

DD/A Registry
81-201

3 MAR 1981

DD/A Registry

81-0475

MEMORANDUM FOR: Deputy Director for Administration

FROM: Thomas H. White
Director of Information Services

DD/A REGISTRY
FILE: OAM-1

SUBJECT: Request for Release [redacted]
[redacted] to the National Security Agency

STAT

STAT

1. On 11 February 1981, Regulations Control Division briefed [redacted] from NSA concerning the CIA regulatory system. The briefing was arranged at the request of the NSA Deputy Director for Plans and Policy who wishes to improve the NSA regulatory system.

STAT

2. [redacted] has requested copies of four CIA regulatory issuances: [redacted] (controlled by "AIUO") [redacted] [redacted] (unclassified) which she considers would be useful in setting up a more efficient and centralized regulatory system at NSA.

STAT
STAT
STAT

STAT

3. Since regulatory issuances are promulgated for Agency employee use only, exceptions to make these issuances available outside the Agency must be approved by the Deputy Director for Administration with the concurrence of any other Deputy Director concerned, if appropriate.

4. NSA will be requested to return these issuances to CIA when they have served NSA purposes. Third Agency rule restricting duplication of these copies will apply.

/s/ Thomas H. White

Thomas H. White

Attachments:

- A.
- B.
- C.
- D.

[redacted]

STAT

APPROVAL:

/s/ William N. Hart

Deputy Director for Administration

5 MAR 1981

Date

for

STAT

Approved For Release 2004/05/05 : CIA-RDP84B00890R000400070071-1

Approved For Release 2004/05/05 : CIA-RDP84B00890R000400070071-1

ADMINISTRATIVE—INTERNAL USE ONLY

STAT

ORGANIZATION



k. INFORMATION SERVICES STAFF

(1) MISSION

- (a) The Chief, Information Services Staff is responsible for planning and managing the Agency Records Management Program, coordinating and responding to public requests under the Freedom of Information and Privacy Acts, implementing Executive Order 12065 concerning national security classification and declassification of Agency records and other information, and maintaining the Agency regulatory system.
- (b) The Chief, Information Services Staff (ISS) is designated the Agency Security Classification Officer, Agency Declassification Officer, Agency Records Management Officer, Agency Archivist, and the officer responsible for liaison with the National Archives and Records Service (NARS) and its Office of the Federal Register. The Chief, ISS is authorized to redelegate in writing these responsibilities to other individuals on the staff. The Chief, ISS also serves as Head of the MI Career Sub-Group; DDA representative to the Public Affairs Advisory Group and the Publications Review Board; Executive Secretary of the Information Review Committee (IRC); Chairman of the IRC Working Group; DCI representative on the Interagency Information Security Committee; and the Agency's focal point for contact with the Information Security Oversight Office.

(2) FUNCTIONS. The Chief, Information Services Staff directs:


- (a) **The Records Management Division (RMD).** Through its components this division directs the Agency Records Management Program which provides for controls over the creation, maintenance, use, and disposition of all Agency records; develops and encourages the application of standards, procedures, and techniques designed to improve the management of records; ensures the maintenance and security of records of permanent value; and facilitates the segregation and disposal of records of temporary value. RMD also is responsible for the Agency Security Classification Program as required by Executive Order 12065. The chief of the division serves as the DDA Records Management Officer.
- (b) **The Information and Privacy Division (IPD).** This division receives and processes all requests submitted to the Agency under the Freedom of Information and Privacy Acts and the mandatory classification review provisions of Executive Order 12065. IPD reviews the requests to determine if sufficient information has been provided to initiate a records search; acknowledges receipt of requests within statutory time requirements; assigns records search and/or review tasks to appropriate Agency components, and provides guidance to them on the interpretation of requesters' queries and on sanitization and release of materials; prepares responses to requesters with the assistance of components that maintain the requested records; assesses processing fees or waives fees as appropriate; processes appeals on denied requests; conducts liaison with other Government agencies regarding the processing of requests; and prepares reports for Congress or other Governmental elements as required by law or Executive order.
- (c) **The Classification Review Division (CRD).** This division manages the Agency program for systematic classification review under Executive Order 12065. CRD establishes systematic classification review guidelines, develops and implements systematic classification review procedures, and prepares classification guides in coordination with other Agency components and the Agency Security Classification Officer. CRD also maintains liaison with other U.S. Government agencies concerning the systematic review of permanent records over which they or the Agency have classification jurisdiction.

L

STAT ADMINISTRATIVE—INTERNAL USE ONLY



ORGANIZATION

- ⌞ (d) **The Regulations Control Division (RCD)**. This division directs and monitors the processing, coordination, and publication of Agency regulatory issuances. RCD is responsible for maintaining editorial standards, working directly with initiators and coordinators of regulatory issuances to resolve substantive differences during coordination, ensuring that time limits imposed by  for completing the regulatory process are adhered to, and preparing coordinated regulatory issuances for the Director of Central Intelligence, Deputy Director for Administration, or Deputy Director for Operations approval.

STA

⌞ (3) **ORGANIZATION**. See organization chart, figure 26.

I. Not Used.

Approved For Release 2004/05/05 : CIA-RDP84B00890R000400070071-1

Approved For Release 2004/05/05 : CIA-RDP84B00890R000400070071-1

INFORMATION AND RECORDS MANAGEMENT

2. CLASSIFICATION REVIEW

SYNOPSIS. This regulation prescribes classification review policies, responsibilities, and functions associated with the Agency information security program.

a. **AUTHORITY.** The authority for Agency classification and declassification policies and procedures is derived from Executive Order 12065, "National Security Information," and from Information Security Oversight Office directives issued pursuant to that order.

25X1

[redacted] establishes the Agency information security program implementing the order and assigns responsibilities for its execution. Program policy and procedures are set forth in HHB

25X1

[redacted]

b. **GENERAL.** Except for mandatory review responsibilities and functions under the Privacy Act, Freedom of Information Act, and Executive Order 12065, the Agency's classification review program is centrally directed and monitored by the Classification Review Division, Information Services Staff, Directorate of Administration (CRD/ISS/DDA). To provide for the expertise required, CRD recruits throughout the Agency for both rotational and permanent assignments. CRD includes, but is not limited to, representatives from the National Foreign Assessment Center and the Directorates of Administration, Science and Technology, and Operations.

c. **DEFINITIONS**

25X1

(1) **RECORD** (See [redacted])

(2) **INFORMATION** is the content or any portion of a record.

(3) **SYSTEMATIC REVIEW** is the methodical examination of records in accordance with officially promulgated guidelines and procedures to determine whether continued security classification is required, and the registration of each such determination.

(4) **OFFICIALLY PROMULGATED GUIDELINES AND PROCEDURES** are instructions and procedures issued by Agency components to identify information that warrants continued classification in the interests of the national security under the requirements of Executive Order 12065 and implementing directives or regulations issued pursuant thereto.

(5) **PERMANENT RECORDS** are records that are to be retained permanently according to records control schedules approved by the Archivist of the United States.

d. **RESPONSIBILITIES AND FUNCTIONS.** The Classification Review Division:

(1) Is responsible for the centralized direction, conduct, and management of the Agency program for systematic classification review required under Executive Order 12065. This program provides for the systematic review of all permanent Agency records twenty years of age and older, including the records of predecessor organizations whose responsibilities and functions are now held by the Agency, and of information in records of non-Agency origin over which the Agency has classification jurisdiction.

(2) Develops, processes, and maintains systematic classification review guidelines, in coordination with other Agency components and in consultation with the Archivist of the United States, for review by the Information Security Oversight Office and approval by the Director of Central Intelligence.

(3) Develops procedures for declassification and related functions and monitors their application throughout the Agency.

(4) Develops and maintains classification guides in coordination with other Agency components and with the Agency Security Classification Officer.

25X1

INFORMATION AND RECORDS MANAGEMENT

- (5) Systematically reviews permanent records containing classified information to determine whether the information continues to require national security classification protection at the level initially assigned or at a lower or higher level, and
 - (a) Declassifies or authorizes the declassification of records determined no longer to require that protection; or
 - (b) Downgrades or upgrades the classification of records determined to require continued protection at a level different from that initially assigned.
- (6) Recommends to the DCI that information determined under systematic or other review procedures to require classification protection beyond twenty years, or thirty years in the case of foreign government information, be so certified as required by Executive Order 12065.
- (7) Creates and maintains appropriate records concerning implementation of the review program, including the machine records systems used to register systematic classification review determinations.
- (8) Advises the Records Management Division, ISS, concerning permanent Agency and predecessor organization records that have been declassified, so that such records may be considered for accession by the National Archives and Records Service (NARS).
- (9) Assists the Archivist of the United States in reviewing for declassification those documents and information in the permanent holdings of the National Archives for which CIA has original or final classification authority; maintains liaison with appropriate NARS officials in order to render this assistance and to ensure that NARS and Agency policies and procedures for such reviews are in harmony.
- (10) Establishes and maintains liaison, as necessary, with other United States Government agencies or departments that hold classified Agency records or copies thereof and with those whose own classified records or copies thereof may be included in Agency records.
- (11) Conducts reviews, in consultation with other Agency components as appropriate, of manuscripts submitted by the Department of State prior to issuance in the unclassified "Foreign Relations of the United States" series in order to ensure that no Agency-related information requiring continued classification protection is published.
- (12) Carries out, as assigned, other functions and responsibilities relating to classification, extension of classification, and declassification including review of writings and texts of oral presentations submitted to the Agency by present and former employees and referred to the DDA for such review by the Agency Publications Review Board.

INFORMATION AND RECORDS MANAGEMENT



25X1

**AGENCY
INFORMATION SECURITY
PROGRAM HANDBOOK**

**CLASSIFYING, DECLASSIFYING, MARKING AND
SAFEGUARDING NATIONAL SECURITY INFORMATION**

DISTRIBUTION: SPECIAL

INFORMATION AND RECORDS MANAGEMENT

FOREWORD

25X

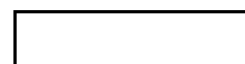
FOREWORD

This handbook prescribes the procedures for implementing Executive Order 12065 within the Agency.

John F. Blake
Deputy Director
for
Administration

DISTRIBUTION: SPECIAL

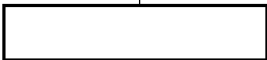
28 November 1978



CONTENTS

<u>Paragraph</u>	<u>Title</u>	<u>Page</u>
CHAPTER I: GENERAL		
1.	PURPOSE AND AUTHORITY	1
CHAPTER II: CLASSIFICATION DESIGNATION, DURATION, REQUIREMENTS, AND PROHIBITIONS		
2.	CLASSIFICATION DESIGNATION	3
3.	DURATION OF CLASSIFICATION	3
4.	PROHIBITIONS	5
5.	CLASSIFICATION REQUIREMENTS	5
CHAPTER III: ORIGINAL AND DERIVATIVE CLASSIFICATION AUTHORITY, PROCEDURES, CRITERIA, AND GUIDES		
6.	CLASSIFICATION AUTHORITY	7
7.	LIMITATIONS ON DELEGATION OF CLASSIFICATION AUTHORITY	7
8.	CLASSIFICATION AUTHORITY DELEGATION PROCEDURES	7
9.	CENTRAL INTELLIGENCE AGENCY CLASSIFICATION CRITERIA	9
	a. MILITARY PLANS, WEAPONS, OR OPERATIONS	9
	b. FOREIGN GOVERNMENT INFORMATION	9
	c. INTELLIGENCE ACTIVITIES, SOURCES, OR METHODS	9
	d. FOREIGN RELATIONS OR FOREIGN ACTIVITIES OF THE UNITED STATES	10
	e. SCIENTIFIC, TECHNOLOGICAL, OR ECONOMIC MATTERS RELATING TO THE NATIONAL SECURITY	11
	f. UNITED STATES GOVERNMENT PROGRAMS FOR SAFEGUARDING NUCLEAR MATERIALS OR FACILITIES	11
	g. OTHER CATEGORIES OF INFORMATION RELATED TO NATIONAL SECURITY AND DETERMINED BY THE DIRECTOR OF CENTRAL INTELLIGENCE TO REQUIRE PROTECTION AGAINST UNAUTHORIZED DISCLOSURE	11
10.	DERIVATIVE CLASSIFICATION AUTHORITY AND PROCEDURES	11
11.	CLASSIFICATION GUIDES	13
CHAPTER IV: IDENTIFICATION AND MARKING OF CLASSIFIED INFORMATION		
12.	IDENTIFICATION AND MARKINGS	15
	a. OVERALL AND PAGE MARKINGS	15
	b. CLASSIFICATION AUTHORITY AND DURATION MARKINGS	15
	(1) Originally Classified Documents	15
	(2) Derivatively Classified Documents	16
	c. AUTOMATIC DOWNGRADING MARKING	16
	d. PORTION MARKING	17
	e. ADDITIONAL MARKINGS	17
	(1) Restricted Data or Formerly Restricted Data	17
	(2) Intelligence Sources and Methods Information	17
	(3) Foreign Government Information	18
	(4) Dissemination and Reproduction Notice	18

25X1



INFORMATION AND RECORDS MANAGEMENT

<u>Paragraph</u>	<u>Title</u>	<u>Page</u>
	f. MARKING TRANSMITTAL DOCUMENTS	18
	g. MARKING FORMS	18
	h. MARKING ELECTRICALLY TRANSMITTED DOCUMENTS	19
	i. MARKING MATERIAL OTHER THAN DOCUMENTS	20
 CHAPTER V: DECLASSIFICATION AND DOWNGRADING		
13.	DECLASSIFICATION AND DOWNGRADING POLICY	23
14.	AUTHORITY TO DECLASSIFY OR DOWNGRADE CLASSIFIED INFORMATION	24
15.	SYSTEMATIC REVIEW FOR DECLASSIFICATION	25
16.	MANDATORY REVIEW FOR DECLASSIFICATION	27
 CHAPTER VI: SAFEGUARDING CLASSIFIED INFORMATION (Reserved)		
 CHAPTER VII: SANCTIONS (Reserved)		
	Figure 1, Sample Memorandum <u>Figure</u>	21

INFORMATION AND RECORDS MANAGEMENT

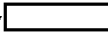



25

CHAPTER I: GENERAL

I. PURPOSE AND AUTHORITY

25X1

This handbook implements the Agency information security program established by  It should be used in conjunction with  and other regulatory issuances published pursuant to the program.

25

28 November 1978

1-2

CHAPTER II: CLASSIFICATION DESIGNATION, DURATION, REQUIREMENTS, AND PROHIBITIONS

2. CLASSIFICATION DESIGNATION

National security information shall be classified by the Agency at one of the three levels designated by E.O. 12065 set forth below. No other classification designations shall be used.

- a. Information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security, shall be classified **Top Secret**.
- b. Information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security, shall be classified **Secret**.
- c. Information, the unauthorized disclosure of which reasonably could be expected to cause identifiable damage to the national security, shall be classified **Confidential**.

3. DURATION OF CLASSIFICATION

Information shall remain classified only as long as its unauthorized disclosure reasonably could be expected to result in at least identifiable damage to the national security. At the time information is classified, it shall be marked with the date or event whose occurrence would make continued classification unnecessary or would make review for declassification appropriate, whichever is earlier. This date or event for automatic declassification, or for review for declassification, must not exceed six years from the date of classification unless it is determined that unauthorized disclosure of the information reasonably could be expected to result in at least identifiable damage to the national security even after a period of six years. In the latter case the information shall be classified for a longer period as provided hereunder. (If the information is not marked with such a date or event it will become automatically declassified in six years.)

- a. Only the DCI or other Agency officials having Top Secret original classification authority may authorize a classification period exceeding six years. Originally classified information that is so designated shall be identified with the authority and reason for the extended classification, as provided in paragraph d below.
- b. When it is determined at the time of initial classification that information should remain classified for a period in excess of six years but designation of a specific date or event for automatic declassification is impossible, the information shall be marked with a date or event for declassification review.
- c. In no case shall the date or event for automatic declassification, or for review for declassification, be set at more than 20 years, except that foreign government information (paragraph 9b below) may be classified for up to 30 years prior to declassification or review. Earlier dates for declassification or review shall be established when appropriate.
- d. Information for which classification is extended by an original Top Secret classifier shall be marked as specified in paragraph 12b(1) below. The reason for extension shall be indicated on the information either in narrative form or by citing one or more of the basic justifications for extension set forth hereunder, which summarize those provided in approved Agency classification guides (paragraph 3e below). Such citations (e.g., 3d3) constitute the Top Secret classifier's certification that the information is expected to retain its national security sensitivity, and therefore requires

INFORMATION AND RECORDS MANAGEMENT

3e

continued protection, during the entire classification period assigned. The following citations may be used, as applicable, for information that:

- (1) Is foreign government information, as described in paragraph 9b below, provided to or acquired by the United States Government with the expressed or implied expectation that its confidentiality would be maintained for a period exceeding six years in length.
 - (2) Pertains to United States Government programs for safeguarding nuclear materials or facilities (paragraph 9f below) and is determined by the Department of Energy or its predecessor agencies, pursuant to the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011, et seq.), to require continued protection beyond six years.
 - (3) Could reveal intelligence activities, sources or methods including CIA missions, functions, organizational or financial data and personnel matters, as further described in paragraph 9c below, which require protection for longer than six years.
 - (4) Is cryptologic information requiring protection beyond six years in accordance with procedures promulgated by the Secretary of Defense pursuant to Executive Order 12065 and approved as to intelligence sources and methods by the Director of Central Intelligence, or pertains to other cryptographic matters requiring such protection.
 - (5) Otherwise concerns intelligence or counterintelligence programs or activities (paragraph 9c below) and could, if disclosed after six years, result in action to negate or impede such activities or programs or expose United States intelligence or counterintelligence vulnerabilities or capabilities.
 - (6) Pertains to a military plan, weapon or weapons system or operation as described in paragraph 9a below and could, if disclosed after six years, result in nullification or reduction in the effectiveness of such a plan, weapon, system, or operation or could otherwise deprive the United States of a military advantage.
 - (7) Concerns diplomatic or other foreign relations matters or activities as described in paragraph 9d below and could, if disclosed after six years, result in action to counter, nullify, or impede the orderly implementation of United States foreign policies, or could deprive the United States of a diplomatic, economic, scientific or technological (paragraph 9e below), or other informational advantage.
 - (8) Could, if revealed after six years, place a person in jeopardy.
- e. Agency guides for derivative classification (paragraph 11 below) set forth for each category of classifiable information a level and duration of classification and, where applicable, a justification for extension of classification beyond six years. The guides reflect a series of original classification decisions made by officials having Top Secret classification authority, in accordance with paragraph a above. Therefore, the guides shall be followed by derivative classifiers in setting classification levels and duration limits, and may also be followed by original classifiers having Top Secret, Secret, or Confidential classification authority. In such cases the information is derivatively classified and shall be marked as specified in paragraph 12b(2) below. Derivative classifiers, and original classifiers having Secret or Confidential authority, otherwise must refer any decisions as to classification of information for periods in excess of six years to officials with original Top Secret classification authority. As provided in paragraph a above, original Top Secret classifiers may extend classification without reference to a guide upon determination based on their knowledge, experience, or common sense that an initial classification period of six years or less would be inappropriate for the information being classified, subject to the provisions of paragraphs 3b, c, and d above.
- f. Top Secret or Secret information shall be marked with a date or event for automatic downgrading to appropriate lower classification levels whenever it can be determined that the occurrence of such a

INFORMATION AND RECORDS MANAGEMENT

25X

4

date or event would sufficiently reduce the degree of national security damage that unauthorized disclosure of the information could cause.

4. PROHIBITIONS

Information shall not be classified in contravention of any provision of E.O. 12065, including the specific prohibitions cited below.

- a. Classification shall not be used:
 - (1) To conceal violations of law or inefficiency or administrative error;
 - (2) To prevent embarrassment to a person, organization, or U.S. Government agency;
 - (3) To restrain competition;
 - (4) To limit dissemination of information that is not classifiable under the Order; or
 - (5) To prevent or delay the public release of such information.
- b. Basic scientific research information not clearly related to the national security shall not be classified.
- c. A product of nongovernmental research that does not incorporate or reveal classified information to which the producer or developer was given prior access shall not be classified until and unless the U.S. Government acquires a proprietary interest in the product. Provisions of the Patent Secrecy Act of 1952 (35 U.S.C. 181-188) are not affected by E.O. 12065.
- d. References to classified documents that do not, in and of themselves, disclose classified information shall not be classified or used as a basis for classification.
- e. No unclassified documents originated on or after 1 December 1978 shall be classified after the Agency has received a request for the document under the Freedom of Information Act (5 U.S.C. 552) or under other mandatory review provisions cited below (paragraph 16) unless:
 - (1) Such classification is consistent with E.O. 12065, and
 - (2) Is authorized personally and in writing by the Director or Deputy Director of Central Intelligence.
- f. Unclassified documents originated prior to 1 December 1978 and subject to FOIA or other mandatory review requests shall not be classified unless such classification is consistent with the Order and is authorized by an official with Top Secret classifying authority.
- g. Classification authority under paragraphs 4e and 4f above shall be exercised personally on a document-by-document basis.
- h. Classification shall not be restored to any document or other item of information that has already been:
 - (1) Declassified (paragraphs 13 through 16 below), and
 - (2) Officially released to the public.

5. CLASSIFICATION REQUIREMENTS

Information may be classified **only** if it concerns one or more of the categories cited in E.O. 12065, as subcategorized in paragraph 9 below, and an official having original classification authority (paragraph 6 below) determines that its unauthorized disclosure is presumed, or reasonably could be expected, to cause at least identifiable damage to the national security.

- a. Such determinations are specified in the Classification Guides authorized for use by derivative classifiers (paragraph 11 below) and may also be made individually by original classifiers provided that the decision to classify that information is not inconsistent with other requirements specified herein or prohibited under any provision of paragraph 4 above.

28 November 1978

5

25X1



INFORMATION AND RECORDS MANAGEMENT

5b

- b. Information to which the above provisions apply shall be classified Top Secret, Secret, or Confidential as appropriate, depending on the degree of damage to the national security that its unauthorized disclosure could cause (paragraph 2 above).
- c. Since the unauthorized disclosure of foreign government information or of a confidential foreign source is **presumed** to cause at least identifiable damage to the national security, all such information may be classified at the Confidential level unless a more restrictive classification is specified by the foreign government(s) or international organization(s) of governments concerned or is otherwise appropriate, or if that presumption is shown to be invalid.
- d. If there is reasonable doubt whether an item of information should be classified Confidential, Secret, or Top Secret, or whether it should be classified at all, the less restrictive classification shall be used or the information shall not be classified.



CHAPTER III: ORIGINAL AND DERIVATIVE CLASSIFICATION AUTHORITY, PROCEDURES, CRITERIA, AND GUIDES

6. CLASSIFICATION AUTHORITY

- a. Authority for original classification of information as Top Secret shall be exercised within the Agency only by the DCI and by principal subordinate officials having frequent need to exercise such authority whom the DCI may designate in writing.
- b. Authority for original classification of information as Secret shall be exercised within the Agency only by officials having Top Secret classification authority, and by subordinates having frequent need to exercise such authority whom the following officials having Top Secret classification authority may designate in writing: the DCI, DDCI, Deputy Directors, Heads of Independent Offices, or Operating Officials.
- c. Authority for original classification of information as Confidential shall be exercised within the Agency only by officials having Top Secret or Secret classification authority, and by subordinates having frequent need to exercise such authority whom the following officials having Top Secret classification authority may designate in writing: the DCI, DDCI, Deputy Directors, Heads of Independent Offices, or Operating Officials.
- d. Authority for derivative classification of information at all three classification levels shall be exercised within the Agency only by officials having original classification authority, and by subordinates having frequent need to exercise such authority whom the following officials may designate in writing: the DCI, DDCI, Deputy Directors, Heads of Independent Offices, or Operating Officials.
- e. An employee or contractor who originates or obtains information believed to require classification but who lacks classification authority:
 - (1) Shall protect the information in accordance with this handbook; and
 - (2) Shall promptly transmit it under appropriate safeguards to an official having classification authority and appropriate subject-matter interest, who shall thereupon assume classification responsibility for the information. Following any necessary consultation, the responsible official shall decide within 30 days whether and at what level to classify the information.

7. LIMITATIONS ON DELEGATION OF CLASSIFICATION AUTHORITY

- a. Delegations of classification authority shall be held to an absolute minimum.
- b. Original classification authority shall not be delegated to Agency personnel who only quote, restate, extract, paraphrase, or summarize classified information or who only apply classification markings derived from source material or as directed by classification guides (paragraphs 10 and 11 below). Such personnel must be delegated derivative classification authority.
- c. Classification authority may not be redelegated.

8. CLASSIFICATION AUTHORITY DELEGATION PROCEDURES

- a. Since National Security Classification Authority (NSCA) is delegated only to officials who exercise such authority in the performance of their assigned duties, the positions they occupy are authorized

INFORMATION AND RECORDS MANAGEMENT

8b

for a particular level of NSCA. Once a position is officially designated for Top Secret, Secret, or Confidential original NSCA or for Derivative NSCA, future occupants acquire such authority by means of the personnel action assigning them to the position. In the case of a multiple incumbency position, NSCA is delegated to all persons assigned to the position.

- b. To initiate or change NSCA for a position, the following procedures will apply:
- (1) To establish Top Secret original NSCA for a position, the requesting office must submit a memorandum through the appropriate Deputy Director, Head of Independent Office, or Operating Official, to the Records Administration Branch, Information Systems Analysis Staff (RAB/ISAS), stating the position number that requires the authority, the position title, the incumbent, and the reason the authority is needed. RAB will prepare a consolidated memorandum for all offices for approval by the DCI.
 - (2) To establish Secret or Confidential original NSCA or Derivative NSCA for a position, a memorandum of delegation containing the same information specified in (1) above must be signed by the appropriate Deputy Director, Head of Independent Office, or Operating Official, and sent to RAB/ISAS.
 - (3) To change NSCA for a position, a memorandum to upgrade, downgrade, or cancel the NSCA must be submitted to RAB/ISAS following the instructions in paragraph 8b(1) or (2) above, as appropriate.
- c. Upon receipt of an approved NSCA delegation memorandum, RAB/ISAS will inform the Position Management and Compensation Division, Office of Personnel, which will make the necessary changes to the staffing complement. RAB/ISAS will forward a copy of the approved delegation memorandum to the requesting office which must then submit a Form 1152, Request for Personnel Action, for each incumbent of the position, containing the following items of information:
- (1) In section 3, indicate "Delegation of NSCA" or "Change of NSCA," as appropriate.
 - (2) In section 7, under NSCA, indicate "0001" for Top Secret, "0002" for Secret, "0003" for Confidential, "0004" for Derivative, or "0000" for Cancellation.
 - (3) In section 18, include a statement citing, by origin and date, the specific memorandum that authorized NSCA for the position.
- d. Personnel lose their NSCA upon rotation unless the new position is specified in the staffing complement as an NSCA position. In that case, the reassignment personnel action, which must include the information required in paragraph 8c above, designates authority for the individual's new assignment, and a separate memorandum to RAB/ISAS is not required. The Office of Personnel will not process personnel actions in which the designated NSCA is inconsistent with the NSCA specified for the position in the staffing complement.
- e. If an individual who requires NSCA is in an assignment category for which there is no established staffing complement position (e.g., a development complement assignment), the procedures outlined in paragraphs 8b and c above must be followed, but the NSCA will be delegated directly to the individual rather than by position. If the individual's successor also requires NSCA, a new delegation memorandum is required.
- f. During the absence of an official who has classification authority, the individual officially designated to act in the official's position may exercise the classification authority of that position.
- g. The Agency Security Classification Officer periodically will review Agency NSCA delegations to ensure that the designated officials have a continuing need to exercise such authority. Following the review, each component must submit a personnel action for each new NSCA delegation or change containing the information specified in paragraph 8c above.

INFORMATION AND RECORDS MANAGEMENT

25X

9

9. CENTRAL INTELLIGENCE AGENCY CLASSIFICATION CRITERIA

Information may be classified only if it falls within one or more of the categories set forth below and its disclosure reasonably could be expected to cause at least identifiable damage to the national security. If the information does not meet any of these criteria but should be protected because its disclosure would damage the national security, the classifier may propose that an additional category be created for that information. Requests for additional categories under paragraph 9g below shall be addressed to the Assistant for Information of the Directorate of Administration, who will obtain the concurrence of the Office of General Counsel and forward them through the Deputy Director for Administration to the Director of Central Intelligence for approval. Upon approval, the Director of the Information Security Oversight Office shall be informed of any such new categories.

a. MILITARY PLANS, WEAPONS, OR OPERATIONS

- (1) Information concerning foreign intentions, capabilities, or activities which pose a potential threat to United States national security interests or to those of allied or other friendly governments.
- (2) Information that could reveal the extent or degree of success achieved by the United States in the collection of information on and assessment of foreign military plans, weapons, capabilities, or operations.
- (3) Information that could reveal defense plans or posture of the United States, its allies, or other friendly countries or enable a foreign nation or entity to develop countermeasures to such plans or posture.
- (4) Information that could reveal the capabilities, vulnerabilities, or deployment of United States weapons or weapons systems.

b. FOREIGN GOVERNMENT INFORMATION

- (1) Information provided to the United States by any element of a foreign government, or international organization of governments, with the explicit or implicit understanding that the information is to be kept in confidence.
- (2) Information produced by the United States, whether unilaterally or jointly with a foreign government or international organization of governments, pursuant to an arrangement with any element of such government or organization evidenced by an exchange of letters, memorandum of understanding, or other written record and requiring that the information, the arrangement itself, or both be kept in confidence.
- (3) Information revealing the past, present, or proposed existence of joint intelligence activities or facilities or the nature thereof in foreign countries.

c. INTELLIGENCE ACTIVITIES, SOURCES, OR METHODS

- (1) Information that could reveal or identify a present, past, or prospective intelligence source, whether a person, organization, group, technical system, mechanism, device, or any other means or instrument that provides, has provided, or is being developed to provide foreign intelligence or foreign counterintelligence.
- (2) Information which could reveal or identify a present, past, or prospective intelligence method, procedure, mode, technique, or requirement used or being developed to acquire, transmit, analyze, correlate, evaluate, or process foreign intelligence or foreign counterintelligence or to support an intelligence source, operation, or activity.
- (3) Information not officially released that could disclose the organizational structure of the Central Intelligence Agency; the numbers and assignments of CIA personnel; the size and composition of the CIA budget, including internal and external funding; logistical and associated support activities and services; security procedures, techniques, and activities

28 November 1978

9

25X1

 INFORMATION AND RECORDS MANAGEMENT

9d

including those applicable to the fields of communications and data processing; or other quantitative or qualitative data that could reveal or indicate the nature, objectives, requirements, priorities, scope or thrust of Agency activities, including the missions, functions, and locations of certain CIA components or installations.

- (4) Information that could disclose the identities of certain CIA personnel or of code designations used by CIA or other agencies to protect such personnel or intelligence sources, methods, and activities.
- (5) Information that could reveal the existence, nature, scope, or effect of, or identify personnel covered under, agreements between the CIA and other agencies of the United States Government, elements of foreign governments, or other entities.
- (6) Information pertaining to contractual relationships with private individuals, commercial concerns, or nongovernmental institutions and entities when such a relationship involves a specific intelligence interest, or reveals the extent or depth of knowledge or technical expertise possessed by CIA, or when disclosure of the relationship could jeopardize the contractor's willingness or ability to provide services to CIA.
- (7) Information pertaining to intelligence-related methodologies, techniques, formulae, equipment, programs or models, including computer simulations, ranging from initial requirements through planning, source acquisition, contract initiation, research, design, and testing to production, personnel training, and operational use.
- (8) Information that could identify research, procedures, or data used by CIA in the acquisition and processing of foreign intelligence or counterintelligence or the production of finished intelligence, when such identification could reveal the particular intelligence interest of the CIA, the value of the intelligence, or the extent of the CIA's knowledge of a particular subject of intelligence or counterintelligence interest.
- (9) Information that could disclose CIA criteria and procedures for the handling of critical intelligence that could affect the national security of the United States or of its allies and that requires the immediate attention of senior Agency officials.
- (10) Information that could reveal, jeopardize, or compromise a cryptographic device, procedure, or system or intelligence data resulting from the employment of such a device, procedure, or system or the sites, facilities, systems, and technologies used or proposed for use in the collection, interpretation, evaluation, or dissemination of signals intelligence.
- (11) Information pertaining to training in intelligence sources, methods, and activities provided under the auspices of CIA to individuals, organizations, or groups that could reveal or identify equipment, materials, training sites, methods and techniques of instruction, or the identities of students and instructors.
- (12) Information not officially released that could disclose CIA policies and procedures used for personnel recruitment, assessment, selection, training, assignment, and evaluation.

d. FOREIGN RELATIONS OR FOREIGN ACTIVITIES OF THE UNITED STATES

- (1) Information that, if disclosed, could lead to foreign political, economic, or military action against the United States or other friendly nations.
- (2) Information that, if revealed, could create, stimulate, or increase international tensions in such manner as to impair the conduct of United States foreign policies.
- (3) Information that, if revealed, could deprive the United States of a diplomatic or economic advantage related to the national security, or that could weaken the position of the United States or its allies in international negotiations, or adversely affect other activities pertinent to the

INFORMATION AND RECORDS MANAGEMENT

10

25

resolution or avoidance of international conflicts or differences having national security significance.

- (4) Information that could disclose plans prepared, under preparation, or contemplated by officials of the United States to meet diplomatic or other contingencies affecting the security of the United States.
 - (5) Information that could identify or otherwise disclose activities conducted abroad in support of national foreign policy objectives, and planned and executed so that the role of the United States Government is not apparent or acknowledged publicly; or information that could reveal support provided to such activities.
 - (6) Information that could reveal that the United States has obtained, or seeks to obtain, certain data or materials from or concerning a foreign nation, organization, or group and thereby could adversely affect United States relations with or activities in a foreign country.
 - (7) Information that, if disclosed, could lead to political or economic instability, or to civil disorder or unrest, in a foreign country or could jeopardize the lives, liberty, or property of United States citizens residing in or visiting such a country or could endanger United States Government personnel or installations there.
- e. SCIENTIFIC, TECHNOLOGICAL, OR ECONOMIC MATTERS RELATING TO THE NATIONAL SECURITY**
- (1) Information that provides the United States with a scientific, technical, engineering, economic, or intelligence advantage of value to the national security.
 - (2) Information concerning CIA research of a scientific or technical nature leading to the development of special techniques, procedures, equipment and equipment configurations, or systems, and their use in the collection or production of foreign intelligence or foreign counterintelligence.
 - (3) Information dealing with the research and development, operational planning, deployment, or use of scientific and technical devices, equipment, or techniques used for national security purposes by the CIA jointly with, or through the cooperation of, other United States or foreign commercial, institutional, or governmental entities.
- f. UNITED STATES GOVERNMENT PROGRAMS FOR SAFEGUARDING NUCLEAR MATERIALS OR FACILITIES**
- (1) Information that could reveal, jeopardize, compromise, or reduce the effectiveness of United States Government programs to safeguard nuclear materials, techniques, capabilities, or facilities.
 - (2) Information on foreign nuclear programs, activities, capabilities, technologies, facilities, plans and intentions, weapons and their deployment that could disclose the nature, scope, or effectiveness of United States intelligence efforts to monitor nuclear developments abroad or could cause such efforts to fail or be restricted in a manner detrimental to national security.
- g. OTHER CATEGORIES OF INFORMATION RELATED TO NATIONAL SECURITY AND DETERMINED BY THE DIRECTOR OF CENTRAL INTELLIGENCE TO REQUIRE PROTECTION AGAINST UNAUTHORIZED DISCLOSURE**
(Such categories may be added later.)

10. DERIVATIVE CLASSIFICATION AUTHORITY AND PROCEDURES

- a. Derivative classification is the classification of information as prescribed by a source document or by an approved classification guide. Personnel with original classification authority may also classify

28 November 1978

11

INFORMATION AND RECORDS MANAGEMENT

10b

- information derivatively. Personnel who do not have original classification authority may classify information only if they are officially designated as derivative classifiers (paragraphs 6 and 7 above).
- b. Derivative classifiers who quote, restate, summarize, prepare extracts from, or paraphrase previously classified information shall:
- (1) Respect original classification decisions, which shall not be altered by the use of a classification level, time limit, or other marking different from the original on any copy, extract, paraphrase, restatement, or summary of any classified item except as specified under approved procedures for downgrading, declassification, or classification review or in accordance with paragraph 10b(3) below;
 - (2) Verify the information's current level of classification, insofar as it may be feasible to do so, before applying the markings; and
 - (3) Determine whether each paraphrase, restatement, extract, or summarization of classified information has removed the original basis for classification. Where checks with originators or other appropriate inquiries show that no classification or a lower level of classification than that initially assigned is applicable, the document or item shall be marked accordingly or shall be issued as unclassified.
- c. Material derivatively classified on the basis of previously classified source information is subject to the provisions set forth below.
- (1) Material that derives its classification from information classified on or after 1 December 1978 shall be marked with the declassification date or event, or the date for declassification review (paragraphs 13-15 below), and with the date or event for downgrading of classification, if any, that was assigned to the source information (paragraph 3 above).
 - (2) Material that derives its classification from information classified prior to 1 December 1978 shall be treated as follows:
 - (a) If the source material bears a declassification date or event twenty years or less from the date of initial classification, 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 classification beyond twenty years, the new material shall be marked for declassification review at twenty years from the initial classification date of the source material.
 - (c) If the source material is foreign government information (paragraph 9b above) bearing no date or event for declassification or is marked for declassification beyond thirty years, the new material shall be marked for declassification review at thirty years from the initial classification date of the source material.
 - (d) Dates or events for downgrading of classification which appear on any item of source material or information shall be assigned to new material in the manner specified under paragraphs 10c(2)(a), (b), and (c) above.
 - (e) When no separate date of classification or date for declassification, review for declassification, or downgrading appears on a source document or other item of source information, the creation date of such a document or item is considered to be the initial classification date and shall be used for marking any new material based upon that item, as specified in paragraphs 10c(2)(a), (b), (c), and (d) above.
- d. Each derivatively classified document or other item of information shall be marked in accordance with paragraph 12b(2) below.
- e. If the combined information derived from more than one source document or classification guide item requires a higher classification level or longer duration than the highest level or longest duration

INFORMATION AND RECORDS MANAGEMENT

11

prescribed by such source documents or guide items, the combined information must be classified by a person with appropriate original classification authority.

11. CLASSIFICATION GUIDES

The Agency shall promulgate classification guides to facilitate the proper and uniform classification of information. These guides may also be used to direct derivative classification.

- a. The classification guides shall be approved in writing by Deputy Directors or Heads of Independent Offices having Top Secret original classification authority. Such approval constitutes an original classification decision.
- b. The approved classification guides shall be submitted through the AI/DDA to the Deputy Director of Central Intelligence for approval as the Agency Classification Guide.
- c. The classification guides shall be based on the Agency classification criteria set forth in paragraph 9 above and shall not include any categories of information not covered therein.
- d. Each classification guide shall specify the information subject to classification in sufficient detail to permit its ready and uniform identification and shall set forth the classification level and duration in each instance as well as, where applicable, justification for any extension beyond six years.
- e. The classification guides shall be used in connection with this handbook, with particular reference to paragraph 12 on identification and markings.
- f. Personnel with derivative classification authority shall classify information as prescribed by the classification guides. Personnel with original classification authority also may classify information in this manner. In either case, the classification of information as prescribed by the guides is derivative classification, and such information shall be marked in accordance with paragraph 12b(2).
- g. Personnel with original classification authority shall ensure that their original classification decisions are consistent with the classification guides as to level and duration of classification.
- h. Access to classification guides shall be restricted to personnel requiring such access for the proper discharge of their official duties. The DDA Classification Guide is designed for Agency-wide applicability and is to be distributed accordingly.
- i. The classification guides shall be kept current and shall be fully reviewed at least every two years. The Directorates and Independent Offices shall submit all proposed additions, deletions, or other changes in the guides to the Agency Security Classification Officer, ISAS/DDA, for coordination. Approval procedures for such changes are the same as those specified in paragraphs 11a and b above. The Agency Security Classification Officer shall maintain the record copy of each guide and of all approved changes thereto.

28 November 1978

13-14

INFORMATION AND RECORDS MANAGEMENT

12

CHAPTER IV: IDENTIFICATION AND MARKING OF CLASSIFIED INFORMATION

12. IDENTIFICATION AND MARKINGS

All national security information classified by the Agency shall be identified and marked as prescribed below (see figure 1).

a. OVERALL AND PAGE MARKINGS

- (1) The highest classification level of information contained within a document shall be typed or stamped at the top and bottom of the outside 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 shall be typed 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 overall classification of the document.
- (2) Only the designations Top Secret, Secret, or Confidential may be used to identify classified information. Markings such as "For Official Use Only" and "Administrative—Internal Use Only" may not be used for that purpose. Terms such as "Medically" or "Sensitive" may not be used in conjunction with classification designations; e.g., "Medically Confidential" or "Secret/Sensitive."

b. CLASSIFICATION AUTHORITY AND DURATION MARKINGS

(1) Originally Classified Documents

In addition to the overall document classification, the following shall be shown on the face of all paper copies of originally classified documents at the time of classification:

- (a) The date and office of origin.
- (b) The identity of the classifier.
- (c) The date or event for declassification or review.
- (d) If the document is classified for more than six years:
 - (1) The identity of the Top Secret classifier who authorized the prolonged classification.
 - (2) The reason the classification is expected to remain necessary despite the passage of time.

The following marking should be typed or stamped in the lower right corner on the face of each originally classified document to identify the information specified in paragraphs 12b(1)(b) through (d) above. (This marking may be placed on the inside front cover of bound publications, provided the overall classification is marked on the outside front cover. Intelligence Information Reports may be marked in accordance with paragraph 12h below.)

ORIGINAL CL BY _____¹
 DECL REVW ON _____²
 EXT BYND 6 YRS BY _____³
 REASON _____⁴

¹ Insert the authorized classifier's employee number or other identifier approved by the Agency Security Classification Officer, ISAS/DDA. (If the authorized classifier is the signer of the document, the word "signer" may be inserted.) If the classifier does not have the required classification authority but is officially acting in the absence of an official who does have such authority, insert the classifier's employee number or other approved identifier followed by the position number of the absent official; e.g., 012345 for PG12.

25X1



INFORMATION AND RECORDS MANAGEMENT

12c

- ² Check the appropriate box to indicate whether the document is to be automatically declassified or reviewed for declassification and insert the date (day, month, year) or event for such action to occur; e.g., 1 Jan 96.
- ³ If the date or event for declassification or review exceeds six years from the date of the document, insert the employee number, or other identifier approved by the Agency Security Classification Officer, of the Top Secret classifier who is authorizing the extended classification. (If this is the same classifier as in ¹ above, the word "same" may be inserted.)
- ⁴ Cite from paragraph 3d of this handbook the applicable reason classification is expected to remain necessary for the extended period (e.g., 3d(3) or provide appropriate reason in narrative form.)

(2) **Derivatively Classified Documents**

In addition to the overall document classification, the following shall be shown on the face of all paper copies of derivatively classified documents at the time of classification.

- (a) The date and office of origin.
- (b) The identity of the derivative classifier.
- (c) The identity of the source document or classification guide item from which the classification is derived.
- (d) The date or event for declassification or review, carried forward from the source document or classification guide.

The following marking should be typed or stamped in the lower right corner on the face of each derivatively classified document to provide the information specified in paragraphs 12b(2)(b) through (d) above. (This marking may be placed on the inside front cover of bound publications, provided the overall classification is marked on the outside front cover.)

DERIVATIVE CL BY _____¹
 DECL REVW ON _____²
 DERIVED FROM _____³

- ¹ Insert the derivative classifier's employee number or other identifier approved by the Agency Security Classification Officer, ISAS/DDA. (If the derivative classifier is the signer of the document, the word "signer" may be inserted.)
- ² Insert the date (day, month, year) or event for automatic declassification or review for declassification carried forward from the source document or classification guide; e.g., 1 Jan 96. If the classification is derived from more than one source, insert the latest date or event. (See paragraph 10c of this handbook for further instructions on declassification dates for derivatively classified information.)
- ³ Cite the source document (e.g., Memo from AB to D/CD dtd 1 Jan 78, Subj: Class. Markings) or the classification guide item (e.g., C9b3.2) from which the classification is derived. If the classification is derived from more than one source, the word "multiple" may be inserted, provided the originator ensures that the identification of each source is shown on the Agency's record copy of the document.

c. AUTOMATIC DOWNGRADING MARKING

If automatic downgrading is appropriate and can be predetermined, or is prescribed by a classification guide or source document, the following marking will be stamped or typed on the face of classified documents in addition to the classification authority and duration marking:

Downgrade to (classification) on (date).

INFORMATION AND RECORDS MANAGEMENT

25X1

12d

d. PORTION MARKING

- (1) Each classified document shall indicate which paragraphs or other portions, including subjects and titles, are classified and which are unclassified. The intent is to eliminate uncertainty as to which portions of a document contain information that must be protected and to facilitate excerpting and declassification review. The symbol "(TS)" for Top Secret, "(S)" for Secret, "(C)" for Confidential, or "(U)" for Unclassified will be placed immediately following the portion of text to which it applies. Industrial contractors involved in Agency-related contractual activities may place the appropriate symbol immediately preceding the portion of text to which it applies. Nontextual portions of a document, such as photographs, graphs, charts, and maps, will be marked in a readily discernible manner, as will their captions. If the name or title of the signer of a document is classified, the typed name or title will be followed by the appropriate classification symbol.
- (2) Subjects and title should be selected so as not to require classification. When a classified subject or title must be used, a short title or other unclassified identifier should be assigned to facilitate receipting and reference, if such an identifier (e.g., a report number or registry number) will not otherwise be assigned.
- (3) If individual portion marking is impracticable, the document must contain a description sufficient to identify the information that is classified and the level of such classification. This may be done by including a statement as the last paragraph of the document or as a footnote or postscript; e.g., "Paragraphs 1, 2, and 4 are Secret, all other portions Unclassified." If all portions of a document are classified at the same level, this may be indicated either by marking each portion or by including a statement; e.g., "All portions of this document are Confidential."
- (4) Waivers from the portion marking requirement may be granted only by the Director of the Information Security Oversight Office (ISOO). Requests for waivers from Agency components must be submitted to RMD/ISS for approval by the Chief, Information Services Staff, DDA, and forwarding to ISOO. Such requests must 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 office'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.

e. ADDITIONAL MARKINGS**(1) Restricted Data or Formerly Restricted Data**

Classified information containing Restricted Data or Formerly Restricted Data as defined in the Atomic Energy Act of 1954, as amended, shall be marked as appropriate:

RESTRICTED DATA

This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.

or

FORMERLY RESTRICTED DATA

Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in Foreign Dissemination. Section 144.b., Atomic Energy Act of 1954.

(2) Intelligence Sources and Methods Information

Classified information involving intelligence sources and methods will be prominently marked:

25X1



12f

INFORMATION AND RECORDS MANAGEMENT

WARNING NOTICE

INTELLIGENCE SOURCES AND METHODS INVOLVED

This marking may be abbreviated "WNINTEL" in electrical communications, in data processing systems, and for reference purposes.

(3) Foreign Government Information

Documents containing foreign government information will be prominently marked:

CONTAINS FOREIGN GOVERNMENT INFORMATION

This marking may be abbreviated "FGI" in electrical communications, in data processing systems, and for reference purposes. Where the fact of foreign origin is so sensitive that it must be concealed from normal recipients of the document, the foreign government information markings should not be used and the document should be marked as if it were wholly of U.S. origin—including a duration of classification not to exceed 20 years.

(4) Dissemination and Reproduction Notice

For classified information that the originator has determined is subject to special dissemination and reproduction controls, a statement notifying the user of the restrictions shall be included in the text of the document or on its face; e.g., "Reproduction requires approval of originator" or "Further dissemination only as directed by (insert appropriate office or official)." This form of control should be limited to information that is so sensitive that other means of control would not offer sufficient protection to the information. Offices receiving authorization to reproduce paper copies of such documents must maintain records showing the number and distribution of reproduced copies.

f. MARKING TRANSMITTAL DOCUMENTS

A transmittal document that contains only unclassified information or information classified lower than the information transmitted by it shall indicate both its own classification and the highest classification of the information transmitted. Type or stamp at the top and bottom of each page of such a transmittal document the highest classification designation of the transmitted information, and in the lower right corner on its face, type or stamp a marking such as:

Unclassified When Detached from (Enclosure) (Attachment)

or

(Classification) When Detached from (Enclosure) (Attachment)

When the transmittal document itself is unclassified, no classification authority and duration marking or portion marking should appear thereon.

g. MARKING FORMS

(1) Only the specific classification markings that apply to each copy of a form may appear thereon. Preprinted annotations such as "Secret when filled in," or "check boxes" to select from preprinted alternative classifications, shall not be used unless approved in each case by the Agency Security Classification Officer, ISS/DDA.

(2) All copies of classified forms must indicate the classification authority and duration information specified in paragraph 12b above. To conserve space, the abbreviations in paragraph 12h below also may be used on forms. Where possible, these markings should be placed in the lower right corner of the form. The classification of the majority of forms will be derived from classification

INFORMATION AND RECORDS MANAGEMENT

12h

guides. Therefore, on most forms, the preprinted "Classification Authority and Duration Line (CADL)" would contain the following derivative classification markings:

- (a) DCL or RVW _____ —(Either the date (day, month, year) or event the form will be automatically declassified or the date or event the form will be reviewed for declassification as determined from the classification guide or source document; e.g., 1 Jan 96.)
- (b) DRV _____ —(Identity of the source from which the classification level and duration is derived; i.e., the classification guide and item number, the identity of the source document, or the word "Multiple", as appropriate.)
- (c) BY _____ —(Derivative classifier's employee number or other identifier approved by the Agency Security Classification Officer.)

A preprinted CADL on a form will normally appear, then, as:

DCL RVW _____ DRV _____ BY _____

OR

DCL RVW _____

DRV _____ BY _____

(NOTE: The CADL must also identify the classifier's office and the date the classification action took place if it is not readily evident from the content of the form.)

- (3) Forms on which the preprinted information is classified will also be preprinted with the classification level, authority, and duration markings prescribed by the originator. When information entered on these forms is determined to require a higher classification level or longer classification duration than the preprinted information, the individual making such a determination must ensure that the form is marked accordingly.
- (4) Existing stocks of forms may be used until depleted, or until 1 December 1979, whichever is sooner. During this period, the preprinted marking IMPDET will equate to "Review on (date 20 years after the date the form is filled in)". Anyone filling in a form that contains preprinted classification markings must line through any markings that do not apply to the completed form. When forms are reprinted, overprinted, or revised for any reason, they must be changed to comply fully with prescribed marking requirements.

h. MARKING ELECTRICALLY TRANSMITTED DOCUMENTS

- (1) To facilitate the efficient use of electrical transmission systems, abbreviations will be used within the message text to indicate the classification authority and duration information specified in paragraph 12b above. These abbreviations, as listed below, normally will be entered as the last line or paragraph of the text as the "Classification Authority and Duration Line (CADL)". (Examples of the use of the abbreviations are provided in paragraph 12h(2) below.)
 - (a) RVW—review for declassification on (date or event document will be reviewed for declassification).
 - (b) DCL—declassified on (date or event document will be automatically declassified).
 - (c) DRV—derived from (identity of the source from which the classification level and duration is derived; i.e., the classification guide and item number, the identity of the source document, or the word "MULTIPLE", as appropriate).
 - (d) BY—derivative classification determined by (derivative classifier's employee number or other identifier approved by the Agency Security Classification Officer).
 - (e) ORG—original classification authority is exercised by (authorized classifier's employee number or other identifier approved by the Agency Security Classification Officer).

28 November 1978

19

25X1

12i

INFORMATION AND RECORDS MANAGEMENT

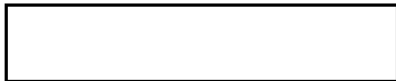
- (f) EXT—extension of classification beyond six years by (employee number, or other identifier approved by the Agency Security Classification Officer, of the Top Secret classifier who is authorizing the extended classification. This is used only when original classification authority is exercised and the date for automatic declassification or review for declassification exceeds six years).
- (g) RSN—reason for extension of classification (citation from paragraph 3d of this handbook which states the applicable reason classification is expected to remain necessary for the extended period, or reason in narrative form. This is used only when original classification authority is exercised and the date for automatic declassification or review for declassification exceeds six years).
- (h) DNG—downgraded on (the date or event when the document will be automatically downgraded. This is determined either from the classification guide or source document, or by the classifier when original classification authority is exercised).
- (i) OFF—office originating the message (this is used only when the office of origin will not otherwise be evident from the transmitted message).
- (2) To demonstrate the use of the above abbreviations in the CADL, assume that today's date is 1 January 1981, that the classifier's employee number is 011111, and that:
- (a) Classification guide item "C9b3.2" prescribes that the category of information in the message will be reviewed for declassification in 20 years.
RVW 01JAN01 DRV C9B3.2 BY 011111
- (b) Classification guide item "B8a2.1" prescribes that the category of information in the message will be automatically declassified in 15 years.
DCL 01JAN96 DRV B8A2.1 BY 011111
- (c) Original classification authority is exercised and the date for review for declassification is more than six years (in this example, 20 years).
RVW 01JAN01 ORG 011111 EXT 022222 RSN 3D3
- (d) Original classification authority is exercised and the date for automatic declassification is more than six years (in this example, 15 years).
DCL 01JAN96 ORG 011111 EXT 022222 RSN 3D3
- (e) Original classification authority is exercised and the date for review for declassification is less than six years (in this example, five years).
RVW 01JAN86 ORG 011111
- (f) Original classification authority is exercised and the date for automatic declassification is less than six years (in this example, five years).
DCL 01JAN86 ORG 011111
- (3) As with other classified documents, electrically transmitted documents must be portion (paragraph marked (see paragraph 12d above). If all portions of the message are classified at the same level, this may be indicated either by marking each portion or by inserting the appropriate classification level following the CADL. For example, if all portions of the document in paragraph 12h(2)(a) above were classified Confidential, the portion marking requirement would be satisfied by:
RVW 01JAN01 DRV C9B3.2 BY 011111 ALL CONFIDENTIAL
- (4) Where required, additional markings such as WNINTEL and FGI will be entered in the next line after the addressee/addressor lines (see paragraph 12e above).

i. MARKING MATERIAL OTHER THAN DOCUMENTS

The classification and associated markings on material other than documents shall be placed by conspicuously stamping, tagging, or other means. If the material cannot be marked, written notification of the security classification and associated markings must be furnished to any recipients of the material.

25X

INFORMATION AND RECORDS MANAGEMENT



SECRET

THIS SAMPLE MEMORANDUM DOES NOT CONTAIN CLASSIFIED INFORMATION

1 December 1978

MEMORANDUM FOR: Chief, AB Division

FROM : John C. Doe
Chief, CD Division

SUBJECT : Marking Documents in Accordance with
Executive Order 12065

25X

1. Each portion of a classified document must be marked to indicate the highest classification of information it contains. For example, this paragraph is marked as if it contained Confidential information, based on an imaginary classification guide #Z, item #9w8.7, which states that this subject matter is classified Confidential to be reviewed for declassification in 20 years.

25X

2. For purpose of illustration, assume that attached to this memo is a report which is classified Secret. Therefore, although this memo is itself only Confidential, it must alert recipients that it is transmitting a Secret document.

25X

John C. Doe

Attachment



DERIVATIVE CL BY 012345
 DECL REVW ON 01Dec98
DERIVED FROM Z9w8.7

Confidential When
Detached from Attachment

SECRET

28 November 1978

Figure 1

21-22

INFORMATION AND RECORDS MANAGEMENT



STAT

13

CHAPTER V: DECLASSIFICATION AND DOWNGRADING

13. DECLASSIFICATION AND DOWNGRADING POLICY

The declassification of classified information is accorded emphasis comparable to that accorded classification. Each item of classified information shall be declassified as early as national security considerations will allow. Criteria for the declassification and downgrading of classified information, as well as decisions concerning individual Agency documents or other items of information being considered for downgrading or declassification, shall be based on the degree to which the passage of time or the occurrence of a specific event or events may have eliminated or reduced the original national security sensitivity of such information.

- a. Agency information reviewed for declassification pursuant to E.O. 12065 and the Freedom of Information Act shall be declassified unless the responsible declassification authority (paragraph 14 below) determines that the information continues to meet the classification requirements established under paragraph 5 above at the time of such review.
- b. Information that continues to meet prescribed classification requirements despite the passage of time is presumed to require continued protection and shall not be declassified except as provided under paragraphs 13c and d below.
- c. The Executive Order provides that in some cases the need to protect properly classified information "may be outweighed by the public interest in disclosure of the information," and that "when such questions arise" the competing interests in protection and disclosure are to be balanced. The Order further provides that the information is to be declassified in such cases if the balance is struck in favor of disclosure. The drafters of the Order recognized that such cases would be rare and that declassification decisions in such cases would remain the responsibility of the Executive Branch. For purposes of these provisions, a question as to whether the public interest favoring the continued protection of properly classified information is outweighed by a public interest in the disclosure of that information will be deemed to exist only in circumstances where, in the judgment of the agency, nondisclosure could reasonably be expected to:
 - (1) Place a person's life in jeopardy.
 - (2) Adversely affect the public health and safety.
 - (3) Impede legitimate law enforcement functions.
 - (4) Impede the investigative or oversight functions of the Congress.
 - (5) Obstruct the fair administration of justice.
 - (6) Deprive the public of information indispensable to public decisions on issues of critical national importance (effective for declassification reviews conducted on or after 1 February 1980).
- d. When a case arises that requires a balancing of interests under paragraph c above, the reviewing official shall refer the matter to an Agency official having Top Secret classification authority, who shall balance. If it appears that the public interest in disclosure of the information may outweigh any continuing need for its protection, the case shall be referred with a recommendation for decision to the appropriate Deputy Director or Head of Independent Office. If those officials believe disclosure may be warranted, they, in coordination with OGC, as appropriate, shall refer the matter and a recommendation to the DDCI. If the DDCI determines that the public interest in disclosure of the information outweighs any damage to national security that might reasonably be expected to result from disclosure, the information shall be declassified.
- e. The Director of the Information Security Oversight Office may, by specific provision of E.O. 12065, require declassification of any item of information deemed to have been classified in contravention of the Order. Any such decision by the Director, ISOO may be appealed by the Director of Central Intelligence to the National Security Council; the information at issue shall remain classified until the

INFORMATION AND RECORDS MANAGEMENT

14

appeal is decided or until one year from the date of the ISOO Director's decision, whichever shall first occur. Staff work and coordination within CIA concerning such appeals or other provisions of E.O. 12065, as well as necessary liaison with the ISOO, is the responsibility of the Chief, Information Services Staff.

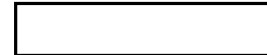
- f. Classified information may be assigned a lower level of classification than that originally assigned thereto.
- (1) This may be accomplished either automatically or by the action of duly authorized Agency officials including, but not limited to, the original classifiers of documents or other items of information being considered for downgrading of classification.
 - (2) Classified information appropriately marked for automatic downgrading (paragraph 12 above) shall be downgraded accordingly without notification to its holders.
 - (3) Classified information not marked for automatic downgrading shall be downgraded, as and when appropriate, by Agency officials authorized to do so in accordance with paragraph 13f(1) above. In such cases, holders of the information shall be notified of the downgrading action to the extent practicable.
- g. The CIA shall, as and when appropriate under any provision hereof, declassify or downgrade classified information acquired from another agency in conjunction with a transfer of functions from such other agency to the CIA. This provision shall not apply to information transferred merely for storage or other purposes unconnected with any transfer of functions.
- h. The CIA shall also declassify or downgrade information in the Agency's possession originated by any agency that has ceased to exist, but shall do so only after appropriate consultation with any other existing agency or agencies having an interest in the subject matter of such information.
- i. Classified information transferred by the CIA for accession into the Archives of the United States shall be declassified by the Archivist of the United States in accordance with E.O. 12065, applicable directives of the Information Security Oversight Office, and appropriate guidelines prepared and promulgated by the CIA pursuant thereto (paragraphs 15i through k below).

14. AUTHORITY TO DECLASSIFY OR DOWNGRADE CLASSIFIED INFORMATION

Except as provided in paragraph 13 above, classified information no longer meeting Agency classification requirements (paragraph 5 above) may be declassified or downgraded by the Agency official who authorized its original classification, if that official is still serving in the same position or capacity; by the duly appointed successor or successors of such an official; by a supervisory official of such an original classifier or of any successor; or by other Agency officials designated by the Director of Central Intelligence to exercise declassification and downgrading authority.

- a. Officials of the CIA's Classification Review Division, Information Services Staff (CRD/ISS), are designated to exercise declassification and downgrading authority for Agency information, constituting permanently valuable records of the United States Government (paragraph 15 below), that:
- (1) Has remained classified, at any level, for a period of at least twenty years, or thirty years in the case of foreign government information (paragraph 9b above); and
 - (2) Is subject to review of classification under applicable provisions of E.O. 12065 and of paragraph 15 below.
- b. CRD may also declassify or downgrade, upon formal request by a duly authorized Agency official, permanently valuable documents or other items of information which have remained classified for shorter periods of time than those specified in paragraph 14a above.

INFORMATION AND RECORDS MANAGEMENT



STA

15

- c. Other CIA officials who declassify or downgrade information shall promptly notify the CRG, using computer input Form 4023A, of each declassification or downgrading action taken in regard to information constituting permanently valuable records (paragraphs 14b and 15).
- d. The Agency Security Classification Officer, ISAS/DDA, shall maintain a current listing of CIA positions and officials designated to exercise declassification or downgrading authority.

15. SYSTEMATIC REVIEW FOR DECLASSIFICATION

Classified information constituting permanently valuable records of the United States Government, as defined by 44 U.S.C. 2103, shall be systematically reviewed for declassification by the Classification Review Group (CRG/ISAS/DDA).

- a. Such classified information shall be so reviewed as it becomes twenty years old if it:
 - (1) Was originated or classified by the Agency or by a predecessor organization, the responsibilities of which are now held by the Agency; or
 - (2) Is of non-Agency origin but substantively refers to Agency affairs, personnel, or activities or to those of such predecessor organizations; and
 - (3) Is in the possession and control of the Agency or other agencies of the United States Government including the Administrator of General Services (pursuant to 44 U.S.C. 2107 or 2107 note); but
 - (4) Is not categorized under paragraph 9b above as foreign government information, which shall be systematically reviewed for declassification by the CRG as it becomes thirty years old and as further provided hereunder.
- b. E.O. 12065 provides that the Director of Central Intelligence is authorized to extend classification beyond twenty years, or thirty years in the case of foreign government information. This authority may not be delegated and may be exercised only in accordance with paragraph 13 above and 15i and j below. All extensions of classification beyond twenty years, or thirty years for foreign government information, must be directed personally and in writing by the DCI. Information for which any Agency component requests such extension of classification shall be listed on a Standard Form 325, which shall be forwarded to the CRG, with copies of all pertinent documents attached, for submission to the DCI and his certification that continued classification is required.
- c. When extension of classification is authorized by the DCI for any document or other information following systematic review at twenty or thirty years, a date no more than ten years from such initial review shall be set for the next review thereof.
- d. Waivers of the above ten-year requirement for further review may be requested from the Director of the Information Security Oversight Office. Such requests shall:
 - (1) Be prepared by Deputy Directors and Heads of Independent Offices and forwarded to the AI/DDA for coordination and submission to the ISOO;
 - (2) Include, when submitted to the ISOO, the personal certification of the DCI that the classified information that is the subject of the request has been systematically reviewed and that a definite date for declassification could not be established through such review; and
 - (3) Specify a recommended date for declassification or for subsequent further review.
- e. In no case shall such a waiver be requested until the information has been reviewed for declassification at least once, and an identifiable need to retain classification for a period in excess of twenty years from the date of such review has been established. Otherwise, the ten-year review requirement specified in paragraph 15c above may not be waived.

28 November 1978

25

STAT

INFORMATION AND RECORDS MANAGEMENT

15f

- f. **Reserved.** (Note: E.O. 12065, section 3-403, provides that the DCI "may establish special procedures for systematic review and declassification of classified information concerning the identities of clandestine human agents." These must be approved by the Director, ISOO.)
- g. **Reserved.** (Note: E.O. 12065, section 3-403, provides that the Secretary of Defense "may establish special procedures for systematic review and declassification of classified cryptologic information"; these procedures would be binding on the Agency and other agencies, just as the procedures on agents provided for in paragraph 15f above would be binding on all other agencies.)
- h. Coordination within the Agency and liaison with the ISOO concerning such special procedures are the responsibility of the AI/DDA.
- i. Following appropriate consultation with the Archivist of the United States and review by the ISOO, the Classification Review Group under the direction of the AI/DDA shall, on or prior to 31 May 1979, issue and maintain guidelines for systematic review covering classified information under the Agency's jurisdiction. Such guidelines shall specify limited categories of information covered under Agency classification criteria (paragraph 9 above) that cannot, because of its national security sensitivity, be declassified automatically but requires item-by-item review to determine whether continued protection is needed. The guidelines shall:
- (1) Be authorized for use by the Archivist of the United States and may, upon approval by the DCI, be used by any agency having custody of such information.
 - (2) Cover foreign government information thirty years old or older and other classified information twenty years old or older.
- j. All information not identified in such guidelines as requiring review and for which no prior automatic declassification date has been established shall be declassified automatically at the end of twenty years from the date of initial classification, except that foreign government information shall not be declassified automatically unless such declassification is specified or agreed to by the foreign government or international organization of governments concerned. Foreign government information shall be declassified only in accordance with paragraph 13 above, the aforementioned applicable guidelines, and any appropriate consultation with such foreign government or organization of governments.
- k. Agency guidelines established pursuant to paragraph 15i above shall be kept current and revised as necessary by CRG through periodic reviews at appropriate intervals:
- (1) Every two years for guidelines covering information subject to review for declassification in twenty years; and
 - (2) Every five years for those guidelines covering foreign government information subject to review for declassification in thirty years.
- l. Not Used.
- m. The Agency shall comply with any requests from the Archivist of the United States for earlier reviews for revision of such guidelines. Copies of these guidelines and of any such revisions thereto shall be furnished to the Information Security Oversight Office by CRG through the AI/DDA.
- n. The Agency shall initiate transition to twenty-year review of classification on 1 December 1978 and shall complete this transition on or before 30 November 1988. Classified nonpermanent records scheduled to be retained for more than twenty years need not be systematically reviewed but shall be reviewed for declassification upon request. All classified Agency records twenty years old or older, wherever located, shall be surveyed to identify those that require scheduling for future disposition. Such scheduling shall be completed on or prior to 30 November 1980.

INFORMATION AND RECORDS MANAGEMENT

16

- o. The CRG shall provide assistance to the Archivist of the United States in the systematic review of thirty-year-old foreign government information and other classified information twenty years old or older. Appropriate CRG personnel shall:
 - (1) 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
 - (2) Submit to the DCI, through the AI/DDA, recommendations for continued classification of documents and categories of information so identified and separated.
- p. Following receipt of such recommendations, the personal, written determinations required under E.O. 12065 shall be made, at the discretion of the DCI, as to which documents and categories of information require continued protection.

16. MANDATORY REVIEW FOR DECLASSIFICATION

Information classified under E.O. 12065, previous Executive orders, or applicable United States Government regulations is subject to mandatory review for declassification and release upon request by any other Government agency, employee of the Government, or individual member of the public provided that each such request reasonably describes or identifies the information being sought. Requests for declassification under this provision shall be acted upon within 60 days.

- a. After review, the information requested or any reasonably segregable portion thereof that is determined no longer to require protection for reasons of national security, as specified under E.O. 12065 and paragraph 13 above, shall be declassified and released unless withholding is otherwise warranted under applicable law. The above notwithstanding:
 - (1) Requests submitted under the provisions of the Freedom of Information Act (5 U.S.C. 552) shall be processed as provided in
 - (2) Classified information covered by paragraphs 16e and f below is exempt from mandatory review for declassification; and
 - (3) Foreign government information (paragraph 9b above) contained in any classified document that is the subject of a mandatory review request shall be declassified only in accordance with paragraphs 15i and j above.
- b. The CIA component of record for all requests submitted to the Agency for mandatory review, declassification, and release of information pursuant to E.O. 12065, the Freedom of Information Act as amended (5 U.S.C. 552), and the Privacy Act of 1974 (5 U.S.C. 552a) is the Information and Privacy Staff (IPS) which is responsible for the administration of the Agency system for receipt, acknowledgement, and processing of such requests. The functions of the IPS include:
 - (1) Maintenance of the Agency records system which contains all official correspondence and other records pertinent to mandatory review requests.
 - (2) Initial determination as to whether each such request provides sufficient data to permit a records search for the information requested.
 - (3) Assignment of record-search requirements to other appropriate Agency components that may be able to locate requested information, and guidance to such components as to the correct interpretation of requesters' queries.
 - (4) Acknowledgement of each request and the preparation of appropriate responses to requesters within prescribed time limits with the assistance of the Agency components that hold or are otherwise responsible for the requested information, and in coordination with the Office of General Counsel.

STAT

[Redacted Box]
16c

INFORMATION AND RECORDS MANAGEMENT

- (5) Correspondence with and referral to any other Government agency or agencies responsible for, or having a direct interest in, classified information that is the subject of a mandatory review request directed to the CIA and that is in the custody of CIA although originated or classified by, or of concern to, such other agency or agencies.
- (6) Processing requests for amendment of Agency records concerning individuals and appeals against CIA decisions on these and other mandatory review requests.
- (7) Establishment of fair and equitable fees chargeable for services rendered, as provided under Title 5 of the Independent Offices Appropriation Act (65 Stat. 290, 31 U.S.C. 483a, 1976), in connection with requests for mandatory review for declassification. Schedules of Agency fees for such services shall be published in the Federal Register by specific provision of E.O. 12065.
- c. Requests originating outside the Agency for mandatory review of information within the jurisdiction of the CIA under the provisions of E.O. 12065, the Freedom of Information Act, or the Privacy Act should be addressed to the Chief, IPS as follows:
 - Information and Privacy Coordinator
Central Intelligence Agency
Washington, D.C. 20505
- d. Requests otherwise addressed to the Agency (e.g., to the Director of Central Intelligence, the Deputy Director, the CIA Office of Personnel, etc.) shall be promptly referred to IPS by any Agency component that receives a request considered to fall under the provisions of either act or of the Order or which is otherwise deemed to constitute a mandatory review request that should be processed in accordance therewith. Upon receipt of such a referral, IPS shall process it as provided herein and as further specified under the detailed procedures established by IPS pursuant to the Order (see paragraph 16i below).
- e. The provisions of paragraph 16a above shall not apply to classified information in the custody of, or of interest to, the Agency and that:
 - (1) Is less than ten years old; and
 - (2) Was originated by the President of the United States, the White House Staff, committees or commissions appointed by the President, or by others acting on behalf of the President.
- f. Such information is exempt from mandatory review for declassification, but classified information meeting the criteria cited in paragraph 16e(2) above and is more than ten years old shall be subject to such review in accordance with procedures developed by the Archivist of the United States. These procedures shall provide for consultation with the Agency in the case of mandatory review requests for information of primary interest to CIA.
- g. Requests under the Freedom of Information or Privacy Act for declassification of classified documents of interest to or originated by CIA or a predecessor agency but in the possession or control of the Administrator of General Services pursuant to 44 U.S.C. 2107 or 2107 note (see paragraph 15a(3) above) shall be referred to the Agency by the Archivist of the United States and shall be processed by IPS in accordance with this handbook (paragraphs 15b and c above). Following referral of any such request by the Archivist, unless instructed to do otherwise, the Agency shall respond directly to each requester as provided herein and under established IPS procedures (see paragraph 16i below).
- h. No CIA component, official, or employee shall, in response to any request for a document or other item of information under the Freedom of Information Act or the mandatory review provisions of E.O. 12065, refuse to confirm the existence or nonexistence of that document or item unless the fact of its existence or nonexistence would itself be classifiable (paragraphs 2, 5, and 9 above).
- i. Other Agency provisions concerning mandatory review for declassification are contained in

STAT

[Redacted Box]