

# CONFIDENTIAL

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

MEMORANDUM FOR: Acting Director of Security

25X1A FROM:

[REDACTED]  
Deputy Director of Security (PTOS)

SUBJECT: Portion Marking of Classified Information  
by CIA Contractors (Request for Change) (U)

1. Action Requested: It is requested that the proposed recommendations be approved. (U)

2. Background: During the Industrial Security Conference in September 1979, a security officer from a large industrial contractor asked the DCI why the Agency required portion marking at the end of a paragraph instead of at the beginning, as other government agencies do. The DCI advised that he would have the Director of Security look into the matter and advise. (C)

Section I-504 of Executive Order 12065 states "...each classified document shall, by marking or other means, indicate clearly which portions are classified, with the applicable classification and which portions are not classified." (U)

Paragraph I.G.9. of Directive I issued by the Information Security Oversight Office of the InterAgency Classification Review Committee states "...portion marking shall be accomplished by placing a parenthetical designator immediately preceding or following (emphasis added) the text it governs." (U)

The [REDACTED] chose to portion mark at the beginning of each paragraph and provided instructions to industry to follow suit. (U)

25X1C

DERIVATIVE CL BY 017511  
 DECL  REVW ON 24 Oct 99  
DERIVED FROM A9c6.1

WARNING NOTICE  
INTELLIGENCE SOURCES  
AND METHODS INVOLVED

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6 OS 9 2563

# CONFIDENTIAL

CONFIDENTIAL

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

Agency policymakers opted to portion mark at the end of the paragraph. Chapter 12 [REDACTED] indicates that "All national security information classified by the Agency shall be identified and marked as prescribed below...." (C)

25X1A

Paragraph 12.d. states that "Each classified document shall indicate which paragraphs or other portions...are classified and which are unclassified." It also states that the proper symbol "will be placed immediately following (emphasis added) the portion of text to which it applies." (C)

The above instruction was inserted into the new industrial security manual, Standard Security Procedures for Contractors, that was released to over [REDACTED] Agency contractors in July 1979. Additionally COMIREX released a document, D-2.9/3, in December 1978 entitled Guidelines to Implementation of Executive Order 12065. This was released to TK contractors and provided an example of portion marking with the classification following the paragraph. The Office of Development and Engineering provided similar instructions to their contractors in a book message cable on 13 December 1978. (C)

25X1A

There is a twofold problem involved; one involves cover and the other involves a major inconvenience for the contractor. Because the CIA is the only government agency in the Intelligence Community which portion marks following the text, it clearly labels all classified documents thus marked as CIA. The same is true of documents going to the contractor from the CIA. This also puts a burden on the contractor's clerical staff who has to remember to mark the CIA's documents differently from the other government agencies, the latter of which usually makes up the bulk of their contractors. (C)

25X1A

[REDACTED] the CIA Classification Officer, opined that it may be necessary to amend Agency regulations before any direction to contractors can be made. However, as the over-riding governmental guidelines prepared by the Information Security Oversight Office allow portion marking either preceding or following the text it governs, it is believed that the Director of Security can change his instructions to the contractors without formal amendment to Agency regulations. (C)

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

CONFIDENTIAL

**CONFIDENTIAL**

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

A change in current procedures would certainly involve considerable time and effort, because it would entail communication to all CIA contractors, as well as a change in the manual. However, in view of the cover problem the current policy presents, I believe we should attempt to amend our portion marking policy as it pertains to contractors. (U)

3. Recommendations: It is recommended that the Security Staff of the Office of Logistics be advised to amend line 5 of paragraph 4.(3)(a) of Standard Security Procedures for Contractors to read as follows: "The symbol '(TS)' for TOP SECRET, '(S)' for SECRET, '(C)' for CONFIDENTIAL, and '(U)' for UNCLASSIFIED may be placed immediately preceding or following the portion of the text to which it applies." It is further recommended that the Security Staff of the Office of Development and Engineering advise their contractors by cable that portion marking may be accomplished at either the beginning or end of the text to which it applies. (U)



25X1A

APPROVED: \_\_\_\_\_  
Acting Director of Security

DISAPPROVED: \_\_\_\_\_  
Acting Director of Security

DATE: \_\_\_\_\_

- Distribution:
- Original - Return to DD/PTOS
  - 1 - AD/Security
  - 1 - DD/PTOS
  - 1 - C/SS/OD&E
  - 1 - C/SS/OL
  - 1 - OS Registry
  - ① - C/PhySD Chrono
  - 1 - ISB Subject
  - 1 - ISB Chrono

25X1A OS:PTOS:PhySD: [redacted] or (16 Oct 79)  
Retyped: C/PhySD [redacted] Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

TATINTL

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

**Next 1 Page(s) In Document Exempt**

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

MONDAY, JULY 3, 1978

PART IV



---

# THE PRESIDENT

## NATIONAL SECURITY INFORMATION

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

# presidential documents

[3195-01]

## Title 3—The President

Executive Order 12065

June 28, 1978

### National Security Information

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

#### TABLE OF CONTENTS

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

## SECTION 1. ORIGINAL CLASSIFICATION.

1-1. *Classification Designation.*

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

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

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

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

1-2. *Classification Authority.*

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

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

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

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

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

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6  
 The President and Chief Executive Officer, Export-Import Bank of the United States  
 Corporation

1-204. *Limitations on Delegation of Classification Authority.*

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

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

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

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

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

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

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

1-3. *Classification Requirements.*

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

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

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

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



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

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

#### 1-4. *Duration of Classification.*

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

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

#### 1-5. *Identification and Markings.*

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

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

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

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

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

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

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

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

**1-6. Prohibitions.**

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

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

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

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

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

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

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

**SECTION 2. DERIVATIVE CLASSIFICATION.**

**2-1. Use of Derivative Classification.**

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

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

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

**2-2. Classification Guides.**

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

## THE PRESIDENT

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

2-3. *New Material.*

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

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

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

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

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

## SECTION 3. DECLASSIFICATION AND DOWNGRADING.

3-1. *Declassification Authority.*

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

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

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

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

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

3-2. *Transferred Information.*

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

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

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

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

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

### 3-3. *Declassification Policy.*

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

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

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

### 3-4. *Systematic Review for Declassification.*

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

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

## THE PRESIDENT

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

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

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

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

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

*3-5. Mandatory Review for Declassification.*

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

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

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

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

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

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

3-6. *Downgrading.*

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

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

SECTION 4. SAFEGUARDING.

4-1. *General Restrictions on Access.*

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

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

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

4-104. Classified information no longer needed in current working files or for reference or record purposes shall be processed for appropriate disposition in accordance with the provisions of Chapters 21 and 33 of Title 44 of the United States Code, which governs disposition of Federal records.

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

4-2. *Special Access Programs.*

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

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

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

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

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

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

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

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

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

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

(a) are engaged in historical research projects, or

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

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

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

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

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

#### 4-4. *Reproduction Controls.*

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

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

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

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

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

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

#### SECTION 5. IMPLEMENTATION AND REVIEW.

##### 5-1. Oversight.

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

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

##### 5-2. Information Security Oversight Office.

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

5-202. The Director shall:

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

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

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

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

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

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

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

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



5-3. *Interagency Information Security Committee.*

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

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

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

5-4. *General Responsibilities.*

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

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

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

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

(a) designate a senior agency official to conduct an active oversight program to ensure effective implementation of this Order;

(b) designate a senior agency official to chair an agency committee with authority to act on all suggestions and complaints with respect to the agency's administration of the information security program;

(c) establish a process to decide appeals from denials of declassification requests submitted pursuant to Section 3-5;

(d) establish a program to familiarize agency and other personnel who have access to classified information with the provisions of this Order and implementing directives. This program shall impress upon agency personnel their responsibility to exercise vigilance in complying with this Order. The program shall encourage agency personnel to challenge, through Mandatory Review and other appropriate procedures, those classification decisions they believe to be improper;

(e) promulgate guidelines for systematic review in accordance with Section 3-402;

(f) establish procedures to prevent unnecessary access to classified information, including procedures which require that a demonstrable need for access to classified information is established before initiating administrative clearance procedures, and which ensures that the number of people granted access to classified information is reduced to and maintained at the minimum number that is consistent with operational requirements and needs; and

(g) ensure that practices for safeguarding information are systematically reviewed and that those which are duplicative or unnecessary are eliminated.

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

5-5. *Administrative Sanctions.*

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

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

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

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

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

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

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

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

SECTION 6. GENERAL PROVISIONS.

6-1. *Definitions.*

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

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

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

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

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

6-2. *General.*

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

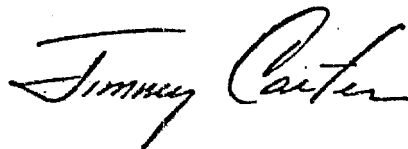
6-202. The Attorney General, upon request by the head of an agency, his duly designated representative, or the Director of the Information Security Oversight Office, shall personally or through authorized representatives of the Department of Justice render an interpretation of this Order with respect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

THE PRESIDENT

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

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

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



THE WHITE HOUSE,  
June 28, 1978.

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

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

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

[3195-01]

Order of June 28, 1978

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

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

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

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

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

This Order shall be published in the FEDERAL REGISTER.



THE WHITE HOUSE,  
June 28, 1978.

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

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

PART V

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6



INTERAGENCY  
CLASSIFICATION  
REVIEW  
COMMITTEE

■

INFORMATION  
SECURITY  
OVERSIGHT  
OFFICE

National Security  
Information

FBI/DOJ

## RULES AND REGULATIONS

[6820-27]

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

## Title 32—National Defense

## CHAPTER XX—INTERAGENCY CLASSIFICATION REVIEW COMMITTEE

(Directive No. 1)

## INFORMATION SECURITY OVERSIGHT OFFICE

## National Security Information

AGENCY: Interagency Classification Review Committee (ICRC).

ACTION: Implementing directive.

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

EFFECTIVE DATE: December 1, 1978.

FOR FURTHER INFORMATION CONTACT:

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

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

## TABLE OF CONTENTS

## Section I. Original Classification

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

## Section II. Derivative Classification

- A Definition.
- B Responsibility.

C Markings Derivatively Classified Documents.

D Classification Guides.

## Section III. Declassification and Downgrading

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

## Section IV. Safeguarding

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

## Section V. Implementation and Review: Challenges to Classification

## Section VI. General Provisions

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

## I. ORIGINAL CLASSIFICATION

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

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

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

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

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

<sup>1</sup> Parenthetical references are to related sections of Executive Order 12065.

shall not create any presumption as to whether the information meets the damage tests (1-302 and 1-303).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. *Dissemination and reproduction notice.* For classified information that the originator has determined, pursuant to section 1-508 of the order, should be subject to special dissemination or reproduction limitations, or both, a statement placing the user on notice of the restrictions shall be included in the text of the document or on its cover sheet; e.g., "Reproduction requires approval of originator," or "Further dissemination only as directed by (Insert appropriate office or official)" (1-506).

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

## II. DERIVATIVE CLASSIFICATION

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

B. *Responsibility.* Derivative application of classification markings is a responsibility of those who incorporate, paraphrase, restate, or generate in new form information that is already classified, and of those who apply markings in accordance with instructions from an authorized classifier or in accordance with an authorized classification guide. Persons who apply derivative classification markings should take care to determine whether their paraphrasing, restating, or summarizing of classified information has removed the basis for classification. Where checks with originators or other appropriate inquiries show that

no classification or a lower classification than originally assigned is appropriate, the derivative document shall be issued as unclassified or shall be marked appropriately (2-101 and 2-102).

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

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

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

3. Dates or events for declassification or review shall be carried forward from the source material or classification guide and shown on a "declassify on" or "review for declassification on" line. If the classification is derived from more than one source, the latest date for declassification or review applicable to the various source materials shall be applied to the new information (2-102(c));

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

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

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

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

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

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

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

those reasons need be recorded only on or with the record copy of the guide (2-201); and

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

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

### III. DECLASSIFICATION AND DOWNGRADING

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

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

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

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

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

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

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

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

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

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

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

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

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



tion 3-401 of Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6 documents or categories of information require continued protection. The agency shall inform the Archivist of the United States of this determination (3-4).

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

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

D. *Procedures for mandatory declassification review.*

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

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

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

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

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

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

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

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

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

#### IV. SAFEGUARDING

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

B. *General restrictions on access.*

1. *Determination of need-to-know.* Classified information shall be made available to a person only when the possessor of the classified information establishes in each instance, except as provided in section 4-3 of the order, that access is essential to the accomplishment of official Government duties or contractual obligations (4-101).

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

C. *Access by historical researchers and former Presidential appointees.* Agencies shall obtain: (1) Written agreements from requestors to safeguard the information to which they are given access as permitted by the order and this directive; and (2) written consent to the agency's review of their notes and manuscripts for the purpose of determining that no classified information is contained therein. A determination of trustworthiness is a precondition to a requestor's access. If the access requested by historical researchers and former Presidential appointees requires the rendering of services for which fair and equitable fees may be charged pursuant to title 5 of the Independent Offices Appropriations Act, 65 Stat. 290, 31 U.S.C. 483a (1976), the requestor shall be so notified and the fees may be imposed (4-3).

D. *Dissemination.* Except as otherwise provided by section 102 of the National Security Act of 1947, 61 Stat. 495, 50 U.S.C. 403 (1976 and Supp. V 1975), classified information originating in one agency may not be disseminated outside any other agency to

## RULES AND REGULATIONS

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

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

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

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

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

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

**2. Secret and confidential.** Secret and confidential information shall be stored in a manner and under the conditions prescribed for top secret information, or in a container or vault that meets the standards for secret or confidential, established pursuant to the provisions of subsections 3 or 4 below (4-103).

**3. Standards for security equipment.** The General Services Administration shall, in coordination with agencies originating classified information, establish and publish uniform standards, specifications, and supply schedules for containers, vaults, alarm systems, and associated security devices suitable for the storage and protection of all categories of classified information. Any agency may establish more stringent standards for its own use. When-

ever new security equipment is procured, it shall be in conformance with the standards and specifications referred to above and shall, to the maximum extent practicable, be of the type designated on the Federal Supply Schedule, General Services Administration (4-103).

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

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

**5. Combinations.—a. Equipment in service.** Combinations to dial-type locks shall be changed only by persons having appropriate security clearance, and shall be changed whenever such equipment is placed in use, whenever a person knowing the combination no longer requires access to the combination, whenever a combination has been subjected to possible compromise, whenever the equipment is taken out of service, and at least once every year. Knowledge of combinations protecting classified information shall be limited to the minimum number of persons necessary for operating purposes. Records of combinations shall be classified no lower than the highest level of classified information to be stored in the security equipment concerned (4-103).

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

**6. Keys.** Heads of agencies shall establish administrative procedures for the control and accountability of keys and locks whenever key-operated, high-security padlocks are utilized. The level of protection provided such keys shall be equivalent to that afford-

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

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

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

**G. Transmittal.—1. Preparation and receipting.** Classified information shall be enclosed in opaque inner and outer covers before transmitting. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee. The outer cover shall be sealed and addressed with no identification of the classification of its contents. A receipt shall be attached to or enclosed in the inner cover, except that confidential information shall require a receipt only if the sender deems it necessary. The receipt shall identify the sender, addressee, and the document, but shall contain no classified information. It shall be immediately signed by the recipient and returned to the sender. Any of these wrapping and receipting requirements may be waived by agency heads under conditions that will provide adequate protection and prevent access by unauthorized persons (4-103).

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

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

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

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

ation, by the U.S. Postal Service, registered mail, or by protective services provided by U.S. air or surface commercial carriers under such conditions as may be prescribed by the head of the agency concerned (4-103).

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

c. *Other areas.* Secret information may be transmitted from, to, or within areas other than those specified in subsections a or b above by one of the means established for top secret information, or by U.S. registered mail through Army, Navy, or Air Force Postal Service facilities provided that the information does not at any time pass out of U.S. citizen control and does not pass through a foreign postal system. Transmittal outside such areas may also be accomplished under escort of appropriately cleared personnel aboard U.S. Government and U.S. Government contract vehicles or aircraft, ships of the United States Navy, civil service manned U.S. Naval ships, and ships of U.S. Registry. Operators of vehicles, captains or masters of vessels, and pilots of aircraft who are U.S. citizens and who are appropriately cleared may be designated as escorts (4-103).

4. *Transmittal of confidential information.* Confidential information shall be transmitted within and between the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories or possessions by one of the means established for higher classifications, or by U.S. Postal Service certified, first class, or express mail service when prescribed by an agency head. Outside these areas, confidential information shall be transmitted only as is authorized for higher classifications (4-103).

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

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

V. IMPLEMENTATION AND REVIEW

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

VI. GENERAL PROVISIONS

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

B. *Posted notice.* If prompt remark-

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

C. *Downgrading, declassification, and upgrading markings.* Whenever a change is made in the original classification or in the dates of downgrading or declassification of any classified information, it shall be promptly and conspicuously marked to indicate the change, the authority for the action, the date of the action, and the identity of the person taking the action. Earlier classification markings shall be cancelled when practicable (4-102).

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

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

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

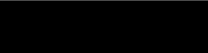
OCTOBER 2, 1978.

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

TATINTL

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

 Paragraph 12d(1), line 6:

After the word "applies" insert the following sentence:

"Industrial contractors involved in Agency-related contractual activities may place the appropriate symbol immediately preceding the portion of text to which it applies."

STATINTL

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

**Next 2 Page(s) In Document Exempt**

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

SECRET

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

*C/ISB*

**DIRECTORATE OF ADMINISTRATION  
CLASSIFICATION GUIDE**

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

SECRET

Copy No.  
**453**

E2 IMPDET  
CL BY: 001777

**SECRET**

27 November 1978

Directorate of Administration Classification Guide

Foreword

1. This Directorate of Administration Classification Guide (DACG) is designed and approved effective 1 December 1978 in accordance with the requirements of E.O. 12065. It sets forth the categories of information to be considered for classification, and provides guidance for determining the proper levels of classification (i.e., Confidential, Secret, or Top Secret). For each classifiable subcategory of information, it also sets forth a classification duration limit and a justification for extending classification beyond six years to a maximum of 20 years, or to 30 years in the case of foreign government information. The Guide is to be used in conjunction with [REDACTED] Section 12 of the Handbook provides guidance on marking each document at time of classification.

25X1A

2. The Guide is essentially a series of predetermined original classification decisions by a Top Secret classifier for information requiring extension of classification beyond six years, and provides the authority for derivative classification. It is to be used by:

a. personnel with original classification authority below the Top Secret level;

b. personnel, as may be designated by their Office Heads, who do not have original classification authority but who can act as classifiers by citing the applicable portion(s) of the Guide as the basis for their classification actions;

c. personnel with original Top Secret classification authority who elect to use the Guide in lieu of citing paragraph 3d [REDACTED]

25X1A

Personnel using the Guide are "derivative classifiers".

i

**SECRET**

Unclassified When Detached  
From Attachment



**SECRET**

3. The DACG is based on the seven general categories of information meriting classification consideration, as specified by E.O. 12065. These seven categories, subdivided into broader subcategories, constitute the Agency classification criteria (unclassified) set forth in Section 9a-9g [REDACTED]. The DACG includes these criteria and breaks them down into specific subcategories applicable to the Directorate of Administration and also applicable to NFAC, the DO, DS&T, and Independent Offices for classification of administrative information or material. The letter "A" has been assigned to the Directorate of Administration to identify the DACG and must preface each citation of the Guide. Consider, for example, the citation A 9a(1) (1.1):

"A" indicates that the citation is from the DACG;

"9" is the Section [REDACTED] containing E.O. 12065 and Agency classification criteria;

"a" is the first of seven E.O. 12065 criteria or categories of information subject to classification;

(1) is the first Agency criterion under "a" and represents a more specific breakdown of information;

(1.1) is the first classifiable DA subcategory under a(1).

When the Guide is cited in derivative classification, the above citation is to be simplified to A 9a 1.1 plus required markings. Note that in some instances no specific breakdown is made under the broad categories of Agency criteria. In these cases, the term "Reserved" is used to indicate the possibility of future subcategorization. Also note that with the exception of categories 9a, b, g, Annex A, and Annex B, which are applicable to the Directorate generally, the specific subcategories listed under 9c-9f are listed by Office of functional interest in alphabetical order for ease of reference.

**SECRET**

25X1A

25X1A

**SECRET**

4. A single level of classification has been established for each subcategory although a range of classification is possible depending upon the sensitivity of the information. A derivative classifier should compare the information or material he believes to require classification with the information and classification level established in the DACG. If the DACG does not apply, a derivative classifier should consult an officer with original classifying authority at Top Secret level who will determine level of classification and, if warranted, classify the information, assign a duration of classification, and provide justification for extension of classification beyond six years.

5. The justifications used in the Guide are also to be used by original Top Secret classifiers in justifying extension of classification beyond six years, as set forth in paragraph 3d [redacted] and attached as Annex B to this Guide. Personnel with original classification authority are thus provided the option of justifying a classification duration extending beyond six years by citing the applicable portion of the Guide, or by citing the Handbook as noted above. This option provides flexibility considering that predetermined classification decisions set forth in the Guide may not always be applicable.

6. As noted above, in the event an item of information is not covered in the DACG, a classification determination must be made by an officer to whom original classification authority has been delegated at the Top Secret level. If such cases occur, the Agency Security Classification Officer, ISAS/DDA, should be advised in writing so that any omission from the DACG can be included in future updates thereof. The DACG should be viewed as an aid to classification, susceptible both to expansion and to improvement.

[redacted]  
John F. Blake  
Deputy Director  
for  
Administration

25X1A

25X1A

**SECRET**

INDEX

**SECRET**

DIRECTORATE OF ADMINISTRATION

CLASSIFICATION GUIDE (DACG)

Index to Principal Criteria

	<u>TAB</u>
SECTION 9 -	
a. Military plans, weapons, or operations	A
b. Foreign government information	B
c. Intelligence activities, sources or methods	C
d. Foreign relations or foreign activities of the United States	D
e. Scientific, technological, or economic matters relating to the national security	E
f. United States Government programs for safeguarding nuclear materials or facilities	F
g. Other categories of information related to national security and determined by the Director of Central Intelligence to require protection against unauthorized disclosure	G
ANNEX A (Cover Classification Guide)	H
ANNEX B (Justifications for Extension of Classification Beyond Six Years)	I

**SECRET**

E2 IMPDET  
CL BY: 001777

A

**SECRET**  
 DIRECTORATE OF ADMINISTRATION  
 CLASSIFICATION GUIDE (DACG)

25X1A

Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
<p>Information shall not be considered for classification unless it concerns one of the categories set forth below and shall not be classified unless its unauthorized disclosure could cause exceptionally grave, serious, or identifiable damage to the national security.(U)</p>			
<p>9a. <u>Military plans, weapons or operations</u></p>			
<p>(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.(U)</p>			
(1.1)	RESERVED		
<p>(2) Information which 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.(U)</p>			
(2.1)	SECRET	20 years (review)	Continued protection of the information at the "Secret" level is required because disclosure could result in action to negate U.S. intelligence collection efforts.
<p>(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 counter-measures to such plans or posture.(U)</p>			
(3.1)	RESERVED		
<p>(4) information that could reveal the capabilities, vulnerabilities or deployment of United States weapons or weapons systems.(U)</p>			
(4.1)	RESERVED		

B

25X1A

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

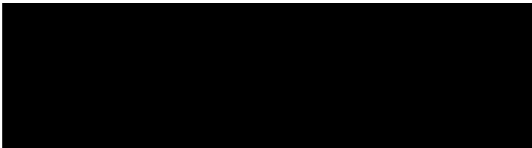
**Next 1 Page(s) In Document Exempt**

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6



C

25X1A

Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
9c. <u>Intelligence activities, sources, or methods</u>  (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.(U)  <u>OFFICE OF FINANCE</u>  (1.1) Information dealing with budget, expenditures, funding or other fiscal aspects which reveals, or if joined with other information, could reveal or identify an intelligence source.(U)	SECRET	20 years (review)	Extended classification at the "SECRET" level is required to protect sensitive technical and human clandestine sources of intelligence which could remain vulnerable to counteraction for a period of at least 20 years. Nullification or reduction in effectiveness of these sources could result in a loss of informational advantage to the United States, causing serious damage to the national security.
	SECRET	20 years (review)	" "

25X1A

25X1A

Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
<u>OFFICE OF TRAINING</u>  (1.3) Information used in regular or special training programs, briefings, consultative activities, or lectures which could reveal or identify an intelligence source, including information contained in historical documents, background materials, analytical studies, reviews, lecture notes, course outlines, student handouts, lesson plans, student reading materials, tests, ADP input and output forms, and audio-visual aids.(U)	SECRET	20 years (review)	Extended classification is required to protect human and technical clandestine sources of intelligence which could remain vulnerable to counteraction for a period of at least 20 years. Nullification or reduction in effectiveness of these sources could result in a loss of informational advantage to the United States causing identifiable damage to the national security.

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6  
 DIRECTORATE OF ADMINISTRATION  
 CLASSIFICATION GUIDE (DACG)

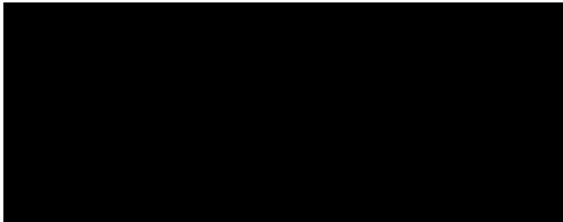
~~SECRET~~

25X1A

Classification Guide Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
(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.(U)			
<u>OFFICE OF COMMUNICATIONS</u>			
(2.1) Information pertaining to CIA's worldwide electronic communications network for transmitting intelligence and related management and administrative information, including training, equipment, circuitry, communications services provided to or obtained from other United States Government components, use of the RF spectrum, capabilities, systems and procedures.(U)	SECRET	20 years (review)	Extended classification at the "SECRET" level is required to protect sensitive cryptologic, technical, and clandestine methods of transmitting intelligence which would remain vulnerable to counteraction for a period of at least 20 years. Compromise of such equipment, procedures, and systems would result in loss of vital information causing serious damage to national security.
(2.2) Information concerning the existence, plans, covert capability, techniques, procedures, equipment systems and subsystems used by CIA in support of clandestine operations.(U)	SECRET	20 years (review)	" "

-7-  
 SECRET

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6  
~~SECRET~~  
 DIRECTORATE OF ADMINISTRATION  
 CLASSIFICATION GUIDE (DACG)

25X1A	Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
	<u>OFFICE OF FINANCE</u>			
	(2.3) Information dealing with budget, expenditures, funding, or other fiscal aspects which reveals or, if joined with other information, could reveal or identify intelligence methods. (U)	SECRET	20 years (review)	Extended classification at the "SECRET" level is required to protect sensitive intelligence or counterintelligence methods which could remain vulnerable to counteraction for a period of at least 20 years. Nullification or reduction in effectiveness could result in a loss of informational advantage to the United States causing serious damage to national security.
25X1C		SECRET	20 years (review)	Extended classification of the information at the "SECRET" level is required because it deals with intelligence funding techniques of current and continuing applicability which, if compromised, could jeopardize personnel and mechanisms involved in on-going operations and adversely impact on foreign relations with resultant serious damage to national security.

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6  
 DIRECTORATE OF ADMINISTRATION  
 CLASSIFICATION GUIDE (DACC)

25X1A	Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
25X1A		SECRET	20 years (review)	Extended classification of the information at the "SECRET" level is required because it deals with intelligence funding techniques which, if disclosed in total, would reveal the Agency's intelligence budget and scope of effort. Such disclosure would cause the hostile powers opposition to intensify their collection efforts against the U.S., as well as undertake defensive action to negate U.S. collection efforts. Such actions could deprive the U.S. of an informational advantage and cause serious damage to national security.
25X1A	<u>OFFICE OF LOGISTICS</u> 	SECRET	6 years (review)	Maintenance of classification for six years and possibly longer is required to protect information concerning logistical support of operations or activities important to national security, the disclosure of which could reasonably be expected to result in negating the support, reducing its effectiveness, or compromising the operation or activity itself, with serious damage to national security.

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6  
 SECRET  
 DIRECTORATE OF ADMINISTRATION  
 CLASSIFICATION GUIDE (DACG)

25X1A	Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
25X1A	[REDACTED]	SECRET	20 years (review)	The information could reveal vulnerability or capability data, the unauthorized disclosure of which could reasonably be expected to result in negating or nullifying the effectiveness of a system, installation or project important to national security and/or place in immediate jeopardy a person important to the national security.
25X1A	[REDACTED]	SECRET	6 years (review)	Protection at SECRET level for six years and possibly longer is required because this information reveals intelligence methods, vulnerability and capability data the unauthorized disclosure of which could result in negating or nullifying effectiveness of a system, installation or project causing serious damage to the national security.
25X1A	[REDACTED]	SECRET	6 years (review)	" "

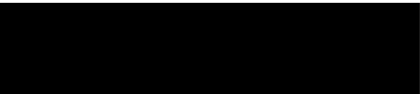

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6  
**SECRET**  
 DIRECTORATE OF ADMINISTRATION  
CLASSIFICATION GUIDE (DACC)

25X1A

Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
(2.10) Information concerning Real Property Acquisition Procedures. (U)	CONFIDENTIAL	6 years (review)	Protection at CONFIDENTIAL level for six years and possibly longer is required because this information reveals intelligence methods, vulnerability and capability data the unauthorized disclosure of which could result in negating or nullifying effectiveness of a system, installation or project causing identifiable damage to the national security.
(2.11) Information concerning quantities of and disposal methods for Agency classified material, classified waste, and excess material. (U)	CONFIDENTIAL	6 years (review)	" "
25X1A [REDACTED]	SECRET	20 years (review)	Extended protection at SECRET level is required because this information reveals intelligence methods, vulnerability and capability data, the unauthorized disclosure of which could result in negating or nullifying effectiveness of a system, installation or project causing serious damage to the national security.



~~SECRET~~  
 Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6  
 DIRECTORATE OF ADMINISTRATION  
CLASSIFICATION GUIDE (DAGG)

25X1A	Classification Guide Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
	(2.13) Information concerning procedures for checking incoming mail. (U)	CONFIDENTIAL	6 years (review)	Protection at CONFIDENTIAL level for six years and possibly longer is required because this information reveals intelligence methods, vulnerability and capability data the unauthorized disclosure of which could result in negating or nullifying effectiveness of a system, installation or project causing identifiable damage to the national security.
25X1A		SECRET	20 years (review)	Extended protection at SECRET level is required because this information reveals intelligence methods, vulnerability and capability data, the unauthorized disclosure of which could result in negating or nullifying effectiveness of a system, installation or project causing serious damage to the national security.
25X1A		SECRET	20 years (review)	" "

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6  
 DIRECTORATE OF ADMINISTRATION  
 CLASSIFICATION GUIDE (DACC)

SECRET

25X1A

Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
--	-------------------------------	----------------------------------	--

OFFICE OF MEDICAL SERVICES

25X1A

[REDACTED]	TOP SECRET	20 years, review, or five years [REDACTED]	Continued protection of the information is essential to national security because it reveals intelligence methods which, if disclosed, could deprive the U.S. of an advantage in methodology and would reveal the target of such methodology. Such disclosure could have an adverse impact on U.S. foreign relations and defense programs with exceptionally grave damage to national security.
------------	------------	--	---

25X1A

25X1A

OFFICE OF PERSONNEL

(2.17) Information concerning employee suggestions to improve, or to propose new methods, procedures, modes, or techniques used or being developed to acquire, transmit, analyze, evaluate or process foreign intelligence or counterintelligence, or to support an intelligence source, operation, or activity.(U)	CONFIDENTIAL	20 years (review)	Continued protection of the information is essential to the national security because it reveals intelligence methods which, if disclosed, could deprive the U.S. of an intelligence advantage with identifiable damage to national security.
---	--------------	----------------------	---

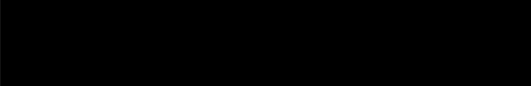
OFFICE OF SECURITY

(2.18) Information concerning the type of equipment and methodology employed in technical surveillance countermeasures.(U)	SECRET	20 years (review)	Extended classification at the SECRET level is required to protect unique intelligence equipment and methods employed in technical surveillance countermeasures which, if compromised, could deprive the Agency of an effective defense against hostile technical surveillance with resultant serious damage to national security.
--	--------	----------------------	--

-13-  
SECRET

~~SECRET~~  
DIRECTORATE OF ADMINISTRATION  
CLASSIFICATION GUIDE (DACG)

25X1A	Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
	(2.19) Information concerning the results of technical surveillance countermeasures inspections.(U)	SECRET	20 years (review)	Extended classification at SECRET level is required because the information concerns operations or activities important to national security and/or could reveal vulnerability or capability data, the unauthorized disclosure of which can reasonably be expected to result in negating or nullifying the effectiveness of a system, operation/ activity, installation or project important to national security and/or impede orderly implementation of plans/operations/activities.
25X1A		SECRET	20 years (review)	Extended classification at the SECRET level is required to protect unique intelligence equipment and methods employed in defense of intelligence installations, which, if disclosed, could result in a vulnerability leading to an informational loss to the U.S. and causing serious damage to national security.

25X1A	Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
25X1A		SECRET	20 years (review)	Extended classification at the SECRET level is required to protect unique intelligence equipment and methods which, if compromised, would result in opposition awareness of CIA capability and the development of countermeasures making clandestine collection of intelligence more difficult. Such negation of CIA capability could deprive the U. S. of an informational advantage with resultant serious damage to national security.
	(2.22) Information pertaining to personnel security information of a counterintelligence nature.(U)	SECRET	20 years (review)	Extended classification at the SECRET level is required to protect sensitive information used in personnel and physical security investigations, which, if compromised, could lead to a penetration and resultant informational loss causing serious damage to national security.

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6  
 SECRET  
 DIRECTORATE OF ADMINISTRATION  
 CLASSIFICATION GUIDE (DACC)

25X1A

Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
(2.23) Information that could reveal, compromise, or jeopardize data processing access procedures and/or controls to computer classified data banks in use, being developed, or proposed for use by CIA.(U)	SECRET	20 years (review)	Extended classification at the SECRET level is required to protect sensitive intelligence methods used to protect classified information in ADP systems. Compromise of such methods could lead to a loss of vital information and serious damage to national security.
(2.24) Information disclosing operational support activities of the Office of Security.(U)	CONFIDENTIAL	20 years (review)	Extended classification is required to protect intelligence methods and techniques of continuing applicability, the unauthorized disclosure of which could result in impeding or negating operations/activities and/or placing in immediate jeopardy a person important to national security.
(2.25) Safe or lock combinations, when coupled with information identifying the lock or the location of the device to which the lock is affixed.(U)	TOP SECRET	Until Combination is changed	Protection of this information is essential because it reveals Agency internal data specifically protected by statute, the unauthorized disclosure of which could result in exceptionally grave damage to national security.
(2.26) Information correlating a staff employee or staff employee equivalent badge and the code number required for valid entry through the Security Access Control System.(U)	CONFIDENTIAL	Until badge or code number is invalidated	Protection of this information is essential because it reveals vulnerability data, the unauthorized disclosure of which would result in identifiable damage to national security.

25X1A

Classification Guide Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
<u>OFFICE OF TRAINING</u>			
(2.27) Information describing covert training techniques and materials used in training which reveal intelligence methods.(U)	CONFIDENTIAL	20 years (review)	Extended classification is required to protect intelligence methods and techniques used in training which have continuing applicability and whose negation could deprive the U.S. of an informational loss with identifiable damage to national security.
(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, <u>security procedures</u> , techniques, and activities including those applicable to the fields of communication 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.(U)			

**SECRET**

25X1A

Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
<u>OFFICE OF FINANCE</u>			
(3.1) The Annual Report of the Central Intelligence Agency and monthly CIA Statement of Financial Condition.(C)	TOP SECRET	20 years (review)	Extended protection of this information at TOP SECRET level is required because it reveals quantitative and qualitative Agency internal data, the nature, objectives, requirements, priorities, scope and thrust of Agency activities, the unauthorized disclosure of which could cause exceptionally grave damage to the national security.
(3.2) Information relating to appropriations to and obligations of CIA, including total amounts, number of employees, details of budgets and expenditures, data on programs and activities, internal distribution or allocation of funds or requisitioning authorities, information on confidential funds received or expended on behalf of other Government agencies.(C)	SECRET	20 years (review)	Extended protection of this information at SECRET level is required because it reveals quantitative and qualitative Agency internal data, including the nature, objectives, requirements, priorities, scope and thrust of Agency activities, the unauthorized disclosure of which could cause serious damage to the national security.
(3.3) Information relating to the Contingency Fund of CIA, the source of the fund, and amount or purpose for which such funds are released.(C)	SECRET	20 years (review)	" "

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6  
SECRET  
DIRECTORATE OF ADMINISTRATION  
CLASSIFICATION GUIDE (DACG)

25X1A


Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
<u>INFORMATION AND PRIVACY STAFF</u>			
(3.4) Names or initials of non-overt DDO components below the Directorate level; names or initials of non-overt NFAC, DDS&T, and DDA components below the Office level. (U)	CONFIDENTIAL	20 years (review)	This information reveals internal Agency data protected by statute, the unauthorized disclosure of which could cause identifiable damage to national security.
<u>OFFICE OF LOGISTICS</u>			
(3.5) Agency Vehicular Assets. Computer printouts and vehicle status card (Form 794) for individual vehicles which include complete description, serial number, motor vehicle number, station name, station location, project name (if any), individual vehicle assigned to (if applicable) Certificate of Origin and vehicle title. (C)	SECRET	6 years (review)	Protection of this information for six years and possibly longer is required because it could reveal vulnerability or capability data, the unauthorized disclosure of which could result in negating or nullifying the effectiveness of a system, installation, or project, or placing in immediate jeopardy a person important to the national security.
(3.6) Information pertaining to construction engineering, and communication and utilities systems at domestic/overseas installations. (C)	CONFIDENTIAL	6 years (review)	Protection of this information for six years and possibly longer is required, because it could reveal sources, methods, vulnerability, and capability data, the unauthorized disclosure of which could result in negating or nullifying effectiveness of a system, installation or project, causing identifiable damage to the national security.



Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

DIRECTORATE OF ADMINISTRATION  
~~SECRET~~  
CLASSIFICATION GUIDE (DACG)

25X1A

Classification Guide Sections 9a - 9g	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
(3.7) Information concerning methods and techniques for providing physical security to a facility.(U)	CONFIDENTIAL	6 years (review)	Protection of this information for six years and possibly longer is required because it reveals vulnerability or capability data, the unauthorized disclosure of which could result in negating or nullifying effectiveness of a system, installation, or project, causing identifiable damage to the national security.
(3.8) Information concerning locations, frequency, and mode of travel for courier runs and sensitive deliveries.(U)	CONFIDENTIAL	6 years (review)	" "
(3.9) Information concerning inventories, listings, computer printouts, of individual Agency stock items or aggregates of items.(U)	SECRET	20 years (review)	Extended protection of this information is required, because it reveals vulnerability or capability data, the unauthorized disclosure of which could result in negating or nullifying effectiveness of a system, installation, or project, causing serious damage to the national security.
	SECRET	20 years (review)	" "

25X1C

Approved For Release 2001/11/08 : ~~SECRET~~ CIA-RDP94B01041R000300080003-6  
 DIRECTORATE OF ADMINISTRATION  
 CLASSIFICATION GUIDE (DACG)

Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
25X1A [REDACTED]			
(3.11) Information concerning the quantitative computer run of overt Agency Metropolitan space and personnel by component. Information not officially released concerning [REDACTED]	SECRET	20 years (review)	Extended protection of this information is required because it could reveal vulnerability/capability data, the unauthorized disclosure of which could result in serious damage to national security.
25X1A [REDACTED]			
(3.12) Information concerning procedures for procurement contracts and contractors.(U)	SECRET	20 years (review)	Extended protection of this information is required, because it could reveal intelligence sources/methods, vulnerability/capability data, the unauthorized disclosure of which could result in negating or nullifying effectiveness of a system, operation, installation, or project, causing serious damage to national security.
(3.13) Information concerning the organization, location, mission and support activities pertinent to staybehind agent networks.(C)	SECRET	6 years (review)	Extended protection of this information is required because its unauthorized disclosure could jeopardize intelligence mechanisms planned or in being, the loss of which could reveal intelligence sources and methods, deprive the U.S. of a defense capability and/or place an individual in jeopardy causing serious damage to the national security.

~~SECRET~~  
 DIRECTORATE OF ADMINISTRATION  
 CLASSIFICATION GUIDE (DACG)

25X1A	Classification Guide Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
	<u>OFFICE OF SECURITY</u>			
25X1A	[REDACTED]	CONFIDENTIAL	20 years (review)	Extended protection at CONFIDENTIAL level is required because this information reveals intelligence methods, vulnerability and capability data, the unauthorized disclosure of which could result in negating or nullifying effectiveness of a system, installation or project, causing identifiable damage to the national security.
<del>25X1A</del>	[REDACTED]	SECRET	20 years (review)	Extended protection at SECRET level is required because this information reveals intelligence operations or activities, the unauthorized disclosure of which could result in negating, nullifying, or impeding their effectiveness, causing serious damage to the national security.
25X1A	<u>OFFICE OF PERSONNEL</u>			
	(3.16) Information disclosing the organizational structure of individual components of the Central Intelligence Agency. (U)	SECRET	20 years (review)	This information is specifically protected by statute, and unauthorized disclosure could result in serious damage to national security.
	(3.17) Current and planning-related information disclosing the numbers, grades, skills and assignments of personnel. (U)	SECRET	10 years (review)	Extended protection at the SECRET level is required because it reveals quantitative and qualitative Agency internal data, including the nature, objectives, requirements, priorities, scope and thrust of Agency activities, the unauthorized disclosure of which could cause serious damage to the national security.



~~SECRET~~

DIRECTORATE OF ADMINISTRATION  
CLASSIFICATION GUIDE (DACG)

25X1A	Classification Guide Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
-------	---	-------------------------------	----------------------------------	--

25X1C  


(5.1) SEE ANNEX A (COVER ANNEX) FOR INFORMATION PERTINENT TO THIS SECTION.(U)

(5.2) " "

(6) Information pertaining to contractual relationships with private individuals, commercial concerns, or non-governmental 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.(U)

OFFICE OF LOGISTICS

(6.1) Information concerning administration of such contracts and methods and procedures for contracting with individuals, non-governmental institutions, or commercial companies where the contractual relationship, product, the identity of the Federal agency involved, the identity of the contractor, or any other aspect of the relationship is classified.(U)

CONFIDENTIAL

20 years  
(review)

Extended protection of this information is essential to protect intelligence activities sources and methods, the unauthorized disclosure of which could result in compromise and loss, negating Agency operations, projects, or systems and causing identifiable damage to the national security.

~~SECRET~~

DIRECTORATE OF ADMINISTRATION  
CLASSIFICATION GUIDE (DAGC)

25X1A

Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
(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.(U)			
<u>OFFICE OF LOGISTICS</u>			
(7.1) Information concerning Agency procurement policies and procedures.(U)	CONFIDENTIAL	6 years (review)	Maintenance of classification of this information for six years and possibly longer is essential because it reveals intelligence methodologies, the unauthorized disclosure of which could cause identifiable damage to national security.
<u>OFFICE OF TRAINING</u>			
(7.2) Information pertaining to analytical methods, computer simulations and models, equipment selection, design, purchase, installation, or procedures, policies and programs for the training of personnel.(U)	SECRET	6 years (review)	Maintenance of classification of this information for six years and possibly longer is essential because it reveals intelligence methodologies, the disclosure of which could cause serious damage to national security.

-25-  
~~SECRET~~

**SECRET**  
 DIRECTORATE OF ADMINISTRATION  
 CLASSIFICATION GUIDE (DACC)

25X1A

Classification Guide Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
<p>(8) Information which 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.(U)</p>			
<p><u>OFFICE OF TRAINING</u></p>			
<p>(8.1) Information dealing with course descriptions, lecture outlines, training aids, texts, student rosters, speaker lists, critiques, and subject identification involving the teaching of Agency unique analytical methods, automated systems, information sources and techniques.(U)</p>	SECRET	6 years (review)	<p>Maintenance of classification of this information for six years and possibly longer is required because it reveals intelligence methods whose unauthorized disclosure could cause serious damage to national security.</p>
<p>(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.(U)</p>			
<p><u>OFFICE OF COMMUNICATIONS</u></p>			
<p>(9.1) Information concerning the CRITIC communication system.(U)</p>	SECRET	20 years (review)	<p>Continued protection of the information is essential to national security because it reveals intelligence sources, methods, vulnerability or capability data, the unauthorized disclosure of which could result in negation of a system, causing serious damage to national security.</p>

25X1A

Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
--	-------------------------------	----------------------------------	--

(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.(U)

DIRECTORATE WIDE

(10.1) Cryptographic information, including all cryptographic keying material, detailed information concerning cryptographic systems, information concerning the weakness of cryptographic systems, any other materials or information concerning cryptographic logic or keying; i.e., photoplates, screen masks, chips, etc.(U)

TOP SECRET

20 years  
(review)

This information is specifically protected by statute and its unauthorized disclosure could result in exceptionally grave damage to the national security.

25X1A

(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.(U)

OFFICE OF TRAINING

(11.1) Video tapes, audio tapes, motion pictures, photographs, slides, vu-graphs, charts, brochures, and other aural-visual materials produced for purposes of announcement, background, or subject information in displays, briefings, scheduled or special training programs, both overt and covert, conducted domestically or in foreign locations.(U)

CONFIDENTIAL

6 years  
(review)

Protection of this information for six years and possibly longer is necessary because it reveals intelligence sources, methods, vulnerability and capability data, the unauthorized disclosure of which could result in nullification of plans, operations, activities, and/or loss of intelligence advantage causing identifiable damage to national security.

25X1A



Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6  
~~SECRET~~  
 DIRECTORATE OF ADMINISTRATION  
 CLASSIFICATION GUIDE (DACG)

25X1A

Classification Guide Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
(11.2) Course descriptions, outlines, syllabus, lecture notes, student materials, reports, evaluations, registration procedures, catalogs, selection criteria, roster, instructor and guest speaker lists, training sites, locations and facilities.(U)	SECRET	6 years (review)	Extended protection of this information is necessary because it reveals intelligence sources, methods, vulnerability and capability data, the unauthorized disclosure of which could result in nullification of plans, operations, activities and/or loss of intelligence advantage causing serious damage to national security.
(11.3) Agency training record, enrollment procedures, student selection criteria, course selection procedures, institution or facility selection policies, procedures, financial arrangements and information which reveals the identification of former, present, or prospective students.(U)	SECRET	20 years (review)	Extended protection of this information is necessary because it reveals intelligence sources, methods and Agency internal data, the unauthorized disclosure of which could result in impeding the training of intelligence personnel, causing serious damage to national security.

~~SECRET~~

25X1A

Classification Guide Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
(12) Information not officially released that could disclose CIA policies and procedures used for personnel recruitment, assessment, selection, training, assignment, and evaluation.(U)			
<u>OFFICE OF MEDICAL SERVICES</u>			
(12.1) Information concerning psychological tests, test results and evaluations of Agency employees and applicants for employment.(U)	CONFIDENTIAL	Unsuccessful Applicant Files: 6 years Employee Files: 20 years review, or six years after separation from the Agency, whichever occurs first.	Extended protection of this information is essential because it reveals intelligence methods, the unauthorized disclosure of which could result in identifiable damage to the national security.
(12.2) Information concerning Medical Evaluation Systems.(U)	CONFIDENTIAL	10 years (review)	Extended protection of this information is essential because it reveals intelligence methods, the unauthorized disclosure of which could result in identifiable damage to the national security.

SECRET  
 Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6  
 DIRECTORATE OF ADMINISTRATION  
 CLASSIFICATION GUIDE (DAGC)

25X1A

Classification Guide <span style="background-color: black; color: black;">[REDACTED]</span> Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
<u>OFFICE OF PERSONNEL</u>			
(12.3) Information concerning recruitment policy and management matters, instructions, directives, guidance and specific action requests to recruiters, and analyses of recruitment activity and results.(U)	SECRET	20 years (review)	Extended protection of this information is essential because it reveals plans, operations, or activities important to national security, the unauthorized disclosure of which can reasonably be expected to result in negating or nullifying the effectiveness of Agency recruitment activity, or impeding its orderly implementation.
(12.4) Information concerning assessment, selection, and evaluation of Agency employees and applicants.(U)	SECRET	20 years (review)	Extended protection of this information is essential because it reveals intelligence methods and Agency internal data specifically protected by statute (CIA Act of 1949), the unauthorized disclosure of which could result in serious damage to the national security.

**SECRET**  
 Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6  
 DIRECTORATE OF ADMINISTRATION  
 CLASSIFICATION GUIDE (DACG)

25X1A

Classification Guide (9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
<u>OFFICE OF TRAINING</u>  (12.5) Information concerning policies and procedures for recruitment, assessment, selection, training, assignment, and evaluation of personnel for the Career Training Program, internal CIA training programs, sensitive U.S. Government conducted or sponsored training programs when the information concerns covert relationships or would identify personnel who have been, are, or may be under cover or would reveal a unique Agency interest in a particular subject matter, training facility or educational institution.(U)	SECRET	20 years (review)	Extended protection of this information is essential because it reveals intelligence methods and Agency internal data specifically protected by statute (CIA Act of 1949), the unauthorized disclosure of which could result in serious damage to the national security.



Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6  
SECRET  
DIRECTORATE OF ADMINISTRATION  
CLASSIFICATION GUIDE (DAG)

25X1A

Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
<u>9d. Foreign Relations or Foreign Activities of the United States</u>			
(1) Information that, if disclosed, could lead to foreign political, economic or military action against the United States or other friendly nations.(U)			
(1.1) RESERVED			
(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.(U)			
(2.1) RESERVED			
(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 resolution or avoidance of international conflicts or differences having national security significance.(U)			
(3.1) RESERVED			

~~SECRET~~  
DIRECTORATE OF ADMINISTRATION  
CLASSIFICATION GUIDE (DACC)

25X1A

Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
(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.(U)			
(4.1) RESERVED			
(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.(U)			
<u>OFFICE OF FINANCE</u>			
(5.1) Information dealing with budget, expenditure, funding or other fiscal aspects which reveals, or information which could, when joined with other information, reveal or identify activities conducted abroad in support of nonattributable national foreign policy objectives of the United States Government.(C)	SECRET	20 years (review)	Extended protection of this information at Secret level is essential because it reveals details of foreign policy and relations matters extending to the highest levels of the Government, the unauthorized disclosure of which could lead to widespread repercussions and serious damage to national security.

~~SECRET~~  
DIRECTORATE OF ADMINISTRATION  
CLASSIFICATION GUIDE (DACG)

25X1A

Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
(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.(U)			
(6.1) RESERVED			
(7) Information which, 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.(U)			
<u>OFFICE OF SECURITY</u>			
(7.1) Information derived from Office of Security surveys of overseas Agency installations, including personal residences, reflecting their security posture and vulnerabilities.(U)	SECRET	20 years (review)	Extended protection of this information is essential because it reveals vulnerability capability data, the unauthorized disclosure of which could result in loss of or impair security protection for Agency operations, installations and personnel, and/or place in immediate jeopardy a person important to national security.



E

**SECRET**  
DIRECTORATE OF ADMINISTRATION  
CLASSIFICATION GUIDE (DACG)

25X1A	Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
-------	--	-------------------------------	----------------------------------	--

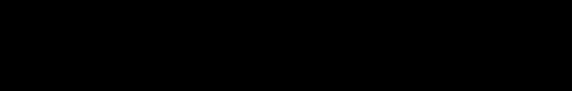
9e. Scientific, technological, or economic matters relating to the national security

(1) Information that provides the United States with a scientific, technical, engineering, economic or intelligence advantage of value to the national security.(U)

(1.1) RESERVED

(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.(U)

OFFICE OF MEDICAL SERVICES

25X1C		TOP SECRET	10 years (review)	Extended protection of this information is essential to national security because it reveals intelligence methods, sources, plans, operations, or activities which, if lost, cannot be regained or replaced or if disclosed, could be negated, nullified or impeded, causing exceptionally grave damage to the national security.
-------	---	------------	----------------------	---

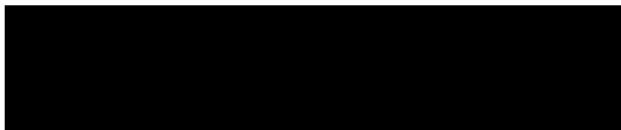
Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

**SECRET**  
DIRECTORATE OF ADMINISTRATION  
CLASSIFICATION GUIDE (DACG)

	Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
--	--	-------------------------------	----------------------------------	--

25X1A

25X1A



(3.1)

RESERVED

F

25X1A

Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
--	-------------------------------	----------------------------------	--

9f. 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.(U)

(1.1) RESERVED

(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 to be restricted in a manner detrimental to national security.(U)

(2.1) RESERVED

G

**SECRET**

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6  
DIRECTORATE OF ADMINISTRATION  
CLASSIFICATION GUIDE (DACG)

25X1A

Classification Guide (Sections 9a - 9g)	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
9g. <u>Other categories of information related to national security and determined by the Director of Central Intelligence to require protection against unauthorized disclosure.</u> (U)			
(1) Information that could be expected to place a person in jeopardy. (U)			
<u>DIRECTORATE WIDE</u>			
(1.1) Any activity of the Directorate of Administration which could place a person in jeopardy. (U) (Not to be used until approved by the DCI)	CONFIDENTIAL	20 years (review or until the state of jeopardy terminates.	Extended protection of this information is essential to protect a person important to the national security and its unauthorized disclosure could result in identifiable damage to the national security.

**SECRET**

H



25X1C

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

**SECRET**

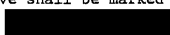
<sup>C</sup>  
A9a5.2

Information that could identify Agency personnel under official cover, but which does not identify the cover organization and which is not otherwise classified or classifiable.

Level of Classification: Confidential

Duration of Initial Classification: 20 years/review

Justification: Central Intelligence Act of 1949 (50 U.S.C. 403a), as amended.

Note: Documents which contain the types of information specified under A9<sup>C</sup>5.1 and A9<sup>C</sup>5.2 above shall be marked "WARNING NOTICE - INTELLIGENCE SOURCES AND METHODS INVOLVED" as provided in section 12 

25X1A

**SECRET**

1

**SECRET**

DIRECTORATE OF ADMINISTRATION CLASSIFICATION GUIDE

ANNEX B

JUSTIFICATIONS FOR USE BY ORIGINAL TOP SECRET CLASSIFIERS FOR EXTENSION OF CLASSIFICATION BEYOND SIX YEARS

Officials with original Top Secret classification authority have the option of using an approved Classification Guide to establish the duration of classification for information (acting as derivative classifiers), or may extend classification beyond six years without reference to a Guide upon a determination based on their knowledge, experience or common sense that an initial classification beyond six years is required (acting as original classifiers). Information for which classification is thus extended shall be marked appropriately (see Paragraph 12b [redacted] and 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 from Paragraph 3d [redacted]. Such citations (e.g., "3d(3)") constitute the Top Secret classifier's certification that the information is expected to retain its [redacted] security sensitivity, and therefore requires continued protection. The following citations may be used, as applicable, for information that:

- (1) Is foreign government information, as described in paragraph 9b [redacted] and this Guide, 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 of [redacted] and this Guide) 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 [redacted] and this Guide, 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 of [redacted] and this Guide) 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 of [redacted] and this Guide 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 of [redacted] and this Guide 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 [redacted] and this Guide) or other informational advantage;
- (8) Could, if revealed after six years, place a person in jeopardy.

**SECRET**

DIRECTORATE OF ADMINISTRATION  
CLASSIFICATION GUIDE

PEN AND INK CHANGES

In Section 4.3, page 23, line 3, after the word surveillance please add the word "countermeasure."

In Annex A, page 39, please change the citation "A9a5.1" to "A9c5.1."

In Annex A, page 40, please change the citation "A9a5.2" to "A9c5.2." Please change the citations in the "Note" from "A9a5.1 and A9a5.2" to "A9c5.1 and A9c5.2."

DISTRIBUTION: SPECIAL

22 December 1978

SECRET

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

SECRET

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6  
CONFIDENTIAL

## DIRECTORATE OF OPERATIONS CLASSIFICATION GUIDE

Copy No. 110

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

E2 IMPDET  
CL BY: 059687



Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

## CONFIDENTIAL

DIRECTORATE OF OPERATIONS CLASSIFICATION GUIDE

### FOREWORD

1. This Directorate of Operations Classification Guide (DOCG) is designed in accordance with the requirements of E.O. 12065 and is approved effective 1 December 1978. It sets forth the categories of information to be considered for classification, and provides guidance for determining the proper levels of classification (i.e., Confidential, Secret, or Top Secret). For each classifiable subcategory of information, it also sets forth a classification duration limit and a justification for extending classification beyond six years to a maximum of 20 years, or to 30 years in the case of foreign government information.

2. The DOCG is based on the seven general categories of information which can be considered for classification as specified by E.O. 12065. These seven categories, subdivided into broader subcategories, constitute the Agency classification criteria (unclassified) set forth in Sections 9a-9g of [REDACTED]. The DOCG is based on these criteria and assigns a level of classification, duration of classification, and justification for extension of classification beyond six years for each category. A Cover Annex applicable to the Agency as a whole is included as Annex A. The DOCG is applicable to Directorate of Operations (DO) information and material and, in addition to DO personnel, is available for use by personnel of NFAC, the DDA, the DS&T, and Independent Offices for classifying DO information and material.

3. The Guide is essentially a series of predetermined original classification decisions by a Top Secret classifier for information requiring extension of classification beyond six years and as such provides the authority for derivative classification. Persons authorized to classify information, whether originally or derivatively, first should attempt to determine the appropriate classification level and duration



CONFIDENTIAL

for that information from the Guide. If the Guide does not meet the requirement, the person should then request an original classifier to classify the information. If the classification, regardless of level, must be extended beyond six years, the extension must be authorized by a Top Secret classifier who will cite as justification for the extension one of the reasons set forth in Section 3d [redacted] attached as Annex B to the Guide. When it becomes apparent that original classification authority is being continually applied to a category of information not covered by the Guide, that fact should be reported to the Agency Security Classification Officer, ISAS/DDA through the component Records Management Officer so that the Guide may be amended. The Guide should be viewed as the standard reference for all classification, susceptible both to expansion and improvement.

25X1A

4. The letter designation "D" has been assigned to the DOCG to identify it in relation to other Directorate Guides. Citations of the DOCG will be made in the following manner, using as an example D9a.1:

"D" indicates that the citation is from the DOCG;

"9" is the Section [redacted] which contains E.O. 12065 and Agency Classification criteria;

25X1A

"a" is the first of seven E.O. 12065 criteria categories for information subject to classification;

"1" is the first Agency criterion under "a" and represents a more specific breakdown of information categories.

When the DOCG is cited in derivative classification, the appropriate citation will be placed on the material with other required markings. For details on complete marking requirements see Section 12 [redacted]

25X1A

25X1A

[redacted]  
John N. McMahon  
Deputy Director for Operations

29/11/78  
Date

**CONFIDENTIAL**

DIRECTORATE OF OPERATIONS  
CLASSIFICATION GUIDE

	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
<u>D9a. Military plans, weapons or operations</u>			
D9a.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.	S	Review in 20 years	Continued protection of the information is essential to the national security because it reveals intelligence sources or methods which, if lost cannot be regained or replaced, or whose disclosure would cause serious damage to the national security; or the information could reveal vulnerability or capability data, the unauthorized disclosure of which can reasonably be expected to result in negating or nullifying the effectiveness of a system, installation or project important to the national security; or the information concerns plans, operations, or activities important to national security, the unauthorized disclosure of which can reasonably be expected to result in negating or nullifying the effectiveness of the plan, operation or activity, or impeding its orderly implementation.
D9a.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.	S	Review in 20 years	Same as D9a.1
D9a.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. (This would include intelligence war planning such as Staybehind, Escape and Evasion, [REDACTED] Covert Action, etc.)	S	Review in 20 years	Same as D9a.1

25X1C

**CONFIDENTIAL**

**CONFIDENTIAL**

D9b. <u>Foreign government information</u>	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
D9b.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.	Equivalent to foreign gvt. classification.	Review in 30 years	This information is foreign government information as defined in E.O. 12065, i.e., information that has been provided to the United States in confidence by, or produced by the United States pursuant to a written joint arrangement requiring confidentiality with, a foreign government or international organization of governments.
D9b.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.	TS, S, C in accordance w/ agreed class. determinations.	Review in 30 years	Same as D9b.1
D9b.3 - Information revealing the past, present, or proposed existence of joint intelligence activities or facilities or the nature thereof in foreign countries.	TS, S, C in accordance w/ agreed class. determinations.	Review in 30 years	Same as D9b.1
D9c. <u>Intelligence activities, sources or methods</u>			
D9c.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. (Human sources include witting or unwitting agents, informants, collaborators, and defectors used in operations or in support of operations.) (For information dealing with cover, see Annex A, Part I (D9c.12) or Part II (D9c.13).)	S	Review in 20 years	Continued protection of the information is essential to the national security because it reveals intelligence sources or methods which, if lost, cannot be regained or replaced, or whose disclosure would cause serious damage to the national security; or the information could reveal vulnerability or capability data, the unauthorized disclosure of which can reasonably be expected to result in negating or nullifying the effectiveness of a system, installation or project important to the national security; or the information concerns plans, operations, or activities important to national security, the unauthorized disclosure of which can reasonably be expected to result in negating or nullifying the effectiveness of the plan, operation or activity, or impeding its orderly implementation.

**CONFIDENTIAL**


**CONFIDENTIAL**

	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
D9c.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. (Methods include cover (See Annex A), security, training, tradecraft, funding, communications, records, technical equipment, and services.)	S	Review in 20 years	Same as D9c.1
D9c.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 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 missions, functions, and locations of certain CIA components or installations. (Such information on intelligence activities includes operational proposals, plans, directives, correspondence, reports, management reviews, summaries and histories.)	S	Review in 20 years	Same as D9c.1; or is information specifically protected by statute.
D9c.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. (For information dealing with cover, see Annex A, Part I (D9c.12) or Part II (D9c.13).)	S	Review in 20 years	Same as D9c.1
D9c.5 - Information that could reveal the existence, nature, scope, or effect of, or identify personnel covered	S or equivalent to foreign gvt. classification.	Review in 20 years/30 years if foreign gvt. information.	Continued protection of the information is essential to the national security because it reveals intelligence sources or methods which, if lost, cannot be regained or replaced, or whose disclosure would cause

25X1C

**CONFIDENTIAL**

**CONFIDENTIAL**

	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
D9c.6 - Information pertaining to contractual relationships with private individuals, commercial concerns, or non-governmental 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.	S	Review in 20 years	Same as D9c.1
D9c.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.	S	Review in 20 years	Same as D9c.1
D9c.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. (Subjects	S	Review in 20 years	Same as D9c.1
			
D9c.9 - 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.	S	Review in 20 years	This information pertains to cryptography and thus its continued protection is absolutely essential to the national security.

25X1C

**CONFIDENTIAL**

**CONFIDENTIAL**



	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
D9c.10- 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.	S	Review in 20 years	Same as D9c.1
D9c.11- Information not officially released, that could disclose CIA policies and procedures used for personnel recruitment, assessment, selection, training, assignment, and evaluation.	C	Review in 20 years	Same as D9c.1
D9c.12- See Annex A, Part I for information concerning cover in general.			
D9c.13- See Annex A, Part II for information concerning certain types of official cover only.			
D9d. <u>Foreign relations or foreign activities of the United States</u>			
D9d.1 - Information that, if disclosed, could lead to foreign political, economic, or military action against the United States or other friendly nations.	S	Review in 20 years	This information concerns foreign relations matters, the continued protection of which is essential to the national security.
D9d.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.	S	Review in 20 years	Same as D9d.1
D9d.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 resolution or avoidance of international conflicts or differences having national security significance.	S	Review in 20 years	Same as D9d.1
D9d.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.	S	Review in 20 years	Same as D9d.1

**CONFIDENTIAL**

**CONFIDENTIAL**

	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
<p>D9d.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.</p>	S	Review in 20 years	<p>Continued protection of this information is essential to the national security because it reveals intelligence sources or methods which, if lost, cannot be regained or replaced, or whose disclosure would cause serious damage to the national security; or the information could reveal vulnerability or capability data, the unauthorized disclosure of which can reasonably be expected to result in negating or nullifying the effectiveness of a system, installation or project important to the national security; or the information concerns plans, operations, or activities important to national security, the unauthorized disclosure of which can reasonably be expected to result in negating or nullifying the effectiveness of the plan, operation or activity, or impeding its orderly implementation; or the information concerns foreign relations matters, the continued protection of which is essential to the national security.</p>
<p>D9d.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.</p>	S	Review in 20 years	<p>Same as D9d.5</p>
<p>D9d.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.</p>	C	Review in 6 years	<p>The information concerns foreign relations matters, the continued protection of which is essential to the national security; or disclosure of the information would place in immediate jeopardy a person important to the national security.</p>
<p>D9e. <u>Scientific, technological or economic matters relating to the national security</u></p>			
<p>D9e.1 - Information that provides the United States with a scientific, technical, engineering, economic, or intelligence advantage of value to the national security.</p>	C	Review in 6 years	<p>The information concerns plans, operations, or activities important to national security, the unauthorized disclosure of which can reasonably be expected to result in negating or nullifying the effectiveness of the plan, operation or activity, or impeding its orderly implementation.</p>

**CONFIDENTIAL**

**CONFIDENTIAL**

	Level of Classification	Duration of Classification	Justification for Extension Beyond Six Years
D9e.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 counter-intelligence.	S	Review in 20 years	Continued protection of the information is essential to the national security because it reveals intelligence activities, sources or methods which, if lost, cannot be regained or replaced, or whose disclosure would cause serious damage to the national security; or the information could reveal vulnerability or capability data, the unauthorized disclosure of which can reasonably be expected to result in negating or nullifying the effectiveness of a system, installation or project important to the national security; or the information concerns plans, operations, or activities important to national security, the unauthorized disclosure of which can reasonably be expected to result in negating or nullifying the effectiveness of the plan, operation, or activity, or impeding its orderly implementation.
D9e.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.	S or equivalent to foreign gvt. classification.	Review in 20 years/30 years if foreign gvt. information.	Same as D9e.2; or the information is foreign government information as defined in E.O. 12065, i.e., information that has been provided to the United States in confidence by, or produced by the United States pursuant to a written joint arrangement requiring confidentiality with, a foreign government or international organization of governments.
D9f. <u>United States Government programs for safeguarding nuclear materials or facilities</u>			
D9f.1 - 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.	S	Review in 20 years	Continued protection of the information is essential to the national security because it reveals intelligence sources or methods which, if lost, cannot be regained or replaced, or whose disclosure would cause serious damage to the national security; or the information could reveal vulnerability or capability data, the unauthorized disclosure of which can reasonably be expected to result in negating or nullifying the effectiveness of a system, installation or project important to the national security; or the information concerns plans, operations, or activities important to national security, the unauthorized disclosure of which can reasonably be expected to result in negating or nullifying the effectiveness of the plan, operation or activity, or impeding its orderly implementation.

**CONFIDENTIAL**



**CONFIDENTIAL**

Level of Classification      Duration of Classification

Justification for Extension Beyond Six Years

D9g. Other categories of information related to national security and determined by the Director of Central Intelligence to require protection against unauthorized disclosure

D9g.1 - Information that could be expected to place an individual in immediate jeopardy.

C

Until jeopardy is no longer a factor. Review in 6 years.

Involves jeopardy of life.

(Other categories may be added later.)

**CONFIDENTIAL**

**CONFIDENTIAL**

DIRECTORATE OF OPERATIONS CLASSIFICATION GUIDE

ANNEX A  
COVER

Part I

References:

- a. Executive Order 12065, Section 1-301(c)  
(Intelligence activities, sources or methods)
- b. Agency Classification Guide, Section D9c  
(Intelligence activities, sources or methods)

D9c.12 Information concerning the acquisition, implementation, use, maintenance and termination of foreign and domestic cover for Agency personnel, activities, and installations, including the operational, financial, logistical, communications, personnel administration, and security aspects of such cover as regards:

- A. The techniques and methods used to establish, maintain, use and terminate official and non-official cover;
- B. The identification of official and non-official cover units, facilities, organizations or installations;
- C. The Agency's use of personnel, funds, materiel, real or other property, equipment or other assets in support of cover facilities or activities;
- D. The identification of Agency employees or agents in relation to their cover, when both the employee or agent and the cover unit or organization are specified;
- E. The identification of official or non-official organizations, entities or persons providing cover;
- F. The identification of official or non-official organizations, entities or persons providing operational, financial, logistical or other support for cover;
- G. The identification of personnel who are, have been, or are expected to be under non-official cover.

Level of Classification: Secret  
Duration of Initial Classification: 20 years/review  
Justification: Central Intelligence Act of 1949 (50 U.S.C. 403a), as amended.

**CONFIDENTIAL**

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

~~CONFIDENTIAL~~

ANNEX A  
COVER

Part II

D9c.13 Information that could identify Agency personnel under official cover, but which does not identify the cover organization and which is not otherwise classified or classifiable.

Level of Classification: Confidential  
Duration of Initial Classification: 20 years/review  
Justification: Central Intelligence Act of 1949 (50 U.S.C. 403a), as amended.

Note: Documents which contain the types of information specified under I and II above shall be marked "WARNING NOTICE - INTELLIGENCE SOURCES AND METHODS INVOLVED" as provided in Section 12 [REDACTED]

25X1A

~~CONFIDENTIAL~~

CONFIDENTIAL

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

CONFIDENTIAL

DIRECTORATE OF OPERATIONS CLASSIFICATION GUIDE  
ANNEX B

JUSTIFICATION FOR USE BY ORIGINAL TOP SECRET CLASSIFIERS  
FOR EXTENSION OF CLASSIFICATION BEYOND SIX YEARS

The following is a list of the justifications to be used to extend classification as taken from paragraph 3d of [redacted] and which are referred to in paragraph 3 of the Foreword to this Guide. They should be cited (e.g., "3d(1)") as applicable, for information that:

25X1A

3d(1) Is foreign government information, as described in paragraph 9b of [redacted] which is identical to paragraph 9b of this Guide), 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.

25X1A

3d(2) Pertains to United States Government programs for safeguarding nuclear materials or facilities as described in paragraph 9f of [redacted] (identical to paragraph 9f of this Guide) 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.

25X1A

3d(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 of [redacted] (identical to paragraph 9c of this Guide), which require protection for longer than six years.

25X1A

3d(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.

3d(5) Otherwise concerns intelligence or counterintelligence programs or activities as described in paragraph 9c of [redacted] (identical to paragraph 9c of this Guide) 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.

25X1A

3d(6) Pertains to a military plan, weapon or weapons systems or operation as described in paragraph 9a of [redacted] (identical to paragraph 9a of this Guide) 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.

25X1A

3d(7) Concerns diplomatic or other foreign relations matters or activities as described in paragraph 9d of [redacted] (identical to paragraph 9d of this Guide) 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 of [redacted] and identical to paragraph 9e of this Guide) or other informational advantage.

25X1A

3d(8) Could, if revealed after six years, place a person in jeopardy.

25X1A

CONFIDENTIAL

Approved For Release 2001/11/08 : CIA-RDP94B01041R000300080003-6

CONFIDENTIAL

CONFIDENTIAL