

CONFIDENTIAL

NOV 1979

MEMORANDUM FOR: Chairman, Markings Task Force

FROM:
DDA Representative, Markings Task Force

SUBJECT: Control Markings

1. The Markings Task Force has been discussing the discontinuation of the control marking, "Administrative - Internal Use Only." The arguments for doing away with it are substantial:

- a. It has been misused a great deal; and
- b. The safeguarding sanctions are not clearly defined.

2. I have discussed the use and need of such a marking with a number of people throughout the DDA. There is a need to protect internal Agency information which if released might be misused or be misleading. These papers include:

- a. Management options and recommendations; and
- b. Administrative planning and procedures.

3. Discussion for the need to have a positive indicator to alert employees that a document contains such information has been lively and interesting. Some of the arguments for and against include:

- a. Some people feel if a piece of paper is not marked, employees will/may take it home and discuss the contents freely.
- b. Unclassified government information doesn't need to be marked as it is U.S. Government property and all employees should be aware of this and handle all such material as prescribed by regulations and law.

UNCLASSIFIED When Separated
From Enclosure

CONFIDENTIAL

CONFIDENTIAL

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080009-0

25X1

c. What about HR [] (attached), "Care and Use of Official Data"? This regulation is under review for revision as the current definition of "Official Data" includes all overt material received by the CIA, including the New York Times, library books, etc. Those reviewing the regulation are having problems coming to grips with the definition.

4. In order to provide proper control over Agency internal documents, I suggest we do one of two things:

a. Write a proper definition of "Official Data" and get the regulation out to all employees. If a component is concerned they may indicate on a document "Official Data - Internal Use Only;" or

b. Develop a new control marking for documents which

(1) reflect opinion or recommendations for management policy; or

(2) administrative procedures.

5. The first option appeals as HR [] spells out control of information in general. Sanctions are provided whether the information is marked or not.

25X1

6. The second option implies a new marking with a new definition. We suggest "Agency Restricted" as a marking to meet this need. This could be defined as:

Information prepared by Agency personnel or consultants, such as that pertaining to opinions, recommendations, interpretations, plans or internal procedures, the disclosure of which could prejudice, hinder or deter the Agency from carrying out essential management or administrative functions.

7. The intent is (1) to ensure that such information is only released to the public through authorized channels and (2) to provide an environment conducive to the uninhibited exchange of ideas. Sanctions for the improper use of an unclassified document should follow those for unauthorized release. (There is opposition to giving a control marking

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080009-0

CONFIDENTIAL

CONFIDENTIAL

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080009-0

to documents containing national security information. We have been relying on the classification to control these papers. I submit that even after classifications are no longer valid, the internal nature of some of these documents will remain.)

8. In summary, we need at least ^{to} provide a positive indicator to control the dissemination of unclassified management information and administrative procedures.

Signed

[Redacted Signature]

25X1

Attachment: a/s

cc: DDO/P
NFAC/
DDS&T
OGC (
DDA/O
ISAS/
ISAS/

[Redacted CC List]

25X1

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080009-0

CONFIDENTIAL

21. CARE AND USE OF OFFICIAL DATA. All information, classified or unclassified, received, compiled or created by the Central Intelligence Agency (except personal copies of unclassified personnel papers) is official data and is the property of the United States Government.

a. POLICY

- (1) All employees are prohibited from using official data for any purpose other than in the performance of their official duties for or on behalf of the Agency. Official data is not to be held in personal files or set aside for personal use or benefit.
- (2) Official data is not to be copied or removed from the files of the Agency for release outside the Agency except by those officials authorized through chain of command by the Director of Central Intelligence.
- (3) Any employee who is served with a subpoena which may require the disclosure of official data to a court, the Congress, or a committee of the Congress will promptly inform the General Counsel of the serving of the subpoena, the nature of the information sought, and any circumstances which may bear upon the desirability of making available the official data, so that the General Counsel may advise the Director.
- (4) When not in use, official data must be kept in storage facilities which have been approved by the Director of Security. Consequently, documents which contain official data are not to be taken home or stored in private residences unless the use of an approved, secure facility has been authorized in advance by the Director of Security.
- (5) In addition to the prohibition against unauthorized disclosure of official data outside the Agency, internal disclosure of official data is limited to those employees whose duties require access to it. Employees are not to disclose official data to those who do not need to know it, nor are they to try to obtain official data they do not need to know.

b. RESPONSIBILITIES

- (1) Each individual employed by the Central Intelligence Agency is responsible for the secure handling of official data and for protecting it against unauthorized disclosure. Termination of Agency employment will not affect these responsibilities.
- (2) The Director of Personnel is to ensure that all personnel processed through headquarters report to the Office of Security to read this regulation and the statutes referred to in subparagraph c below before entering on duty or separating from the Agency.
- (3) Chiefs of [] installations are to ensure that all [] personnel not processed through headquarters read this regulation and the statutes referred to in subparagraph c before entering on duty or separating from the Agency.
- (4) Any authorized representative of CIA who negotiates with individuals or organizations for services is to ensure that the appropriate statutory provisions are incorporated in the Secrecy Agreement or contract. The incorporation may be by reference where feasible.

25X1

Revised: 14 November 1969 (508)

CONFIDENTIAL

GROUP 1 Excluded from automatic downgrading and declassification

53

CONFIDENTIALApproved For Release HR 2006/04/19 : CIA-RDP86-00674R000300080009-0 **SECURITY**

- c. **STATUTORY REFERENCES.** Sections 793, 794, and 798, Title 18 of United States Code prohibit certain activities with respect to defense information and provide penalties for violation. Section 793 provides generally that persons who lose defense information without reporting such loss, or gather or transmit defense information with the intent or with reason to believe such information will be used to the injury of the United States or to the advantage of any foreign nation are subject to a fine of \$10,000 or 10 years imprisonment or both. Section 794 provides generally that persons who communicate or deliver or attempt to communicate or deliver defense information to any foreign government with intent or reason to believe such information will be used to the injury of the United States or to the advantage of a foreign government are subject to imprisonment for not more than 20 years. If this statute is violated during wartime, the punishment is death or imprisonment for not more than 30 years. Both sections 793 and 794 provide like penalties for a conviction of conspiracy to violate either section. Section 798 provides generally that persons who communicate or otherwise make available to an unauthorized person or publisher, or use in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government any classified information relating to cryptography or communications intelligence are subject to a fine of \$10,000 or 20 years imprisonment or both.

CONFIDENTIAL

THIS SAMPLE LETTER DOES NOT CONTAIN CLASSIFIED INFORMATION

CONFIDENTIAL ①

INFORMATION SECURITY OVERSIGHT OFFICE ②
Washington, D.C. 20405

September 30, 1978 ③

SUBJECT: MINIMUM REQUIRED MARKINGS FOR CLASSIFIED DOCUMENTS (U) ④

TO: ALL EXECUTIVE BRANCH AGENCIES

⑨ (C) Each portion of a classified document shall be marked to indicate the highest classification of information it contains. For example, this paragraph is marked as if it contained Confidential information.

(U) The circled numbers on this page indicate those markings required for all classified documents. The footnotes below refer to the appropriate paragraph of this directive.

(U) Other markings shall be applied to classified material depending on the content:

- If it is determined that the information should be downgraded automatically, see para. I.G.4.
- If the document does not contain classified information but is used to transmit classified material, see para I.G.11.
- If the document contains foreign government information, see para. I.G.12.
- If the document contains Restricted Data or Formerly Restricted Data, see para. I.H.1.
- If the document contains information on intelligence sources and methods, see para. I.H.2.
- If it is determined that the information requires limitations on reproduction and/or dissemination, see para. I.H.3.

I.M. AWARE
Director

Classified by ⑤ _____

Declassify Review for Declassification on _____ ⑥

Extended by ⑦ _____

Reason for extension ⑧ _____

① **CONFIDENTIAL**

FOOTNOTES

- | | | | |
|---------------------------|-------------|--|--------|
| 1. Page markings | I.G.7. | 6. Date/event for declassification/ review (check appropriate block) | I.G.3. |
| 2. Office of origin | I.G.2. | 7. Extension: authority | I.G.5. |
| 3. Date of classification | I.G.2. | 8. Extension: reason | I.G.6. |
| 4. Subjects and titles | I.G.8. & 9. | 9. Mandatory portion marking | I.G.9. |
| 5. Identity of classifier | I.G.1. | | |

THIS SAMPLE LETTER DOES NOT CONTAIN CLASSIFIED INFORMATION

CONFIDENTIAL ①

INFORMATION SECURITY OVERSIGHT OFFICE ②
Washington, D.C. 20405

September 30, 1978 ③

SUBJECT: MINIMUM REQUIRED MARKINGS FOR CLASSIFIED DOCUMENTS (U) ④

TO: ALL EXECUTIVE BRANCH AGENCIES

⑨ (C) Each portion of a classified document shall be marked to indicate the highest classification of information it contains. For example, this paragraph is marked as if it contained Confidential information.

(U) The circled numbers on this page indicate those markings required for all classified documents. The footnotes below refer to the appropriate paragraph of this directive.

(U) Other markings shall be applied to classified material depending on the content:

- If it is determined that the information should be downgraded automatically, see para. I.G.4.
- If the document does not contain classified information but is used to transmit classified material, see para I.G.11.
- If the document contains foreign government information, see para. I.G.12.
- If the document contains Restricted Data or Formerly Restricted Data, see para. I.H.1.
- If the document contains information on intelligence sources and methods, see para. I.H.2.
- If it is determined that the information requires limitations on reproduction and/or dissemination, see para. I.H.3.

I.M. AWARE
Director

Classified by ⑤ _____

Declassify Review for
Declassification on ⑥ _____

Extended by ⑦ _____

Reason for extension ⑧ _____

① **CONFIDENTIAL**

FOOTNOTES

- | | | | |
|---------------------------|-------------|---|--------|
| 1. Page markings | I.G.7. | 6. Date/event for declassification/
review (check appropriate block) | I.G.3. |
| 2. Office of origin | I.G.2. | 7. Extension: authority | I.G.5. |
| 3. Date of classification | I.G.2. | 8. Extension: reason | I.G.6. |
| 4. Subjects and titles | I.G.8. & 9. | 9. Mandatory portion marking | I.G.9. |
| 5. Identity of classifier | I.G.1. | | |

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080009-0

CONFIDENTIAL

Original Classification Not to Exceed 6 years

CONFIDENTIAL

CL BY: C/S/TS classifier's employee
DECL ON: a. 13 September 1980
or b. Event

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080009-0

CONFIDENTIAL

Marking Original Classification on Documents Classified
in Excess of 6 years but Not in Excess of 20 years

CONFIDENTIAL

CL BY: C/S/TS classifier's employee no.

DECL ON: a. 13 September 1980
or b. Event

OR REVW ON 13 September 1988

EXT BY TS classifier

REASON class. guide #

[If classifier is not TS]

SECRET

Downgrading Documents

SECRET

CL BY: S/TS classifier's employee no.
DOWNGRADE TO C on a. spec. date
b. Event

DECL ON: a. spec. date
b. Event
OR REVW ON same as a or b
EXT BY IS classifier
REASON class. guide #

Derivative

Single Source

If the source material bears a declassification date or event 20 years or less from the date of origin, the date or event shall be carried forward to the new material.

If the source material bears no declassification date or event, or bears an indeterminate date or event such as "Upon Notification by Originator," "Cannot Be Determined," "Impossible to Determine," etc., or is marked for declassification beyond 20 years, the new material shall be marked with a date for review for declassification at 20 years from the date of original classification of the source material.

SECRET

CL BY: anyone's employee no.
SOURCE: class guide or source doc.
DECL ON: spec. date or event
OR REVW ON: date for declass review
as cited on source doc.

SECRET

Derivative

Multiple

If the source material bears a declassification date or event 20 years or less from the date or origin, the date or event shall be carried forward to the new material.

If the source material bears no declassification date or event, or bears an indeterminate date or event such as "Upon Notification by Originator," "Cannot Be Determined," "Impossible to Determine," etc., or is marked for declassification beyond 20 years, the new material shall be marked with a date for review for declassification at 20 years from the date of original classification of the source material.

SECRET

CL BY: anyone's employee no.

SOURCE: Multiple

DECL ON:	<u>latest date or event of source materials</u>
OR REVW ON:	<u>latest date or event of source materials</u>

SECRET

Foreign Information

If the source material is foreign government information bearing no date or event for declassification or is marked for declassification beyond 30 years, the new material shall be marked for review for declassification at 30 years from the time the information was originated by the foreign entity or acquired or classified by the US, whichever is earlier.

SECRET

CL BY: anyone's employee no.

SOURCE: a. Id of source doc.

b. Mem. of Undtg.

c. class guide #

REVW ON: date (30 years)

after info was originated by
foreign government or class. by U.S.

CHAPTER XX—INTERAGENCY CLASSIFICATION REVIEW COMMITTEE

(Directive No. 1)

INFORMATION SECURITY OVERSIGHT OFFICE

National Security Information

AGENCY: Interagency Classification Review Committee (ICRC).

ACTION: Implementing directive.

SUMMARY: The Interagency Classification Review Committee is publishing this directive to implement Executive Order 12065, relating to the classification, downgrading, declassification and safeguarding of national security information. This directive was approved by the National Security Council for publication and issuance on September 29, 1978. The Executive order is intended to increase openness in Government by limiting classification and accelerating declassification but at the same time, providing improved protection against unauthorized disclosure for that information that requires such protection in the interest of national security. This directive sets forth guidelines to agencies on original and derivative classification, downgrading, declassification and safeguarding of national security information.

EFFECTIVE DATE: December 1, 1978.

FOR FURTHER INFORMATION CONTACT:

Robert W. Wells, Executive Director, ICRC, Telephone: 202-724-1578.

SUPPLEMENTARY INFORMATION: This directive is issued pursuant to the provisions of section 6-204 of Executive Order 12065. The purpose of the directive is to assist in the implementation of Executive Order 12065, and users of the directive shall refer concurrently to the Executive order for guidance.

TABLE OF CONTENTS

Section I. Original Classification

- A Definition.
- B Classification Authority.
- C Request for Classification Authority.
- D Record Requirements.
- E Classification Procedure.
- F Foreign Government Information.
- G Standard Identification and Markings.
- H Additional Markings Required.
- I Abbreviations.

Section II. Derivative Classification

- A Definition.
- B Responsibility.

C Marking Derivatively Classified Documents.

Section III. Declassification and Downgrading

- A Record Requirements.
- B Declassification Policy.
- C Systematic Review for Declassification.
- D Procedures for Mandatory Declassification Review.

Section IV. Safeguarding

- A General.
- B General Restrictions on Access.
- C Access by Historical Researchers and Former Presidential Appointees.
- D Dissemination.
- E Accountability Procedures.
- F Storage.
- G Transmittal.
- H Loss or Possible Compromise.
- I Destruction.

Section V. Implementation and Review: Challenges to Classification

Section VI. General Provisions

- A Notification.
- B Posted Notice.
- C Downgrading, Declassification, and Upgrading Markings.
- D Combat Operations.
- E Publication and Effective Date.

I. ORIGINAL CLASSIFICATION

A. Definition. "Original classification" as used in the order means an initial determination that information requires protection against unauthorized disclosure in the interest of national security, and a designation of the level of classification (1).¹

B. Classification authority. In the absence of an authorized classifier, anyone designated to act in that person's absence may exercise the classifier's authority (1-204).

C. Request for classification authority. Requests for original classification authority for agencies not listed in section 1-2 of the order shall be submitted to the President through the Information Security Oversight Office. Requests shall include: (1) The designation of the officials for whom or positions for which authority is sought, (2) the level of authority requested, and (3) the justification for such requests, including a description of the type of information that is anticipated to require original classification (1-2).

D. Record requirements. Agencies and officials granted original classification authority pursuant to section 1-2 of the order shall maintain a current listing, by classification designation, of individuals to whom or positions to which original classification authority has been delegated (1-2).

E. Classification procedure. Except as provided in section 1-303 of the order, the fact that the information concerns one or more of the qualifying criteria or categories of information

¹Parenthetical references are to related sections of Executive Order 12065.

shall not create any presumption as to whether information meets the criteria of section 1-303.

F. Foreign government information.—1. Identification. "Foreign government information" is:

a. Information provided to the United States by a foreign government or international organization of governments in the expectation, express or implied, that the information is to be kept in confidence; or

b. Information produced by the United States pursuant to a written joint arrangement with a foreign government or international organization of governments requiring that either the information or the arrangement, or both, be kept in confidence. Such a written joint arrangement may be evidenced by an exchange of letters, a memorandum of understanding, or other written record (1-303 and 6-103).

2. Duration of classification. Unless the guidelines developed pursuant to section 3-404 of the order or other guidelines prescribe dates or events for declassification or for review for declassification:

a. Foreign government information shall not be assigned a date or event for automatic declassification unless such is specified or agreed to by the foreign government or international organization of governments.

b. Foreign government information classified after the effective date of the order shall be assigned a date for review for declassification up to 30 years from the time the information was classified or acquired. (1-402 and 3-404).

G. Standard identification and markings. At the time of original classification, the following shall be shown on the face of paper copies of all classified documents:

1. Identity of classifier. The identity of the classifier, unless also the signer or approver of the document, shall be shown on a "classified by" line; e.g., "Classified by John Doe" or "Classified by Director, XXX" (1-501(a)).

2. Date of classification and office of origin. The date and office of origin on a document at the time of its origination may be considered the date of classification and identification of the office of origin (1-501(b)).

3. Date or event for declassification or review. The date for automatic declassification or for declassification review shall be shown on a "declassify on" or a "review for declassification on" line; e.g., "Declassify on 1 November 1984," "Declassify on completion of State visit," or "Review for declassification on 1 November 1998" (1-501(c)).

4. Downgrading markings. When it is determined (e.g., in a classification guide) that a classified document should be downgraded automatically

at a certain date or upon a certain event, that date or event shall be recorded on the face of the document; e.g., "Downgraded to Secret on 1 November 1990" or "Downgraded to Confidential on 1 December 1985" (1-5).

5. *Identity of extension authority.* The identity of the official who authorizes a date for declassification or for review for declassification that is more than 6 years beyond the date of the document's classification shall be shown on the document, unless that official also is the classifier, signer, or approver of the document. This marking shall be shown substantially as follows: "Extended by (Insert name or title of position of agency head or Top Secret classification authority)" (1-502).

6. *Reason for extension.* When classification is extended beyond 6 years, the reason shall be stated on the document either in narrative form or by reference to an agency regulation that states the reason for extension in narrative form. The reason shall be shown substantially as follows: "Reason for extension: (State reason or applicable reference)" (1-502).

7. *Overall and page marking of documents.* The overall classification of a document shall be marked, stamped, or affixed permanently 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). Each interior page of a classified document shall be marked or stamped at the top and bottom either according to the highest classification of the content of the page, including the designation "Unclassified" when appropriate, or according to the highest overall classification of the document. In any case, the classification marking of the page shall not supersede the classification marking of portions of the page marked with lower levels of classification (1-501(d)).

8. *Subject and titles.* Whenever practicable, subjects and titles shall be selected so as not to require classification. When the subject or title is classified, an unclassified identifier may be assigned to facilitate receipting and reference (1-5).

9. *Mandatory portion marking.* Classifiers shall identify the level of classification of each classified portion of a document (including subjects and titles), and those portions that are not classified. Portion marking shall be accomplished by placing a parenthetical designator immediately preceding or following the text that it governs. The symbols "(TS)" for top secret, "(S)" for secret, "(C)" for confidential, and "(U)" for unclassified shall be used for this purpose. If individual portion marking is impracticable, the document shall contain a description suffi-

cient to identify the information that is classified and the level of such classification. A waiver of the portion marking requirement may be granted by the Director of the Information Security Oversight Office. Requests for such waivers shall be made by the head of an agency or designee to the Director and shall include: (a) Identification of the information or classes of documents for which such waiver is sought, (b) a detailed explanation of why the waiver should be granted, (c) the agency's best judgment as to the anticipated dissemination of the information or class of documents for which waiver is sought, and (d) the extent to which the information subject to the waiver may form a basis for classification of other documents (1-504).

10. *Material other than documents.* The classification and associated markings prescribed by this directive of documents shall, where practicable, be affixed to material other than documents by stamping, tagging, or other means. If this is not practicable, recipients shall be made aware of the classification and associated markings by notification or other means as prescribed by the agency (1-5).

11. *Transmittal documents.* A transmittal document shall indicate on its face the highest classification of the information transmitted by it and the classification, if any, of the transmittal document. For example, an unclassified transmittal document should bear a notation substantially as follows: "Unclassified When Classified Enclosure Is Detached" (1-5).

12. *Marking foreign government information.* Except in those cases where such markings would reveal intelligence information, foreign government information incorporated in United States documents shall, whenever practicable, be identified in such manner as to ensure that the foreign government information is not declassified prematurely or made accessible to nationals of a third country without consent of the originator. Documents classified by a foreign government or an international organization of governments shall, if the foreign classification is not in English, be marked with the equivalent U.S. classification. Foreign government information not classified by a foreign government or an international organization of governments but provided to the United States in confidence by a foreign government or by an international organization of governments shall be classified at an appropriate level and shall be marked with the U.S. classification accordingly (1-5).

H. *Additional markings required.* In addition to the marking requirements in paragraph G, the following markings shall, as appropriate, be displayed

prominently on classified information. When display of these additional markings is not practicable, their applicability to the information shall be included in the written notification of the assigned classification (1-5).

1. *Restricted data or formerly restricted data.* For classified information containing restricted data or formerly restricted data as defined in the Atomic Energy Act of 1954, as amended, such markings as may be prescribed by the Department of Energy in regulations issued pursuant to the act shall be applied.

2. *Intelligence sources and methods information.* For classified information involving intelligence sources or methods: "Warning Notice—Intelligence Sources and Methods Involved".

3. *Dissemination and reproduction notice.* For classified information that the originator has determined, pursuant to section 1-506 of the order, should be subject to special dissemination or reproduction limitations, or both, a statement placing the user on notice of the restrictions shall be included in the text of the document or on its cover sheet; e.g., "Reproduction requires approval of originator," or "Further dissemination only as directed by (Insert appropriate office or official)" (1-506).

I. *Abbreviations.* Classified documents that are transmitted electrically may be marked with abbreviations or codes in a single line to satisfy the requirements of each subsection of paragraphs G and H in a manner consistent with economic and efficient use of electrical transmission systems, provided that the full text represented by each such abbreviation or code and its relation to each subsection of paragraphs G and H is readily available to each expected user of the classified documents affected.

II. DERIVATIVE CLASSIFICATION

A. *Definition.* "Derivative classification" as used in the order means a determination that information is in substance the same as information that is currently classified, and a designation of the level of classification (2-1).

B. *Responsibility.* Derivative application of 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 classifier or in accordance with an authorized classification guide. Persons who apply derivative classification markings should take care to determine whether their paraphrasing, restating, or summarizing of classified information has removed the basis for classification. Where checks with originators or other appropriate inquiries show that

classification or a lower classification than originally assigned is appropriate, the derivative classification shall be issued as unclassified or shall be marked appropriately (2-101 and 2-102).

2. *Marking derivatively classified documents.* Paper copies of derivatively classified documents shall be marked at the time of origination as follows:

a. The classification authority shall show on a "classified by" line; e.g., "Classified by (Insert identity of classification guide)" or "Classified by (Insert source of original classification)." If the classification is derived from more than one source, the single phrase "multiple sources" may be used, provided that identification of each such source is maintained with the file or record copy of the document (2-102(c));

b. The identity of the office originating the derivatively classified document shall be shown on the face of the document (2-102);

c. Dates or events for declassification or review shall be carried forward from the source material or classification guide and shown on a "declassify" or "review for declassification on" line;

d. If the classification is derived from more than one source, the latest date for declassification or review applicable to the various source materials shall be applied to the new information (2-102(c));

e. The classification marking provisions of sections I.G. 7 through 9 and I. 12 are also applicable to derivatively classified documents (2-102(c));

f. Any additional marking under section I.H. of this directive appearing on source material shall be carried forward to the new material when appropriate (2-102(c)); and

g. Any abbreviation or code permitted under section I. I. of this directive may be applied to derivatively classified documents.

3. *Classification guides.*—1. *Requirements.* Classification guides issued pursuant to section 2-2 of the order shall:

a. Identify the information to be protected, using categorization to the extent necessary to insure that the information involved can be identified readily and uniformly (2-201);

b. State which of the classification designations (i.e., top secret, secret, or confidential) applies to the information (2-201);

c. State the duration of classification in terms of a period of time or future event. When such duration is to exceed 6 years, the reason for such extension shall be provided in the guide. However, if the inclusion of classified information would result in a level of classification for a guide that would inhibit its desirable and required dissemination,

those reasons need be recorded only on or with the record copy of the document.

d. Indicate how the designations, time limits, markings, and other requirements of the order and this directive are to be applied, or make specific reference to agency regulations that provide for such application (2-201).

2. *Review and record requirements.* Each classification guide shall be kept current and shall be reviewed at least once every 2 years. Each agency shall maintain a list of all its classification guides in current use (2-2).

III. DECLASSIFICATION AND DOWNGRADING

A. *Record requirements.* Agencies and officials granted original classification authority pursuant to section 1-2 of the order shall maintain a record of individuals or positions designated as declassification authorities pursuant to section 3-103 of the order (3-103).

B. *Declassification policy.* In making determinations under section 3-303 of the order, officials shall respect the intent of the order to protect foreign government information and confidential foreign sources (3-303).

C. *Systematic Review for Declassification.*—1. *Systematic review guidelines.*

a. *U.S. originated information.* Systematic review guidelines shall be kept current through review at least every 2 years, unless earlier review for revision is requested by the Archivist of the United States (3-402).

b. *Foreign government information.* Within 1 year after the effective date of the order, heads of affected agencies shall, in consultation with the Archivist and in accordance with the provisions of section 3-404 of the order, develop systematic review guidelines for 30-year-old foreign government information. These guidelines shall be kept current through review by agency heads at least once every 2 years, unless earlier review for revision is requested by the Archivist of the United States. A copy of these guidelines and any revisions thereto shall be furnished to the Information Security Oversight Office. Upon request, the Department of State shall provide advice and such assistance as is necessary to effect foreign government coordination of the guidelines (3-404).

2. *Systematic review procedures.*—a. *Scheduling for systematic review.* Classified nonpermanent records that are scheduled to be retained for more than 20 years need not be systematically reviewed but shall be reviewed for declassification upon request. Within 60 days of the effective date of the order, heads of agencies and officials designated by the President pursuant to section 1-2 of the order shall

direct that all classified records 20 years old or older, whether held in agency or in Federal records centers, be surveyed to identify those that require scheduling for future disposition. Such scheduling shall be accomplished within 2 years of the effective date of the order (3-401).

b. *Extending classification after review.*—(1) *Foreign government information.* Agency heads listed in section 1-2 and officials designated by the President pursuant to section 1-201 of the order may extend the classification of foreign government information beyond 30 years, but only in accordance with sections 3-3 and 3-404. This authority may not be delegated. When classification is extended beyond 30 years, a date no more than 10 years later shall be set for declassification or for the next review. Subsequent reviews for declassification shall be set at no more than 10-year intervals (3-404).

(2) *Waivers of further review.* Heads of agencies listed in section 1-2 and officials designated by the President pursuant to section 1-201 of the order may request from the Director of the Oversight Office a waiver of the 10-year review requirement for both U.S.-originated and foreign government information. Such requests shall include a personal certification by the agency head that the classified information for which the waiver is sought has been systematically reviewed as required, and that a definitive date for declassification could not be determined. Waivers should not be requested unless the results of the review have established an identifiable need to continue classification for a period in excess of 20 additional years. Each request shall include a recommended date or event for subsequent review or automatic declassification (3-401).

c. *Assistance to the Archivist.*—(1) The head of each agency shall designate experienced personnel to assist the Archivist of the United States in the systematic review of 20-year-old U.S.-originated information and 30-year-old foreign government information accessioned into the National Archives of the United States. Such personnel shall:

(a) Provide guidance and assistance to National Archives employees in identifying and separating documents and specific categories of information within documents that are deemed to require continued classification; and

(b) Submit to the head of the agency recommendations for continued classification that identify documents or specific categories of information so separated.

(2) The head of the agency shall then make the determinations personally and in writing required under sec-

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080009-0

tion 3-401 of the order as to which documents or categories of information require continued protection. The agency shall inform the Archivist of the United States of this determination (3-4).

d. *Special procedures.* Special procedures for systematic review and declassification of classified cryptologic information and classified information concerning the identities of clandestine human agents promulgated in accordance with the provisions of section 3-403 of the order shall be binding on all agencies (3-403).

e. *Foreign relations series.* In order to permit the editors of foreign relations of the United States to meet their mandated goal of publishing 20 years after the event, heads of departments and agencies are requested to assist the editors in the Department of State by facilitating access to appropriate classified materials in their custody and by expediting declassification review of items from their files selected for publication (3-4).

D. *Procedures for mandatory declassification review.*

1. *U.S.-originated information.—a. Action on an initial request.* Each Agency shall designate, in its implementing regulations published in the FEDERAL REGISTER, offices to which requests for mandatory review for declassification may be directed. Upon request for declassification pursuant to section 3-5 of the order, agencies shall apply the following procedures:

(1) The designated offices shall acknowledge receipt of the request.

(2) Whenever a request does not reasonably describe the information sought, the requestor shall be notified that unless additional information is provided or the scope of the request is narrowed, no further action will be undertaken (3-501).

b. *Information in the custody of and under the exclusive declassification authority of an agency.* The designated office shall determine whether, under the declassification provisions of section 3-3 of the order, the requested information may be declassified and, if so, shall make such information available to the requestor, unless withholding is otherwise warranted under applicable law. If the information may not be released in whole or in part, the requestor shall be given a brief statement as to the reasons for denial, a notice of the right to appeal the determination to a designated agency appellate authority (including name, title, and address of such authority), and a notice that such an appeal must be filed with the agency within 60 days in order to be considered (3-501).

c. *Information classified by agencies other than the custodial agency.* When an agency receives a request for infor-

mation in its custody that was classified by another agency, it shall forward the request to the appropriate agency for review, together with a copy of the document containing the information requested where practicable, and with its recommendation to withhold any of the information where appropriate. Unless the agency that classified the information objects on grounds that its association with the information requires protection, the agency that received the request shall also notify the requestor of the referral. After the agency that classified the information completes its review (in coordination with other agencies that a direct interest in the subject matter), a response shall be sent to the requestor in accordance with the procedures described above. If requested, the agency shall also communicate its determination to the referring agency (3-501).

d. *Action on appeal.* The head of an agency or a designee shall establish procedures to act within 30 days upon all appeals of denials of requests for declassification. These procedures shall provide for meaningful appellate consideration, shall be forwarded to the Oversight Office for review, and shall be published in the FEDERAL REGISTER. In accordance with these procedures, agencies shall determine whether continued classification is required in whole or in part, notify the requestor of the determination, and make available any information that is declassified and otherwise releasable. If continued classification is required under the provisions of section 3-3 of the order, the requestor shall be notified of the reasons therefor. If requested, the agency shall also communicate the appeal determination to any referring agency (3-5 and 5-404(c)).

e. *Fees.* If the request requires the rendering of services for which fair and equitable fees may be charged pursuant to title 5 of the Independent Offices Appropriation Act, 65 Stat. 290, 31 U.S.C. 483a (1976), such fees may be imposed at the discretion of the agency rendering the services. Schedules of such fees shall be published in the FEDERAL REGISTER (3-501).

2. *Foreign government information.* Except as provided hereinafter, requests for mandatory review for the declassification of classified documents that contain foreign government information shall be processed and acted upon in accordance with the provisions of section D.1 above. If the agency receiving the request is also the agency that initially received or classified the foreign government information, it shall determine whether the foreign government information in the document may be declassified and

referral in accordance with agency policy or guidelines, after consulting with other agencies that have subject matter interest as necessary. 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, which shall take action as described above, including its recommendation to withhold any of the information where appropriate. In those cases where agency policy or guidelines do not apply, consultation with the foreign originator through appropriate channels may be advisable prior to final action on the request (3-5).

IV. SAFEGUARDING

A. *General.* Information classified pursuant to Executive Order 12065 or prior orders shall be afforded a level of protection against unauthorized disclosure commensurate with its level of classification (4-1).

B. *General restrictions on access.*

1. *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 section 4-3 of the order, that access is essential to the accomplishment of official Government duties or contractual obligations (4-101).

2. *Determination of trustworthiness.* A person is eligible for access to classified information only after a showing of trustworthiness as determined by agency heads based upon appropriate investigations in accordance with applicable standards and criteria (4-101).

C. *Access by historical researchers and former Presidential appointees.* Agencies shall obtain: (1) Written agreements from requestors to safeguard the information to which they are given access as permitted by the order and this directive; and (2) written consent to the agency's review of their notes and manuscripts for the purpose of determining that no classified information is contained therein. A determination of trustworthiness is a precondition to a requestor's access. 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, 65 Stat. 290, 31 U.S.C. 483a (1976), the requestor shall be so notified and the fees may be imposed (4-3).

D. *Dissemination.* Except as otherwise provided by section 102 of the National Security Act of 1947, 61 Stat. 495, 50 U.S.C. 403 (1970 and Supp. V 1975), classified information originating in one agency may not be disseminated outside any other agency to

which it has been made available without the consent of the originating agency (4-403).

E. Accountability procedures.—1. *Top secret.* Top secret control officers 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; however, heads of agencies may authorize the annual inventory of top secret documents in repositories, libraries, or activities that store large volumes of such information to be limited to documents to which access has been afforded within the past 12 months. The Director of the Oversight Office may grant a waiver with respect to the requirement of an annual inventory for storage systems involving large volumes of information if security measures with respect to such storage systems are adequate to prevent access by unauthorized persons (4-103).

2. *Secret and confidential.* Secret and confidential classified information shall be subject to such controls and current accountability records as the head of the agency may prescribe (4-103).

F. Storage. Classified information shall be stored only in facilities or under conditions adequate to prevent unauthorized persons from gaining access to it (4-103).

1. *Top secret.* Top secret information shall be stored in a GSA-approved, safe-type, steel file cabinet having a built-in, three-position, dial-type combination lock or within an approved vault, or vault-type room, or in other storage facility that meets the standards for top secret established under the provisions of subsection 3 below. In addition, heads of agencies shall prescribe such additional, supplementary controls as are deemed appropriate to restrict unauthorized access to areas where such information is stored (4-103).

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 or vault that meets the standards for secret or confidential, established pursuant to the provisions of subsections 3 or 4 below (4-103).

3. *Standards for security equipment.* The General Services Administration 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 categories of classified information. Any agency may establish more stringent standards for its own use. When-

ever 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 designated on the Federal Supply Schedule, General Services Administration (4-103).

4. *Exception to standards for security equipment.*—a. Secret and confidential information may also be stored in a steel filing cabinet having a built-in, three-position, dial-type, changeable combination lock, or a steel filing cabinet equipped with a steel lock bar, provided it is secured by a three-position, changeable, combination padlock approved by GSA for the purpose. The storage of secret information in the steel filing cabinets described above requires the use of such supplementary controls as the head of the agency deems necessary to achieve the degree of protection warranted by the sensitivity of the information involved (4-103).

b. For protection of bulky secret and confidential material (for example, weaponry containing classified components) in magazines, strong rooms, or closed areas, access openings may be secured by changeable combination or key-operated, high-security padlocks approved by GSA. When key-operated padlocks are used, keys shall be controlled in accordance with subsection 6 below (4-103).

5. *Combinations.*—a. *Equipment in service.* Combinations to dial-type locks shall be changed only by persons having 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 the combination, whenever a combination has been subjected to possible compromise, whenever the equipment is taken out of service, and at least once every year. Knowledge of combinations protecting classified information 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 to be stored in the security equipment concerned (4-103).

b. *Equipment out of service.* When security equipment having a built-in combination lock is taken out of service, the lock shall be reset to the standard combination 50-25-50. Combination padlocks shall be reset to the standard combination 10-20-30 (4-103).

6. *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 afford-

ed the classified information being protected. Under no circumstances may keys be removed from the premises. They shall be stored in a secure container (4-103).

7. *Responsibilities of custodians.* Persons entrusted with classified information shall be responsible for providing protection and accountability for such information at all times and for locking classified information in approved security equipment whenever it is not in use or under direct supervision of authorized persons. Custodians shall follow procedures that insure unauthorized persons do not gain access to classified information (4-103).

8. *Inspections.* Individuals charged with the custody of classified information shall conduct the necessary inspections within their areas to insure adherence to procedural safeguards prescribed to protect classified information. Agency security officers shall insure that periodic inspections are made to determine whether procedural safeguards prescribed by agency regulations are in effect at all times (4-103).

G. Transmittal.—1. *Preparation and receipting.* Classified information shall be enclosed in opaque inner and outer covers before transmitting. 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 under conditions that will provide adequate protection and prevent access by unauthorized persons (4-103).

2. *Transmittal of top secret.* The transmittal of top secret information shall be by specifically designated personnel, by State Department diplomatic pouch, by a messenger-courier system specially created for that purpose, or over authorized secure communications circuits (4-103).

3. *Transmittal of secret.* The transmittal of secret material shall be effected in the following manner:

a. *The 50 States, District of Columbia, and Puerto Rico.* Secret information may be transmitted within and between the 50 States, District of Columbia, and Puerto Rico by one of the means authorized for top secret infor-

mation, 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 (4-103).

b. *Canadian Government Installations.* Secret information may be transmitted to and between United States Government and Canadian Government installations in the 50 States, the District of Columbia, and Canada by United States and Canadian registered mail with registered mail receipt (4-103).

c. *Other areas.* Secret information may be transmitted from, to, or within areas other than those specified in subsections a or b above 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 (4-103).

4. *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 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 (4-103).

H. *Loss or possible compromise.* Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to an official designated by the agency or organization. In turn, the originating agency shall be notified about the loss or compromise in order that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect of such a compromise. An immediate inquiry shall be initiated by the agency under whose cognizance the loss or compromise occurred, for the purpose of taking corrective measures and appropriate administrative, disciplinary, or legal action (4-103).

I. *Destruction.* Nonrecord classified information that has served its intended purpose shall be destroyed in accordance with procedures and methods approved by the head of the agency. The method of destruction selected must preclude recognition or reconstruction of the classified information or material (4-103).

V. IMPLEMENTATION AND REVIEW

Challenges to classification. Agency programs established to implement the order shall encourage holders of classified information to challenge classification in cases where there is reasonable cause to believe that information is classified unnecessarily, improperly, or for an inappropriate period of time. These programs shall provide for action on such challenges or appeals relating thereto within 30 days of receipt and for notification to the challenger of the results. When requested, anonymity of the challenger shall be preserved (5-404(d)).

VI. GENERAL PROVISIONS

A. *Notification.* Notification of unscheduled changes in classification or changes in duration of classification may be by general rather than specific notice (4-102).

B. *Posted notice.* If prompt remark-

ing of large quantities of information would be unduly burdensome, the custodian may attach a change of classification notice to the storage unit in lieu of the marking action otherwise required. Each notice shall indicate the change, the authority for the action, the date of the action, and the storage units to which it applies. Items permanently withdrawn from such storage units shall be marked promptly in accordance with the marking provisions herein. However, when information subject to a posted downgrading, upgrading, or declassification notice is withdrawn from one storage unit solely for transfer to another, or a storage unit containing such information is transferred from one place to another, the transfer may be made without marking if the notice is attached to or remains with each shipment (4-102).

C. *Downgrading, declassification, and upgrading 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 (4-102).

D. *Combat operations.* The provisions of the order and this Directive with regard to dissemination, transmittal, or safeguarding of classified information may be so modified in connection with combat or combat-related operations as the Secretary of Defense may by regulations prescribe (4-103).

E. *Publication and effective date.* This directive shall be published in the FEDERAL REGISTER. It shall become effective December 1, 1978 (6-204).

JAMES B. RHOADS,
Acting Chairman, Interagency
Classification Review Committee.

OCTOBER 2, 1978.

(FR Doc. 78-28101 Filed 10-4-78; 8:45 am)

ORIGINAL CL BY _____
 DECL REW ON _____
EXT BYND 6 YRS BY _____
REASON _____

DERIVATIVE CL BY _____
 DECL REW ON _____
DERIVED FROM _____

02

CL DERIVED BY _____
 DECL REW ON _____
DERIVED FROM _____

**MONDAY, JULY 3, 1978
PART IV**



THE PRESIDENT

■

**NATIONAL SECURITY
INFORMATION**

**Executive Order 12065
and Order Designating
Certain Officials
Within the Executive
Office of the President
To Classify
Information**

Revised Order

presidential documents

[3195-01]

Title 3—The President

Executive Order 12065

June 28, 1978

National Security Information

By the authority vested in me as President by the Constitution and laws of the United States of America, in order to balance the public's interest in access to Government information with the need to protect certain national security information from disclosure, it is hereby ordered as follows:

TABLE OF CONTENTS

	<i>[FR page]</i>
SECTION 1. ORIGINAL CLASSIFICATION:	
1-1 Classification Designation	[28950]
1-2 Classification Authority	[28950]
1-3 Classification Requirements	[28951]
1-4 Duration of Classification	[28952]
1-5 Identification and Markings	[28952]
1-6 Prohibitions	[28953]
SECTION 2. DERIVATIVE CLASSIFICATION:	
2-1 Use of Derivative Classification	[28953]
2-2 Classification Guides	[28953]
2-3 New Material	[28954]
SECTION 3. DECLASSIFICATION AND DOWNGRADING:	
3-1 Declassification Authority	[28954]
3-2 Transferred Information	[28954]
3-3 Declassification Policy	[28955]
3-4 Systematic Review for Declassification	[28955]
3-5 Mandatory Review for Declassification	[28956]
3-6 Downgrading	[28957]
SECTION 4. SAFEGUARDING:	
4-1 General Restrictions	[28957]
4-2 Special Access Programs	[28957]
4-3 Access by Historical Researchers and Former Presidential Appointees	[28958]
4-4 Reproduction Controls	[28958]
SECTION 5. IMPLEMENTATION AND REVIEW:	
5-1 Oversight	[28959]
5-2 Information Security Oversight Office	[28959]
5-3 Interagency Information Security Committee	[28960]
5-4 General Responsibilities	[28960]
5-5 Administrative Sanctions	[28961]
SECTION 6. GENERAL PROVISIONS:	
6-1 Definitions	[28961]
6-2 General	[28961]

28950

THE PRESIDENT

SECTION 1. ORIGINAL CLASSIFICATION.

1-1. *Classification Designation.*

1-101. Except as provided in the Atomic Energy Act of 1954, as amended, this Order provides the only basis for classifying information. Information may be classified in one of the three designations listed below. If there is reasonable doubt which designation is appropriate, or whether the information should be classified at all, the less restrictive designation should be used, or the information should not be classified.

1-102. "Top Secret" shall be applied only to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

1-103. "Secret" shall be applied only to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

1-104. "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause identifiable damage to the national security.

1-2. *Classification Authority.*

1-201. *Top Secret.* Authority for original classification of information as Top Secret may be exercised only by the President, by such officials as the President may designate by publication in the FEDERAL REGISTER, by the agency heads listed below, and by officials to whom such authority is delegated in accordance with Section 1-204:

- The Secretary of State
- The Secretary of the Treasury
- The Secretary of Defense
- The Secretary of the Army
- The Secretary of the Navy
- The Secretary of the Air Force
- The Attorney General
- The Secretary of Energy
- The Chairman, Nuclear Regulatory Commission
- The Director, Arms Control and Disarmament Agency
- The Director of Central Intelligence
- The Administrator, National Aeronautics and Space Administration
- The Administrator of General Services (delegable only to the Director, Federal Preparedness Agency and to the Director, Information Security Oversight Office)

1-202. *Secret.* Authority for original classification of information as Secret may be exercised only by such officials as the President may designate by publication in the FEDERAL REGISTER, by the agency heads listed below, by officials who have Top Secret classification authority, and by officials to whom such authority is delegated in accordance with Section 1-204:

- The Secretary of Commerce
- The Secretary of Transportation
- The Administrator, Agency for International Development
- The Director, International Communication Agency

1-203. *Confidential.* Authority for original classification of information as Confidential may be exercised only by such officials as the President may designate by publication in the FEDERAL REGISTER, by the agency heads listed below, by officials who have Top Secret or Secret classification authority, and by officials to whom such authority is delegated in accordance with Section 1-204:

THE PRESIDENT

28951

The President and Chairman, Export-Import Bank of the United States
The President and Chief Executive Officer, Overseas Private Investment Corporation

1-204. Limitations on Delegation of Classification Authority.

(a) Authority for original classification of information as Top Secret may be delegated only to principal subordinate officials who have a frequent need to exercise such authority as determined by the President or by agency heads listed in Section 1-201.

(b) Authority for original classification of information as Secret may be delegated only to subordinate officials who have a frequent need to exercise such authority as determined by the President, by agency heads listed in Sections 1-201 and 1-202, and by officials with Top Secret classification authority.

(c) Authority for original classification of information as Confidential may be delegated only to subordinate officials who have a frequent need to exercise such authority as determined by the President, by agency heads listed in Sections 1-201, 1-202, and 1-203, and by officials with Top Secret classification authority.

(d) Delegated original classification authority may not be redelegated.

(e) Each delegation of original classification authority shall be in writing by name or title of position held.

(f) Delegations of original classification authority shall be held to an absolute minimum. Periodic reviews of such delegations shall be made to ensure that the officials so designated have demonstrated a continuing need to exercise such authority.

1-205. Exceptional Cases. When an employee or contractor of an agency that does not have original classification authority originates information believed to require classification, the information shall be protected in the manner prescribed by this Order and implementing directives. The information shall be transmitted promptly under appropriate safeguards to the agency which has appropriate subject matter interest and classification authority. That agency shall decide within 30 days whether to classify that information. If it is not clear which agency should get the information, it shall be sent to the Director of the Information Security Oversight Office established in Section 5-2 for a determination.

1-3. Classification Requirements.

1-301. Information may not be considered for classification unless it concerns:

- (a) military plans, weapons, or operations;
- (b) foreign government information;
- (c) intelligence activities, sources or methods;
- (d) foreign relations or foreign activities of the United States;
- (e) scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities; or

(g) other categories of information which are related to national security and which require protection against unauthorized disclosure as determined by the President, by a person designated by the President pursuant to Section 1-201, or by an agency head.

1-302. Even though information is determined to concern one or more of the criteria in Section 1-301, it may not be classified unless an original classification authority also determines that its unauthorized disclosure reasonably could be expected to cause at least identifiable damage to the national security.

28952

THE PRESIDENT

1-303. Unauthorized disclosure of foreign government information or the identity of a confidential foreign source is presumed to cause at least identifiable damage to the national security.

1-304. Each determination under the criterion of Section 1-301(g) shall be reported promptly to the Director of the Information Security Oversight Office.

1-4. Duration of Classification.

1-401. Except as permitted in Section 1-402, at the time of the original classification each original classification authority shall set a date or event for automatic declassification no more than six years later.

1-402. Only officials with Top Secret classification authority and agency heads listed in Section 1-2 may classify information for more than six years from the date of the original classification. This authority shall be used sparingly. In such cases, a declassification date or event, or a date for review, shall be set. This date or event shall be as early as national security permits and shall be no more than twenty years after original classification, except that for foreign government information the date or event may be up to thirty years after original classification.

1-5. Identification and Markings.

1-501. At the time of original classification, the following shall be shown on the face of paper copies of all classified documents:

- (a) the identity of the original classification authority;
- (b) the office of origin;
- (c) the date or event for declassification or review; and
- (d) one of the three classification designations defined in Section 1-1.

1-502. Documents classified for more than six years shall also be marked with the identity of the official who authorized the prolonged classification. Such documents shall be annotated with the reason the classification is expected to remain necessary, under the requirements of Section 1-3, despite the passage of time. The reason for the prolonged classification may be stated by reference to criteria set forth in agency implementing regulations. These criteria shall explain in narrative form the reason the information needs to be protected beyond six years. If the individual who signs or otherwise authenticates a document also is authorized to classify it, no further annotation of identity is required.

1-503. Only the designations prescribed by this Order may be used to identify classified information. Markings such as "For Official Use Only" and "Limited Official Use" may not be used for that purpose. Terms such as "Conference" or "Agency" may not be used in conjunction with the classification designations prescribed by this Order; e.g., "Agency Confidential" or "Conference Confidential."

1-504. In order to facilitate excerpting and other uses, each classified document shall, by marking or other means, indicate clearly which portions are classified, with the applicable classification designation, and which portions are not classified. The Director of the Information Security Oversight Office may, for good cause, grant and revoke waivers of this requirement for specified classes of documents or information.

1-505. Foreign government information shall either retain its original classification designation or be assigned a United States classification designation that shall ensure a degree of protection equivalent to that required by the entity that furnished the information.

1-506. Classified documents that contain or reveal information that is subject to special dissemination and reproduction limitations authorized by

THE PRESIDENT

28953

this Order shall be marked clearly so as to place the user on notice of the restrictions.

1-6. Prohibitions.

1-601. Classification may not be used to conceal violations of law, inefficiency, or administrative error, to prevent embarrassment to a person, organization or agency, or to restrain competition.

1-602. Basic scientific research information not clearly related to the national security may not be classified.

1-603. A product of non-government research and development that does not incorporate or reveal classified information to which the producer or developer was given prior access may not be classified under this Order until and unless the government acquires a proprietary interest in the product. This Order does not affect the provisions of the Patent Secrecy Act of 1952 (35 U.S.C. 181-188).

1-604. References to classified documents that do not disclose classified information may not be classified or used as a basis for classification.

1-605. Classification may not be used to limit dissemination of information that is not classifiable under the provisions of this Order or to prevent or delay the public release of such information.

1-606. No document originated on or after the effective date of this Order may be classified after an agency has received a request for the document under the Freedom of Information Act or the Mandatory Review provisions of this Order (Section 3-5), unless such classification is consistent with this Order and is authorized by the agency head or deputy agency head. Documents originated before the effective date of this Order and subject to such a request may not be classified unless such classification is consistent with this Order and is authorized by the senior official designated to oversee the agency information security program or by an official with Top Secret classification authority. Classification authority under this provision shall be exercised personally, on a document-by-document basis.

1-607. Classification may not be restored to documents already declassified and released to the public under this Order or prior Orders.

SECTION 2. DERIVATIVE CLASSIFICATION.**2-1. Use of Derivative Classification.**

2-101. Original classification authority shall not be delegated to persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide.

2-102. Persons who apply such derivative classification markings shall:

- (a) respect original classification decisions;
- (b) verify the information's current level of classification so far as practicable before applying the markings; and
- (c) carry forward to any newly created documents the assigned dates or events for declassification or review and any additional authorized markings, in accordance with Sections 2-2 and 2-301 below. A single marking may be used for documents based on multiple sources.

2-2. Classification Guides.

2-201. Classification guides used to direct derivative classification shall specifically identify the information to be classified. Each classification guide shall specifically indicate how the designations, time limits, markings, and other requirements of this Order are to be applied to the information.

28954

THE PRESIDENT

2-202. Each such guide shall be approved personally and in writing by an agency head listed in Section 1-2 or by an official with Top Secret classification authority. Such approval constitutes an original classification decision.

2-3. *New Material.*

2-301. New material that derives its classification from information classified on or after the effective date of this Order shall be marked with the declassification date or event, or the date for review, assigned to the source information.

2-302. New material that derives its classification from information classified under prior Orders shall be treated as follows:

(a) If the source material bears a declassification date or event twenty years or less from the date of origin, that date or event shall be carried forward on the new material.

(b) If the source material bears no declassification date or event or is marked for declassification beyond twenty years, the new material shall be marked with a date for review for declassification at twenty years from the date of original classification of the source material.

(c) If the source material is foreign government information bearing no date or event for declassification or is marked for declassification beyond thirty years, the new material shall be marked for review for declassification at thirty years from the date of original classification of the source material.

SECTION 3. DECLASSIFICATION AND DOWNGRADING.

3-1. *Declassification Authority.*

3-101. The authority to declassify or downgrade information classified under this or prior Orders shall be exercised only as specified in Section 3-1.

3-102. Classified information may be declassified or downgraded by the official who authorized the original classification if that official is still serving in the same position, by a successor, or by a supervisory official of either.

3-103. Agency heads named in Section 1-2 shall designate additional officials at the lowest practicable echelons to exercise declassification and downgrading authority.

3-104. If the Director of the Information Security Oversight Office determines that information is classified in violation of this Order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the National Security Council. The information shall remain classified until the appeal is decided or until one year from the date of the Director's decision, whichever occurs first.

3-105. The provisions of this Order relating to declassification shall also apply to agencies which, under the terms of this Order, do not have original classification authority but which had such authority under prior Orders.

3-2. *Transferred Information.*

3-201. For classified information transferred in conjunction with a transfer of functions—not merely for storage purposes—the receiving agency shall be deemed to be the originating agency for all purposes under this Order.

3-202. For classified information not transferred in accordance with Section 3-201, but originated in an agency which has ceased to exist, each agency in possession shall be deemed to be the originating agency for all purposes under this Order. Such information may be declassified or downgraded by the agency in possession after consulting with any other agency having an interest in the subject matter.

3-203. Classified information transferred to the General Services Administration for accession into the Archives of the United States shall be declassi-

THE PRESIDENT

28955

fied or downgraded by the Archivist of the United States in accordance with this Order, the directives of the Information Security Oversight Office, and the agency guidelines.

3-204. After the termination of a Presidential administration, the Archivist of the United States shall review and declassify or downgrade all information classified by the President, the White House Staff, committees or commissions appointed by the President, or others acting on the President's behalf. Such declassification shall only be undertaken in accordance with the provisions of Section 3-504.

3-3. Declassification Policy.

3-301. Declassification of classified information shall be given emphasis comparable to that accorded classification. Information classified pursuant to this and prior Orders shall be declassified as early as national security considerations permit. Decisions concerning declassification shall be based on the loss of the information's sensitivity with the passage of time or on the occurrence of a declassification event.

3-302. When information is reviewed for declassification pursuant to this Order or the Freedom of Information Act, it shall be declassified unless the declassification authority established pursuant to Section 3-1 determines that the information continues to meet the classification requirements prescribed in Section 1-3 despite the passage of time.

3-303. It is presumed that information which continues to meet the classification requirements in Section 1-3 requires continued protection. In some cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head, a senior agency official with responsibility for processing Freedom of Information Act requests or Mandatory Review requests under this Order, an official with Top Secret classification authority, or the Archivist of the United States in the case of material covered in Section 3-503. That official will determine whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure.

3-4. Systematic Review for Declassification.

3-401. Classified information constituting permanently valuable records of the Government, as defined by 44 U.S.C. 2103, and information in the possession and control of the Administrator of General Services, pursuant to 44 U.S.C. 2107 or 2107 note, shall be reviewed for declassification as it becomes twenty years old. Agency heads listed in Section 1-2 and officials designated by the President pursuant to Section 1-201 of this Order may extend classification beyond twenty years, but only in accordance with Sections 3-3 and 3-402. This authority may not be delegated. When classification is extended beyond twenty years, a date no more than ten years later shall be set for declassification or for the next review. That date shall be marked on the document. Subsequent reviews for declassification shall be set at no more than ten year intervals. The Director of the Information Security Oversight Office may extend the period between subsequent reviews for specific categories of documents or information.

3-402. Within 180 days after the effective date of this Order, the agency heads listed in Section 1-2 and the heads of agencies which had original classification authority under prior orders shall, after consultation with the Archivist of the United States and review by the Information Security Oversight Office, issue and maintain guidelines for systematic review covering twenty-year old classified information under their jurisdiction. These guide-

THE PRESIDENT

lines shall state specific, limited categories of information which, because of their national security sensitivity, should not be declassified automatically but should be reviewed item-by-item to determine whether continued protection beyond twenty years is needed. These guidelines shall be authorized for use by the Archivist of the United States and may, upon approval of the issuing authority, be used by any agency having custody of the information. All information not identified in these guidelines as requiring review and for which a prior automatic declassification date has not been established shall be declassified automatically at the end of twenty years from the date of original classification.

3-403. Notwithstanding Sections 3-401 and 3-402, the Secretary of Defense may establish special procedures for systematic review and declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review and declassification of classified information concerning the identities of clandestine human agents. These procedures shall be consistent, so far as practicable, with the objectives of Sections 3-401 and 3-402. Prior to implementation, they shall be reviewed and approved by the Director of the Information Security Oversight Office and, with respect to matters pertaining to intelligence sources and methods, by the Director of Central Intelligence. Disapproval of procedures by the Director of the Information Security Oversight Office may be appealed to the National Security Council. In such cases, the procedures shall not be implemented until the appeal is decided.

3-404. Foreign government information shall be exempt from automatic declassification and twenty year systematic review. Unless declassified earlier, such information shall be reviewed for declassification thirty years from its date of origin. Such review shall be in accordance with the provisions of Section 3-3 and with guidelines developed by agency heads in consultation with the Archivist of the United States and, where appropriate, with the foreign government or international organization concerned. These guidelines shall be authorized for use by the Archivist of the United States and may, upon approval of the issuing authority, be used by any agency having custody of the information.

3-405. Transition to systematic review at twenty years shall be implemented as rapidly as practicable and shall be completed no more than ten years from the effective date of this Order.

3-5. Mandatory Review for Declassification.

3-501. Agencies shall establish a mandatory review procedure to handle requests by a member of the public, by a government employee, or by an agency, to declassify and release information. This procedure shall apply to information classified under this Order or prior Orders. Except as provided in Section 3-503, upon such a request the information shall be reviewed for possible declassification, provided the request reasonably describes the information. Requests for declassification under this provision shall be acted upon within 60 days. After review, the information or any reasonably segregable portion thereof that no longer requires protection under this Order shall be declassified and released unless withholding is otherwise warranted under applicable law.

3-502. Requests for declassification which are submitted under the provisions of the Freedom of Information Act shall be processed in accordance with the provisions of that Act.

3-503. Information less than ten years old which was originated by the President, by the White House Staff, or by committees or commissions appointed by the President, or by others acting on behalf of the President, including such information in the possession and control of the Administrator

THE PRESIDENT

38957

of General Services pursuant to 44 U.S.C. 2107 or 2107 note, is exempted from the provisions of Section 3-501. Such information over ten years old shall be subject to mandatory review for declassification. Requests for mandatory review shall be processed in accordance with procedures developed by the Archivist of the United States. These procedures shall provide for consultation with agencies having primary subject matter interest. Any decision by the Archivist may be appealed to the Director of the Information Security Oversight Office. Agencies with primary subject matter interest shall be notified promptly of the Director's decision on such appeals and may further appeal to the National Security Council through the process set forth in Section 3-104.

3-504. Requests for declassification of classified documents originated by an agency but in the possession and control of the Administrator of General Services, pursuant to 44 U.S.C. 2107 or 2107 note, shall be referred by the Archivist to the agency of origin for processing in accordance with Section 3-501 and for direct response to the requestor. The Archivist shall inform requestors of such referrals.

3-505. No agency in possession of a classified document may, in response to a request for the document made under the Freedom of Information Act or this Order's Mandatory Review provision, refuse to confirm the existence or non-existence of the document, unless the fact of its existence or non-existence would itself be classifiable under this Order.

3-6. Downgrading.

3-601. Classified information that is marked for automatic downgrading is downgraded accordingly without notification to holders.

3-602. Classified information that is not marked for automatic downgrading may be assigned a lower classification designation by the originator or by other authorized officials when such downgrading is appropriate. Notice of downgrading shall be provided to holders of the information to the extent practicable.

SECTION 4. SAFEGUARDING.

4-1. General Restrictions on Access.

4-101. No person may be given access to classified information unless that person has been determined to be trustworthy and unless access is necessary for the performance of official duties.

4-102. All classified information shall be marked conspicuously to put users on notice of its current classification status and, if appropriate, to show any special distribution or reproduction restrictions authorized by this Order.

4-103. Controls shall be established by each agency to ensure that classified information is used, processed, stored, reproduced, and transmitted only under conditions that will provide adequate protection and prevent access by unauthorized persons.

4-104. 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 of the United States Code, which governs disposition of Federal records.

4-105. Classified information disseminated outside the Executive branch shall be given protection equivalent to that afforded within the Executive branch.

4-2. Special Access Programs.

4-201. Agency heads listed in Section 1-201 may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this Order or prior Orders. Such pro-

THE PRESIDENT

grams may be created or continued only by written direction and only by those agency heads and, for matters pertaining to intelligence sources and methods, by the Director of Central Intelligence. Classified information in such programs shall be declassified according to the provisions of Section 3.

4-202. Special access programs may be created or continued only on a specific showing that:

(a) normal management and safeguarding procedures are not sufficient to limit need-to-know or access;

(b) the number of persons who will need access will be reasonably small and commensurate with the objective of providing extra protection for the information involved; and

(c) the special access controls balance the need to protect the information against the full spectrum of needs to use the information.

4-203. All special access programs shall be reviewed regularly and, except those required by treaty or international agreement, shall terminate automatically every five years unless renewed in accordance with the procedures in Section 4-2.

4-204. Within 180 days after the effective date of this Order, agency heads shall review all existing special access programs under their jurisdiction and continue them only in accordance with the procedures in Section 4-2. Each of those agency heads shall also establish and maintain a system of accounting for special access programs. The Director of the Information Security Oversight Office shall have non-delegable access to all such accountings.

4-3. Access by Historical Researchers and Former Presidential Appointees.

4-301. The requirement in Section 4-101 that access to classified information may be granted only as is necessary for the performance of official duties may be waived as provided in Section 4-302 for persons who:

(a) are engaged in historical research projects, or

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

4-302. Waivers under Section 4-301 may be granted only if the agency with jurisdiction over the information:

(a) makes a written determination that access is consistent with the interests of national security;

(b) takes appropriate steps to ensure that access is limited to specific categories of information over which that agency has classification jurisdiction;

(c) limits the access granted to former Presidential appointees to items that the person originated, reviewed, signed or received while serving as a Presidential appointee.

4-4. Reproduction Controls.

4-401. Top Secret documents may not be reproduced without the consent of the originating agency unless otherwise marked by the originating office.

4-402. Reproduction of Secret and Confidential documents may be restricted by the originating agency.

4-403. Reproduced copies of classified documents are subject to the same accountability and controls as the original documents.

4-404. Records shall be maintained by all agencies that reproduce paper copies of classified documents to show the number and distribution of reproduced copies of all Top Secret documents, of all documents covered by special access programs distributed outside the originating agency, and of all Secret and all Confidential documents which are marked with special dissemination and reproduction limitations in accordance with Section 1-506.

4-405. Sections 4-401 and 4-402 shall not restrict the reproduction of documents for the purpose of facilitating review for declassification. However,

THE PRESIDENT

28959

such reproduced documents that remain classified after review must be destroyed after they are used.

SECTION 5. IMPLEMENTATION AND REVIEW.**5-1. Oversight.**

5-101. The National Security Council may review all matters with respect to the implementation of this Order and shall provide overall policy direction for the information security program.

5-102. The Administrator of General Services shall be responsible for implementing and monitoring the program established pursuant to this Order. This responsibility shall be delegated to an Information Security Oversight Office.

5-2. Information Security Oversight Office.

5-201. The Information Security Oversight Office shall have a full-time Director appointed by the Administrator of General Services subject to approval by the President. The Administrator also shall have authority to appoint a staff for the Office.

5-202. The Director shall:

(a) oversee agency actions to ensure compliance with this Order and implementing directives;

(b) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program, including appeals from decisions on declassification requests pursuant to Section 3-503;

(c) exercise the authority to declassify information provided by Sections 3-104 and 3-503;

(d) develop, in consultation with the agencies, and promulgate, subject to the approval of the National Security Council, directives for the implementation of this Order which shall be binding on the agencies;

(e) report annually to the President through the Administrator of General Services and the National Security Council on the implementation of this Order;

(f) review all agency implementing regulations and agency guidelines for systematic declassification review. The Director shall require any regulation or guideline to be changed if it is not consistent with this Order or implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation or guideline shall remain in effect until the appeal is decided or until one year from the date of the Director's decision, whichever occurs first.

(g) exercise case-by-case classification authority in accordance with Section 1-205 and review requests for original classification authority from agencies or officials not granted original classification authority under Section 1-2 of this Order; and

(h) have the authority to conduct on-site reviews of the information security program of each agency that handles classified information and to require of each agency such reports, information, and other cooperation as necessary to fulfill his responsibilities. If such reports, inspection, or access to specific categories of classified information would pose an exceptional national security risk, the affected agency head may deny access. The Director may appeal denials to the National Security Council. The denial of access shall remain in effect until the appeal is decided or until one year from the date of the denial, whichever occurs first.

28960

THE PRESIDENT

5-3. *Interagency Information Security Committee.*

5-301. There is established an Interagency Information Security Committee which shall be chaired by the Director and shall be comprised of representatives of the Secretaries of State, Defense, Treasury, and Energy, the Attorney General, the Director of Central Intelligence, the National Security Council, the Domestic Policy Staff, and the Archivist of the United States.

5-302. Representatives of other agencies may be invited to meet with the Committee on matters of particular interest to those agencies.

5-303. The Committee shall meet at the call of the Chairman or at the request of a member agency and shall advise the Chairman on implementation of this order.

5-4. *General Responsibilities.*

5-401. A copy of any information security regulation and a copy of any guideline for systematic declassification review which has been adopted pursuant to this Order or implementing directives, shall be submitted to the Information Security Oversight Office. To the extent practicable, such regulations and guidelines should be unclassified.

5-402. Unclassified regulations that establish agency information security policy and unclassified guidelines for systematic declassification review shall be published in the FEDERAL REGISTER.

5-403. Agencies with original classification authority shall promulgate guides for security classification that will facilitate the identification and uniform classification of information requiring protection under the provisions of this Order.

5-404. Agencies which originate or handle classified information shall:

- (a) designate a senior agency official to conduct an active oversight program to ensure effective implementation of this Order;
- (b) designate a senior agency official to chair an agency committee with authority to act on all suggestions and complaints with respect to the agency's administration of the information security program;
- (c) establish a process to decide appeals from denials of declassification requests submitted pursuant to Section 3-5;
- (d) establish a program to familiarize agency and other personnel who have access to classified information with the provisions of this Order and implementing directives. This program shall impress upon agency personnel their responsibility to exercise vigilance in complying with this Order. The program shall encourage agency personnel to challenge, through Mandatory Review and other appropriate procedures, those classification decisions they believe to be improper;
- (e) promulgate guidelines for systematic review in accordance with Section 3-402;
- (f) establish procedures to prevent unnecessary access to classified information, including procedures which require that a demonstrable need for access to classified information is established before initiating administrative clearance procedures, and which ensures that the number of people granted access to classified information is reduced to and maintained at the minimum number that is consistent with operational requirements and needs; and
- (g) ensure that practices for safeguarding information are systematically reviewed and that those which are duplicative or unnecessary are eliminated.

5-405. Agencies shall submit to the Information Security Oversight Office such information or reports as the Director of the Office may find necessary to carry out the Office's responsibilities.

THE PRESIDENT

28961

5-5. *Administrative Sanctions.*

5-501. If the Information Security Oversight Office finds that a violation of this Order or any implementing directives may have occurred, it shall make a report to the head of the agency concerned so that corrective steps may be taken.

5-502. Officers and employees of the United States Government shall be subject to appropriate administrative sanctions if they:

(a) knowingly and willfully classify or continue the classification of information in violation of this Order or any implementing directives; or

(b) knowingly, willfully and without authorization disclose information properly classified under this Order or prior Orders or compromise properly classified information through negligence; or

(c) knowingly and willfully violate any other provision of this Order or implementing directive.

5-503. Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, or other sanction in accordance with applicable law and agency regulations.

5-504. Agency heads shall ensure that appropriate and prompt corrective action is taken whenever a violation under Section 5-502 occurs. The Director of the Information Security Oversight Office shall be informed when such violations occur.

5-505. Agency heads shall report to the Attorney General evidence reflected in classified information of possible violations of Federal criminal law by an agency employee and of possible violations by any other person of those Federal criminal laws specified in guidelines adopted by the Attorney General.

SECTION 6. GENERAL PROVISIONS.

6-1. *Definitions.*

6-101. "Agency" has the meaning defined in 5 U.S.C. 552(e).

6-102. "Classified information" means information or material, herein collectively termed information, that is owned by, produced for or by, or under the control of, the United States Government, and that has been determined pursuant to this Order or prior Orders to require protection against unauthorized disclosure, and that is so designated.

6-103. "Foreign government information" means information that has been provided to the United States in confidence by, or produced by the United States pursuant to a written joint arrangement requiring confidentiality with, a foreign government or international organization of governments.

6-104. "National security" means the national defense and foreign relations of the United States.

6-105. "Declassification event" means an event which would eliminate the need for continued classification.

6-2. *General.*

6-201. Nothing in this Order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended. "Restricted Data" and information designated as "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued pursuant thereto.

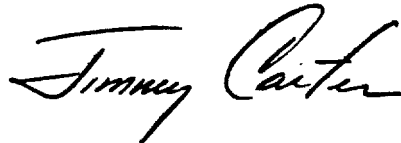
6-202. The Attorney General, upon request by the head of an agency, his duly designated representative, or the Director of the Information Security Oversight Office, shall personally or through authorized representatives of the Department of Justice render an interpretation of this Order with respect to any question arising in the course of its administration.

28962

THE PRESIDENT

6-203. Executive Order No. 11652 of March 8, 1972, as amended by Executive Order No. 11714 of April 24, 1973, and as further amended by Executive Order No. 11862 of June 11, 1975, and the National Security Council Directive of May 17, 1972 (3 CFR 1085 (1971-75 Comp.)) are revoked.

6-204. This Order shall become effective on December 1, 1978, except that the functions of the Information Security Oversight Office specified in Sections 5-202(d) and 5-202(f) shall be effective immediately and shall be performed in the interim by the Interagency Classification Review Committee established pursuant to Executive Order No. 11652.



THE WHITE HOUSE,
June 28, 1978.

[FR Doc. 78-18505 Filed 6-29-78; 4:18 pm]

EDITORIAL NOTE: The President's statement of June 29, 1978, on issuing Executive Order 12065, is printed in the Weekly Compilation of Presidential Documents (vol. 14, No. 26).

THE PRESIDENT

28963

[3195-01]

Order of June 28, 1978

Designation of Certain Officials Within the Executive Office of the President To Classify National Security Information

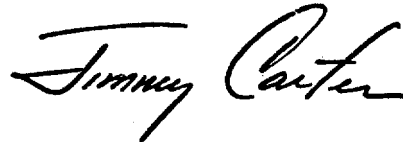
Pursuant to the provisions of Section 1-201 of Executive Order 12065 of June 28, 1978, entitled "National Security Information", I hereby designate the following officials within the Executive Office of the President to originally classify information as "Top Secret"

The Vice President
The Assistant to the President for National Security Affairs
The Director, Office of Management and Budget
The Director, Office of Science and Technology Policy
The Special Representative for Trade Negotiations
The Chairman, Intelligence Oversight Board

Pursuant to the provisions of Section 1-202 of said Order, I designate the Chairman of the Council of Economic Advisers and the President's Personal Representative for Micronesian Status Negotiations to originally classify information as "Secret".

Any delegation of this authority shall be in accordance with Section 1-204 of the Order.

This Order shall be published in the FEDERAL REGISTER.



THE WHITE HOUSE,
June 28, 1978.

[FR Doc. 78-18506 Filed 6-29-78; 4:19 pm]

STAT

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080009-0

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080009-0