United States Government is not apparent or acknowledged publicly, and functions in support of such activity, but which is not intended to influence United States political processes, public opinion, policies or media and does not include diplomatic activities or the collection and production of intelligence or related support functions.

(h) *Unauthorized Disclosure.* A communication or physical transfer of classified information to an unauthorized recipient.

(i) *Derivative Classification.* A determination that information is, in substance, the same as information that is currently classified and a designation of the level of classification.

(j) *Information.* Any information or material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government.

(k) *National Security Information.* Information that has been determined pursuant to the Order or any predecessor order to require protection against unauthorized disclosure and that is so designated.

(l) *Foreign Government Information.* (1) Information provided by a foreign government or governments, an international organization of governments, or any elements thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or

(2) Information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

(m) *National Security.* The national defense or foreign relations of the United States.

(n) *Confidential Source.* Any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship, or both be held in confidence.

(o) *Original Classification.* An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

Donald T. Regan,

Secretary of the Treasury.

[FR Doc. 82-35489 Filed 12-30-82; 8:45 am]

BILLING CODE 4810-25-M

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

50 CFR Part 663

[Docket No. 21227-261]

Pacific Coast Groundfish Fishery

AGENCY: National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice of deferred effective date and request for comment.

SUMMARY: Final regulations implementing the Pacific Coast Groundfish Fishery Management Plan delayed until Janaury 1, 1983, the effectiveness of certain provisions dealing with vessel identification and gear specifications. The intended effect of this notice is to further defer the regulation that imposes specific marking requirements for each mile of trap or longline groundlines while the Secretary reconsiders this provision.

DATES: The effective date of groundline marking provisions contained in the second sentence of § 663.26(d)(4) and the second sentence of § 663.26(f)(2) is deferred. Comments on this provision must be received by February 2, 1983.

ADDRESSES: Send comments to H. A. Larkins, Director, Northwest Region.

National Marine Fisheries Service, 7600 Sand Point Way NE, BIN C15700, Seattle, Washington 98115.

FOR FURTHER INFORMATION CONTACT:
H. A. Larkins, 206–527–6150.

SUPPLEMENTARY INFORMATION: The Pacific Coast Groundfish Fishery Management Plan (FMP) was approved by the Assistant Administrator for Fisheries, NOAA, on January 4, 1982, and its final implementing regulations at 50 CFR Parts 611 and 663 (47 FR 43964) were published on October 5, 1982. Several provisions in the FMP were new or more restrictive than previous requirements and were thought to impose an economic burden on domestic fishermen if imposed immediately. Consequently, these provisions were deferred for three months to allow a grace period for compliance by fishermen.

The Pacific Fishery Management Council (Council) recommended at its November 17–18, 1982 meeting, and the Assistant Administrator concurs, that the previously deferred provisions should become effective at 0001 PST, January 1, 1983, except for the one-mile marking of longline and trap groundlines, which should be deferred indefinitely. The primary reason for delaying the effectiveness of this groundline regulation is to give the Council and the Secretary time to determine whether the groundline marking of each mile of trap and longline gear is unsafe, ineffective, impractical, and unenforceable, as public testimony has indicated. The exact wording of this deferred provision is—

Section 663.26(d)(4) for traps—"Traps laid on a groundline must also be marked at the surface every one mile of groundline with a pole and flag, and either a light or a radar reflector."; and

Section 663.26(f)(2) for longline gear—"Every one mile of groundline must also be marked at the surface with a pole and flag, and either a light or a radar reflector."

Comments on the need for this provision may be sent to the Regional Director at the above address.

(16 U.S.C. 1801 *et seq.*)

Dated: December 28, 1982.

Carmen J. Blondin,

Deputy Assistant Administrator for Fisheries Resource Management, National Marine Fisheries Service.

[FR Doc. 82-35550 Filed 12-28-82; 1:47 pm]

BILLING CODE 3510-22-M