(Billing Code 6820-AF) APR 2

INFORMATION SECURITY OVERSIGHT OFFICE

32 CFR Part 2001

(Directive No. 1)

National Security Information

AGENCY: Information Security Oversight Office (ISOO)

ACTION: Implementing directive; Final rule.

SUMMARY: The Information Security Oversight Office is publishing this directive (final rule) pursuant to section 5.2(b)(1) of Executive Order , relating to national security information. The National Security Council approved this Directive on 1982. The Executive order prescribes a uniform information security system; it also establishes a monitoring system to enhance its effectiveness. This Directive sets forth guidance to agencies on original and derivative classification, downgrading, declassification and safeguarding of national security information.

EFFECTIVE DATE: August 1, 1982.

FOR FURTHER INFORMATION CONTACT: Steven Garfinkel, Director, ISOO.

Telephone: 202-633-6880.

SUPPLEMENTARY INFORMATION: This Directive is issued pursuant to the provisions of section 5.2(b)(1) of Executive Order . The purpose of the Directive is to assist in implementing Executive Order , and

users of the Directive shall refer concurrently to that Order for guidance.

LIST OF SUBJECTS IN 32 CFR 2001

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 32 of the Code of Federal Regulations, Part 2001, is revised to read as follows:

Part 2001 -- National Security Information

TABLE OF CONTENTS

Authority: Section 5.2(b)(1), E.O. .

FR .

Subpart A--Original Classification

2001.1 Classification levels.

(a) Limitations [1.1(b)]*. Markings other than "Top Secret," "Secret," and "Confidential," such as "For Official Use Only" or "Limited Official Use," shall not be used to identify national security information. In addition, no other term or phrase shall be used in conjunction with one of the three authorized classification levels, such as "Secret Sensitive" or "Agency Confidential."

(b) Reasonable doubt [1.1(c)]. When there is reasonable doubt about the need to classify information, the originator of the information shall safeguard it as if it were "Confidential" information in accordance with Subpart D, pending the determination about its classification. When there is reasonable doubt about the appropriate classification level, the originator of the information shall safeguard it at the higher level in accordance with Subpart D, pending the determination of its classification

*Bracketed references are to related sections of Executive Order .

level. Upon the determination of classification or level of classification, the information that is classified shall be marked as provided in §2001.5.

2001.2 Classification authority.

(a) General [1.2]. The exercise of classification and declassification authority inherently includes the consideration of the public interest served by protection or disclosure.

(b) Requests for original classification authority [1.2]. The head of an executive branch entity who has not been delegated original classification authority by the President may submit a request for such authority to the President through the Information Security Oversight Office. The request shall provide a complete justification for the level of classification authority sought, including a description of the information that will require original classification and the anticipated frequency of original classification actions.

(c) Listing classification authorities [1.2]. Any official who delegates original classification authority shall maintain a current listing of persons or positions receiving those delegations. If possible, these listings shall be unclassified.

(d) Exceptional cases [1.2(e)]. Information described in section 1.2(e) of Executive Order (hereinafter "the Order"), shall be handled as provided in §2001.1(b).

2001.3 Classification categories.

(a) Foreign government information (FGI)[1.3(a)(3)]. FGI need not fall within any other classification category listed in section 1.3(a) of the Order to be classified.

(b) 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 information. Classification on this basis shall be fully supported by a written explanation to be maintained with the record copy of the information.

(c) 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, the agency of primary interest shall determine the degree of damage to the national security, the need for continued classification, and what action must be taken to prevent similar occurrences.

2001.4 Duration of classification.

(a) Information not marked for declassification [1.4]. Information classified under predecessor Orders that does not bear a specific date or event for declassification shall remain classified until reviewed for declassification.

(b) 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 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 Director of the Information Security Oversight Office.

2001.5 Identification and markings [1.5(a), 1.5(b) and 1.5(c)]. A uniform system requires that standard markings be applied to national security information. Except in extraordinary circumstances as provided in section 1.5(a) of the Order, or as indicated herein, the marking of paper documents shall not deviate from the following prescribed formats. These markings shall also be affixed to media other than paper documents, or the originator shall

provide holders or recipients of the information with written instructions for protecting the information.

(a) Classification level. As markings, the classification levels "Top Secret," "Secret," and "Confidential" shall be used to indicate: (1) that information requires protection as national security information under the Order; (2) the highest level of classification contained in a document; and (3) the classification level of each page and portion of a document.

(1) Overall marking. The highest level of classification of information in a document shall be marked in bold letters at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, 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. An authorized official 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. 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 or following 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. 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 shall be assigned to facilitate reference. A subject or title lacking a parenthetical designator shall be presumed to be unclassified.

(b) 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 (name, position, or other identifier)"

(c) Agency and office of origin. If the originating agency and office is not identified by the letterhead, logo or other means, it shall be placed below the "CLASSIFIED BY" line.

(d) Declassification and downgrading instructions. Declassification and downgrading instructions shall be shown as follows:

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

"DECLASSIFY ON: (date)"

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

"DECLASSIFY ON: (description of event)"

(3) for information not to be automatically declassified:

"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:

"DOWNGRADE TO (classification level)
ON (date or description of event)"

(e) Special markings.

(1) Transmittal documents [1.5(c)]. A document shall indicate on its face 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 IS REMOVED"

(ii) for a classified transmittal document:

"UPON REMOVAL OF ATTACHMENTS THIS DOCUMENT IS (classification level of the transmittal letter standing alone)"

(2) Restricted Data or Formerly Restricted Data [6.2(a)]. Documents containing both national security information and Restricted Data or Formerly Restricted Data shall include markings prescribed in regulations issued by the Secretary of Energy under the Atomic Energy Act of 1954, as amended.

(3) Intelligence sources and methods [1.5(c)]. Documents that contain information relating to intelligence sources and methods shall include the following marking:

"WARNING NOTICE--INTELLIGENCE
SOURCES AND METHODS INVOLVED"

(4) Foreign government information (FGI) [1.5(c)]. Documents that contain FGI shall include the following marking:

"FOREIGN GOVERNMENT INFORMATION"

If the fact of foreign origin must be concealed, the marking shall not be used and the document shall be marked as if it were wholly of U.S. origin.

(5) Electrically transmitted information (messages) [1.5(c)]. National security information that is transmitted electrically shall be marked as follows:

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

(ii) a "CLASSIFIED BY" line is not required;

(iii) the duration of classification shall appear as follows:

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

"DECL: (date)"

(B) for information to be declassified upon occurrence of a specific event:

"DECL: (description of event)"

(C) for information not to be automatically declassified which requires the originating agency's determination (see also §2001.5(d)(3)):

"DECL: OADR"

(D) 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)"

(iv) portion marking shall be as prescribed in §2001.5(a)(3);

(v) special markings shall follow the marking for highest level of classification. These include:

(A) Restricted Data or Formerly Restricted Data:

"RD" for Restricted Data
"FRD" for Formerly Restricted Data

(B) information concerning intelligence sources and methods:

"WNINTEL"

(C) foreign government information:

"FGI"

If the fact of foreign origin must be concealed, the marking shall not be used and the message shall be marked as if it were wholly of U.S. origin.

(vi) Agency prescribed markings [1.5(c) and 5.3(c)]. Officials delegated original classification authority by the President may prescribe additional markings to control reproduction and dissemination, including markings required for special access programs authorized by section 4.2(a) of the Order.

(f) Changes in classification markings [4.1(b)]. When a change is made in the level or the duration of originally classified information, all holders should be promptly notified. 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.

2001.6 Limitations on classification [1.6(c)].

Before reclassifying information as provided in section 1.6(c) of the Order, the authorized official shall

consider the following factors, which shall be addressed in the report to the Director of the Information Security Oversight Office required by section 1.6(c) of the Order:

(a) The elapsed time following disclosure;

(b) the nature and extent of disclosure;

(c) the ability to bring the fact of reclassification to the attention of personnel 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

2001.20 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 entity who has the authority to declassify, downgrade or upgrade the information.

2001.21 Classification guides.

(a) General [2.2(a)]. Classification guides shall, at a minimum:

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

(2) state which classification level applies to each element of information; and

(3) prescribe declassification instructions for each element 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 automatically declassified without the approval of the originating agency.

(b) Requirement for review [2.2(a)]. Classification guides shall be reviewed and updated at least every two years. Each agency shall maintain a list of its classification guides in current use.

(c) Waivers [2.2(c)]. An authorized official's decision to waive the requirement to issue classification guides for specific classes of documents or information should be based, at a minimum, on an evaluation of the following factors:

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

(2) the practicality of producing and disseminating the guide because of the sensitive nature of the information;

(3) the anticipated 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.

2001.22 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 §2001.5(a) through (d) and such markings prescribed by §2001.5(e) as are applicable. Information for these markings shall be taken from the source document or instructions in the appropriate classification guide. When markings are omitted because they may reveal a confidential source or relationship not otherwise evident, as described in section 1.5(a) of the Order, the information may not be used as a basis for derivative classification.

(a) The authority for classification shall be shown as follows:

"CLASSIFIED BY (description of source document or classification guide)"

If a document is classified on the basis of more than one source document or classification guide, the authority for classification shall be shown 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 in its "CLASSIFIED BY" line rather than the term "MULTIPLE SOURCES."

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

"DECLASSIFY ON: (date, description of event, or 'ORIGINATING AGENCY'S DETERMINATION REQUIRED' (OADR))"

Subpart C--Declassification and Downgrading

2001.30 Listing declassification authorities [3.1(b)]. Officials authorized to delegate declassification authority shall maintain a current listing of persons or positions receiving those delegations. If possible, these listings shall be unclassified.

2001.31 Systematic review for declassification [3.3].

(a) Permanent records. Systematic review is required only on classified records, and presidential papers or

records that the the Archivist of the United States, acting under the Federal Records Act, has determined to be of sufficient historical or other value to warrant preservation.

(b) Non-permanent records. Unless they are subject to an ongoing Mandatory Review or Freedom of Information Act request, non-permanent classified records shall be disposed of in accordance with schedules approved by the Administrator of General Services under the Records Disposal Act.

(c) Responsibilities.

(1) In meeting responsibilities assigned by section 3.3(a) of the Order, the Archivist shall:

(i) Establish procedures, in consultation with the Director of the Information Security Oversight Office, for the systematic declassification review of permanent records, and presidential papers or records accessioned into the National Archives;

(ii) conduct systematic declassification reviews in accordance with guidelines provided by the head of the agency that originated the information or, with respect to foreign government information, in accordance with

guidelines provided by the Director of the Information Security Oversight Office; or, with respect to presidential information, in accordance with guidelines developed by the Archivist;

(iii) conduct systematic declassification reviews of accessioned records, and presidential papers or records as they become 30 years old, except for information concerning intelligence activities (including special activities), sources or methods created after 1945, and information concerning cryptology created after 1945;

(iv) review for declassification accessioned records, and presidential papers or records concerning intelligence activities (including special activities), sources or methods created after 1945 and cryptology records created after 1945 as they become fifty years old;

(v) establish systematic review priorities for accessioned records, and presidential papers or records based on the degree of researcher interest and the potential for declassifying a significant portion of the information;

(vi) review for declassification, with the concurrence of the originating agency, accessioned records, and presidential papers or records, prior to the timeframes

established in paragraphs (c)(1)(iii) and (iv) of this section;

(vii) re-review for declassification accessioned records, and presidential papers or records upon the determination that the followup review will be productive, both in terms of researcher interest and the potential for declassifying a significant portion of the information.

(2) Officials delegated original classification authority by the President under this or predecessor Orders shall:

(i) Within six months of the effective date of this Order issue declassification guidelines, in consultation with the Archivist and the Director of the Information Security Oversight Office, to assist the Archivist in the conduct of systematic reviews;

(ii) make every reasonable effort, consistent with applicable law, to have accessioned into the National Archives all permanently valuable classified records at the time they become subject to systematic review by the Archivist;

(iii) designate experienced personnel to assist the Archivist in the systematic review process;

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

(3) Within six months of the effective date of this Order the Director of the Information Security Oversight Office shall issue, in consultation with the Archivist and the heads of concerned agencies, systematic review guidelines for foreign government information. The Secretary of State shall assist the Director as may be necessary in coordinating these guidelines with foreign governments. The Director shall review and update these guidelines every five years unless earlier review is requested by the Archivist.

(d) Special procedures. All agency heads shall be bound by the special procedures for systematic review of classified cryptologic records and classified records pertaining to intelligence activities (including special activities), sources or methods issued by the Secretary of Defense and the Director of Central Intelligence, respectively.

2001.32 Mandatory review for declassification [3.4].

(a) U.S. originated information.

(1) Each agency head shall publish in the Federal Register the identity of a person or office to which mandatory declassification review requests may be addressed.

(2) Processing.

(i) Requests for classified records in the custody of the originating agency. A valid mandatory review request need not identify the requested information by date or title of the responsive records, but must be of sufficient particularity to allow agency personnel to locate the records containing the information sought with a reasonable amount of effort. Agency responses to mandatory review requests shall be governed by the amount of search and review time required to process the request. For those requests requiring less than eight hours of search and review time, agencies shall notify the requester of their declassification determinations within 10 working days from receipt of the request. For requests requiring more than eight hours of search and review time, agencies shall either make a prompt declassification determination and notify the requester accordingly, or inform the requester of the additional time needed to process the request. In no case shall the agency response time for a final determination exceed one year from the date of receipt of the initial request. When information

cannot be declassified in its entirety, agencies will make reasonable efforts to release those declassified portions of the requested information that constitute a coherent segment. Upon the denial of an initial request, the agency shall also notify the requester of the right of an administrative appeal which must be filed within 60 days of receipt of the denial.

(ii) Requests for classified records in the custody of an agency other than the originating agency. When an agency receives a mandatory declassification review request for records in its possession originated by another agency, it shall forward the request to that agency. If practicable, the forwarding agency shall include a copy of the records requested together with its recommendations for action. Upon receipt, the originating agency shall process the request in accordance with §2001.32(a)(2)(i).

(iii) Appeals of denials of mandatory declassification review requests. The agency appellate authority 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 agency appellate authority shall notify the requester of the additional time needed and provide the requester with the reason for the extension. In no case shall the agency response time for a final determination exceed six months from the date

of receipt of the appeal. The agency appellate authority shall notify the requester in writing of the final determination and of the reasons for any denial.

(b) Foreign government information. Except as provided in this paragraph, agency heads shall process mandatory review requests for classified records containing foreign government information in accordance with §2001.32(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 the agency receiving the request 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.

(c) Fees. In responding to mandatory review requests for classified records, agency heads may charge fees in accordance with section 483a of title 31, United States Code. The schedules of fees published in the Federal Register by agencies in implementation of Executive Order 12065 shall remain in effect until they are revised.

2001.33 FOIA and Privacy Act requests [3.4]. Agency heads 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

2001.40 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. An agency head may delegate the authority prescribed in this Subpart to the senior agency official delegated responsibility for the program under section 5.3(a) of the Order.

2001.41 Accountability procedures [4.1(b)].

(a) Top Secret. Top Secret control officials shall be designated to receive, transmit, and maintain current access and accountability records for Top Secret information. An inventory of Top Secret documents shall be made at least annually. Agency heads may waive the requirement for an annual inventory of storage systems containing large volumes of Top Secret information upon a determination that the safeguarding of this information is not jeopardized by the inventory waiver. Waivers shall be

in writing and be available for review by the Information Security Oversight Office.

(b) Secret and Confidential. Agency heads shall prescribe the accountability requirements for Secret and Confidential information.

2001.42 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) Top Secret. Top Secret information shall be stored in a GSA-approved security container with an approved, built-in, three-position, dial-type combination lock; in a vault protected by an alarm system and response force; or in other types of storage facilities that meet the standards for Top Secret established under the provisions of §2001.42(c). In addition, heads of agencies shall prescribe supplementary controls to restrict unauthorized access to areas in which such information is stored.

(b) 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 as prescribed in §2001.42(c) or (d).

(c) Standards for security equipment. The Administrator of General Services shall, in coordination with agencies originating classified information, establish and publish uniform standards, specifications, and supply schedules for containers, vaults, alarm systems, and associated security devices suitable for the storage and protection of all levels of 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.

(d) Exception to standards for security equipment.

(1) Secret and Confidential information may also be stored in a safe-type filing cabinet having a built-in, three-position, dial-type combination lock, or a steel filing cabinet equipped with a steel lock bar secured by a GSA-approved three-position combination padlock. The storage of Secret information in the cabinets described above requires the use of such supplementary controls as the head of the agency deems necessary.

(2) 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 appropriate agency head. At a minimum, such requirements shall prescribe the use of key-operated, high-security padlocks approved by the General Services Administration.

(e) 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 the 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.

(f) Keys. Heads of agencies 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.

(g) Responsibilities of custodians. Persons charged with the custody of classified information are responsible for protecting it from persons not authorized access to it, to include securing it in approved equipment or facilities whenever it is not in use or under the direct supervision of authorized persons. They are also responsible for meeting accountability requirements prescribed by the head of the agency.

(h) Hand carrying of classified information. Agency regulations shall prescribe procedures and appropriate restrictions concerning the escort or hand carrying of classified information, including the hand carrying of classified information on commercial carriers.

(i) Inspections. Agency heads shall require periodic inspections to be made to ensure compliance with the provisions of this Order and ISOO Directives. Persons charged with the custody of classified information shall conduct the necessary inspections within their areas to ensure compliance with procedures prescribed to protect classified information.

2001.43 Transmittal [4.1(b)].

(a) Preparation and receipting. Classified information to be transmitted 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. Any of these wrapping and receipting requirements may be waived by agency heads if conditions provide equivalent protection to prevent access by unauthorized persons.

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

(c) Transmittal of Secret. The transmittal of Secret material 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, 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) Canadian government installations. Secret information may be transmitted to and between United States Government and Canadian Government installations in the United States and Canada by United States and Canadian registered mail with registered mail receipt.

(3) Other areas. Secret information may be transmitted from, to, or within areas other than those specified in §2001.43(c)(1) or (2) by one of the means established for Top Secret information, or by U.S. registered mail through Army, Navy, or Air Force 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 and U.S. Government contract vehicles or aircraft, ships of 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 information. 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, first class, or express mail service when prescribed by an agency head. Outside these areas, Confidential information shall be transmitted only as is authorized for higher classifications.

2001.44 Loss or possible compromise [4.1(b)]. Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to an official designated for this purpose by the person's agency or organization. The agency that originated the information shall be notified of the loss or possible compromise so that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect of the compromise. The agency under whose cognizance the loss or possible compromise occurred shall initiate an inquiry to (a) determine cause, (b) place responsibility, and (c) take corrective measures and appropriate administrative, disciplinary, or legal action.

2001.45 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 in accordance with procedures and methods prescribed by the head of the agency. The method of destruction must preclude reconstruction of the classified information or material.

2001.46 Special access programs [4.2(a)]. Agency heads designated pursuant to section 1.2(a) of the Order 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 will be limited to the minimum necessary to meet the objective of providing extra protection for the information.

2001.47 Reproduction controls [4.1(b)].

(a) Top Secret documents shall not be reproduced without the consent of the originating agency.

(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.

2001.48 Emergency planning [4.1(b)]. Agency heads 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 classified information located in foreign countries.

2001.49 Emergency authority [4.1(b)]. Those 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 the national security.

Subpart E--Implementation and Review

2001.50 Agency regulations [5.3(b)]. Each head of an agency shall issue regulations in accordance with 5 U.S.C. 552(a) to implement the Order and 32 CFR Part 2001 no later than December 31, 1982. Those portions that affect members of the public shall include, at a minimum, information relating to the agency's mandatory review program and instructions for submitting suggestions or complaints regarding the agency's information security program.

2001.51 Security education [5.3(a)]. Each agency or other entity that creates or handles national security information is required under the Order to establish a security education program. The program established shall be sufficient to familiarize all necessary personnel with the provisions of the Order and its implementing directives and regulations and to impress upon them their individual security responsibilities. The program shall also provide for initial, refresher, and termination briefings.

Subpart F--General Provisions

2001.60 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) Classification guide: A document issued by an authorized original classifier that prescribes the appropriate level and duration of classification of specified information to be classified derivatively.

(c) Originating agency: The agency or other entity responsible for the initial determination that particular information is classified.

(d) Multiple sources: The term used to indicate that a document is derivatively classified when it contains classified information derived from more than one previously classified document.

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

(f) 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 includes, 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."

(g) Intelligence activity: An activity that an agency within the Intelligence Community is authorized to conduct pursuant to Executive Order 12333.

(h) Special intelligence activity: An activity conducted in support of national foreign 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.

(i) Unauthorized disclosure: A communication or physical transfer of classified information to an unauthorized recipient.

2001.61 Publication and effective date [6.2(f)]. Part 2001 shall be published in the Federal Register. It shall become effective August 1, 1982.

Steven Garfinkel
Director, Information
Security Oversight Office

, 1982