Approved For Release 2003/09/04 : CIA-RDP84B00890R000300040002-1

13 August 1981
OGC 81-06910

81-1714

MEMORANDUM FOR: Director, National Foreign Assessment Center
Deputy Director for Operations
Deputy Director for Science & Technology
Deputy Director for Administration
Comptroller
Legislative Counsel
Director of Personnel
Director of Public Affairs
Director, Equal Employment Opportunity
Director of Security
Special Assistant to the DCI for
Compartmentation
Director of Information Services, DDA

FILE: Legal

STAT FROM: [redacted]
Office of General Counsel

SUBJECT: Revision of Executive Order 12065,
"National Security Information"

Enclosed for your review is the final draft of the revision of Executive Order 12065. This draft will hopefully be finalized by the end of next week (21 August 1981), and provided to the National Security Council for eventual presentation to the President. Comments concerning this draft should be provided to me by telephone no later than Monday, 17 August 1981. Because this draft represents the fruits of months of negotiation between the members of the interagency group, comments should be limited to changes which are thought essential to the effective administration of the Order.

[redacted] STAT

Executive Order _____

National Security Information

The interests of the United States and its citizens require that certain information in the Government's possession concerning our national defense and foreign relations be uniformly protected against unauthorized disclosure. It also is essential that the public be informed concerning the activities of its Government. To ensure that national security information is adequately safeguarded, this Order identifies the information to be so protected, prescribes classification, declassification, and safeguarding standards to be followed, and establishes a monitoring system to ensure its effectiveness.

SECTION 1. ORIGINAL CLASSIFICATION.

1-1. Classification Designation.

1-101. Information that requires protection against unauthorized disclosure in the interest of national security shall be classified in one of the three categories listed below. If there is a reasonable doubt as to which category is appropriate or whether the information should be classified at all, the information shall be protected at an appropriate level of classification until a final determination is made as to the need for protection and the level of required protection. No other categories of classification shall be used to identify information as requiring protection in the interest of national

security, except as otherwise provided by statute. Nothing in this Order shall be construed as limiting the protection afforded national security information by other provisions of law.

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

1-103. "Secret" shall be applied 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 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 agency heads or officials as the President may designate by publication in the Federal Register, and by officials to whom such authority is delegated in accordance with Section 1-204.

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

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

1-204. Limitation on Delegation of Original Classification Authority.

(a) Authority for original classification of information as Top Secret may be delegated only to principal subordinate officials who have a need to exercise such authority as determined by the President, by agency heads or officials designated pursuant to Section 1-201, or by senior officials with Top Secret classification authority who have been designated in writing to exercise this authority by such agency heads.

(b) Authority for original classification of information as Secret may be delegated only to subordinate officials who have a need to exercise such authority as determined by the President, by agency heads or officials designated pursuant to Section 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 need to exercise such authority as determined by the President, by agency heads designated pursuant to Section 1-201, 1-202, and 1-203, and by officials with Top Secret classification authority.

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

(e) Delegations of original classification authority shall be limited to the absolute minimum required to exercise such authority to effectively and efficiently administer this Order. Agency heads will be responsible for ensuring that officials so designated have a demonstrable and 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 a manner consistent with this Order and its implementing directives. The information shall be transmitted promptly under adequate safeguards to the agency which has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 30 days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the

Information Security Oversight Office for review. The Director shall consult with any agency determined to have a subject matter interest in this information before making a classification determination.

1-3. Classification Requirements.

1-301. Information shall be considered for classification if it concerns:

(a) military plans, weapons, or operations;

(b) the vulnerabilities or capabilities of systems, installations, projects, or plans vital to the national security;

(c) foreign government information;

(d) intelligence activities, including special activities, or intelligence sources or methods;

(e) foreign relations or foreign activities of the United States;

(f) scientific, technological, or economic matters relating to the national security;

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

(h) cryptology;

(i) an individual whose life or safety may be placed in jeopardy by disclosure of such information;

(j) techniques, procedures or material relating to the protective mission of the United States Secret Service or other agencies with similar responsibilities;

(k) a confidential source as defined in section 6-105; or

(l) other categories of information which are related to national security and which require protection against unauthorized disclosure as determined by the President or agency heads who have original classification authority. Any determination made under this subsection shall be reported promptly to the Director of the Information Security Oversight Office.

1-302. Information which is determined to concern one or more of the criteria in Section 1-301 shall be classified when an original classification authority also determines that its unauthorized disclosure reasonably could be expected to cause damage to the national security. In considering whether the

disclosure of information could be expected to cause damage to the national security, it is not necessary to consider such information in isolation. Information shall be classified if its unauthorized disclosure, when considered in the context of other information, reasonably could be expected to cause such damage.

1-303. Unauthorized disclosure of foreign government information, information which could compromise the identity of a confidential source, information relating to intelligence activities, including special activities, or intelligence sources or methods, or cryptology is presumed to cause damage to the national security.

1-304. Information classified in accordance with Section 1-3 shall not be automatically declassified as a result of any unofficial publication, or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information.

1-4. Duration of Classification.

1-401. Information shall be classified for as long as required by national security considerations. Procedures shall be developed by agencies to ensure the effectiveness and integrity of the classification system while eliminating the accumulation of classified information which no longer requires protection. Information should be considered for downgrading or declassification as soon as practicable based on the degree to which the passage of time or the occurrence of a specific event

or events may have eliminated or reduced the original national security sensitivity of this information. If appropriate, original classification authorities shall set a specific date or event for declassification at the time the information is originally classified.

1-402. Except as permitted under the systematic review for declassification procedures of Section 3-3, information subject to automatic declassification pursuant to limitations on duration of classification specified in predecessor orders shall not be automatically declassified.

1-5. Identification and Markings.

1-501. At the time of original classification, the following shall be shown on the face of all classified documents, and prominently displayed, where practicable, on all other forms of classified information, except where such markings would reveal a confidential source or relationship not otherwise evident from the face of such documents or information:

(a) the office of origin;

(b) the date or event for declassification or the notation " Declassify Upon Notification of Originator"; and

(c) one of the three classification designations defined in Section 1-1.

1-502. Only the designations Top Secret, Secret, or Confidential may be used to identify classified information. Markings such as "For Official Use Only", "Limited Official Use" or "Sensitive" may not be used for that purpose.

1-503. Each classified document shall be marked or shall otherwise indicate which portions are classified with the appropriate classification designation, and which portions are not classified. The President and agency heads designated pursuant to Section 1-2 may, for good cause, except information under their classification jurisdiction from this portion-marking requirement.

1-504. 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.

1-6. Limitations on Classification.

1-601. Classification shall be determined solely on the basis of national security considerations. In no case shall information be classified in order to conceal violations of law, inefficiency or administrative error, to prevent embarrassment to a person, or organization or agency, or to restrain competition,

or to prevent for any other reason the release of information which does not require protection in the interest of national security.

1-602. 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.

1-603. A document may be classified after an agency has received a request for the document under the Freedom of Information Act or Privacy Act of 1974, or the Mandatory Review provisions of this Order (Section 3-4) if such classification is consistent with this Order and is authorized by the agency head, the deputy agency head, or by senior agency officials designated by such agency heads. Classification authority under this provision shall be exercised personally, on a document-by-document basis.

1-604. Information which has been reviewed for declassification under the procedural and substantive criteria of E.O. 12065 pursuant to a Freedom of Information Act or Privacy Act or Mandatory Review request which is still pending at the time this Order becomes effective, need not be rereviewed under the provisions of this Order, though an agency may in its sole discretion apply the provisions of this Order.

SECTION 2. DERIVATIVE CLASSIFICATION.

2-1. Use of Derivative Classification.

2-101. 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 need not possess original classification authority.

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

(a) observe and respect original classification decisions, which shall not be altered by the use of a classification level, time limit, or other marking different from the original on any copy, extract, paraphrase, restatement, or summary of any classified item except as specified under approved procedures for downgrading, declassification, or classification review in accordance with Section 3 below; and

(b) carry forward to any newly created documents any assigned dates or events for declassification and any additional authorized markings. A single declassification date or event may be used for documents classified on the basis of multiple sources.

2-2. Classification Guides.

2-201. Agencies may promulgate classification guides to facilitate the proper and uniform classification of information. To the extent that information is classified pursuant to these guides, such classification is derivative classification.

2-202. Each guide shall be approved personally and in writing by an appropriate classification authority. Such approval constitutes an original classification decision.

Section 3. DECLASSIFICATION AND DOWNGRADING.

3-1. Declassification Authority.

3-101. Information shall be declassified or downgraded as soon as national security considerations permit. Information that continues to meet the classification requirements prescribed by Section 1-3 despite the passage of time will continue to be protected in accordance with this Order.

3-102. Agencies shall designate appropriate officials to exercise declassification and downgrading authority. To the fullest extent practicable, information shall be declassified or downgraded by the official who authorized the original classification if that official is still serving in the same position, or by the originator's officially authorized successor. Declassification and downgrading authority also may

7

be exercised by a supervisory official of the original classifier or successor, or by officials delegated such authority by a senior agency official designated pursuant to Section 5-401(a).

3-103. The provisions of this section relating to declassification shall apply to agencies which, under the terms of this Order, do not have original classification authority, but which had such authority under predecessor orders.

3-2. Transferred Information.

3-201. In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this Order.

3-202. In the case of classified information which is not officially transferred in accordance with Section 3-201, but originated in an agency which has ceased to exist and for which there is no successor agency, each agency in possession shall be deemed to be the originating agency for purposes of this Order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency which has an interest in the subject matter of the information.

3-203. Classified information transferred to the General Services Administration for accession into the Archives of the United States shall be downgraded or declassified in accordance with this Order, with directives of the President issued through the National Security Council, and with agency guidelines

promulgated in consultation with the Information Security Oversight Office.

3-3. Systematic Review for Declassification.

3-301. The President and agency heads designated pursuant to Section 1-2, including the heads of agencies which had original classification authority under predecessor orders, may establish procedures for the systematic review of classified information constituting permanently valuable records of the Government, as defined in 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, for the purpose of declassifying or downgrading such information in accordance with the classification requirements of Section 1-3. Guidelines concerning systematic review for declassification may be issued by such agency heads for classified information under their jurisdiction after consultation with the Archivist of the United States and review by the Information Security Oversight Office. Information for which no systematic declassification guidelines are issued, or information which is not identified in these guidelines as requiring systematic review, and for which a prior automatic declassification date has not been established, will be subject to review for declassification in accordance with the mandatory review for declassification provisions of Section 3-4.

3-302. The Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central

Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities, including special activities, or intelligence sources and methods.

3-303. Guidelines issued pursuant to this section will be used by the Archivist of the United States and, upon approval of the issuing authority, any agency having custody of the information.

3-4. Mandatory Review for Declassification.

3-401. Except as provided in Section 3-402, all information classified under this Order or predecessor orders shall be subject to a review for declassification by the originating agency provided:

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

(2) The request describes the documents or material containing the information sought with sufficient specificity to enable the agency to locate it with a reasonable amount of effort.

3-402. Information less than ten years old which was originated by the President, 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 3-401. Such information over ten years old shall be subject to mandatory review for declassification in accordance with the provisions of this section.

3-403. Agencies conducting a mandatory review for declassification shall declassify and release information that no longer requires protection under this Order unless withholding otherwise is warranted under applicable law.

3-404. Agency heads shall develop procedures to process requests for the mandatory review of classified information. The Secretary of Defense shall develop special procedures for the review of classified cryptologic information, and the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities, including special activities, or intelligence sources or methods, after appropriate consultation with affected agencies. The Archivist shall develop special procedures for the review of information in the possession and control of the Administrator of General Services pursuant to 44 U.S.C. 2107 or 2107 note. The above procedures shall be reviewed by the Director, Information Security Oversight Office to ensure, to the extent practicable, that these procedures are consistent with this Order.

3-404. (a) In response to a request for information under the Freedom of Information Act, the Privacy Act, or the Mandatory

Review provisions of this Order, an agency shall refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classifiable under this Order.

(b) When an agency receives any request for documents in its custody that were classified by another agency, it shall refer the request to the agency of origin for processing, and may, after consultation with the originating agency, inform the requestor of the referral. In such cases the referring agency shall respond to the requestor consistent with section 3-404(a).

3-405. Requests for declassification which are submitted under the provisions of the Freedom of Information Act or Privacy Act shall be processed in accordance with the provisions of those Acts. Agencies shall coordinate their review of classified information with other agencies that have a direct interest in the subject matter.

SECTION 4. SAFEGUARDING.

4-1. General Restrictions on Access.

4-101. A person is eligible for access to classified information only after a formal determination of trustworthiness has been reached by agency heads or designated senior officials and provided that such access is essential to the accomplishment of authorized and lawful Government purposes or contractual obligations. Agency heads designated pursuant to section 1-2 shall issue and maintain minimum security investigative standards that must be satisfied for each of the three national security

information classification designations before access to such information is provided.

4-102. Controls shall be established by each agency to ensure that classified information is used, processed, stored, reproduced, transmitted and destroyed only under conditions that will provide adequate protection and prevent access by unauthorized persons. Originating agencies may place restrictions on the reproduction of classified documents and establish other accountability controls in conformity with this policy of protecting classified information from unauthorized disclosure.

4-103. Classified information shall not be disseminated outside the Executive Branch except under conditions which ensure that the information will be given protection equivalent to that afforded within the Executive Branch.

4-104. Except as provided by directives issued by the President through the National Security Council, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency.

4-2. Special Access Programs.

4-201. Agency heads designated pursuant to Section 1-201 may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this Order or predecessor orders. Procedures governing the creation, continuance, and maintenance of such special access programs will be developed by these agency heads. Such programs may be created or continued

only by written direction of these agency heads. For special access programs pertaining to intelligence activities, including special activities, or intelligence sources and methods, this function will be exercised by the Director of Central Intelligence, who will ensure the establishment of minimium security, access, dissemination and control standards for such programs.

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 in the exercise of an agency's sole discretion 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 in the exercise of its sole discretion:

(a) determines in writing that access is consistent with the interests of national security;

(b) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that such information is safeguarded in a manner consistent with this Order; and

(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.

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. The National Security Council will be assisted in this monitoring function by the 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 Assistant to the President for National Security subject to approval by the President. The

Assistant also shall have authority to appoint a staff for the Office.

5-202. The Director shall:

(a) oversee agency actions and review agency implementing regulations 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. Actions taken by the Director under this subsection may be appealed by affected agencies to the National Security Council;

(c) develop, in consultation with the agencies, and promulgate, subject to the approval of the National Security Council, directives for the implementation of this Order;

(d) report annually to the President through the National Security Council on the implementation of this Order;

(e) review requests for original classification authority from agencies or officials not granted original classification authority pursuant to Section 1-2; and

(f) have authority, consistent with the protective purposes of this Order, to require each agency to furnish such reports or information as is necessary to fulfill the Director's responsibilities.

5-3. General Responsibilities.

5-301. Agencies which originate or handle classified information shall:

(a) designate a senior agency official to direct and administer an Information Security Program to include an active oversight program to ensure effective implementation of this Order. This program shall familiarize agency and other personnel who have access to classified information with the provisions of this Order and implementing directives and shall impress upon agency personnel their responsibility to exercise vigilance in complying with this Order;

(b) establish a process to decide appeals from denials of declassification requests submitted pursuant to Section 3-4; and

(c) 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 persons granted access to classified information is reduced to and maintained at the minimum number that is consistent with operational and security requirements and needs.

5-302. Unclassified regulations or guidelines that establish agency information security policy shall be published in the FEDERAL REGISTER.

5-4. Sanctions.

5-401. If the Information Security Oversight Office finds that a violation of this Order or any implementing directive may have occurred, it shall make a report to the head of the agency concerned so that corrective steps may be taken.

5-402. Officers and employees of the United States Government shall be subject to appropriate sanctions if they:

(a) knowingly, willfully or negligently disclose without authorization information properly classified under this Order or predecessor orders; or

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

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

Unauthorized disclosure for purposes of this section includes either a communication or physical transfer of classified information to an unauthorized person.

5-403. Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, or other sanction in accordance with applicable law and agency regulations.

5-404. Agency heads shall ensure that appropriate and prompt corrective action is taken whenever a violation under Section 5-402 occurs.

SECTION 6. GENERAL PROVISIONS.

6-1. Definitions.

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

6-102. "Information" as used in this Order, includes any information or material, regardless of its physical form or characteristics, that is owned by, produced for, by, or under the control of the United States Government.

6-103. "Classified information" means information that has been determined pursuant to this Order or predecessor orders to

require protection against unauthorized disclosure, and that is so designated.

6-104. Foreign government information means:

(a) Any document, material, or information provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that this document, material, or information is to be held in confidence; or

(b) Any information or material produced by the United States pursuant to or as a result of a joint arrangement, with a foreign government or organization of governments requiring that the information, the arrangement, or both be held in confidence.

6-105. "National security" means the national defense and foreign relations of the United States.

6-106. "Confidential source" means the identity of any individual or organization which has provided, or which may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship or both be held in confidence.

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.

6-203. Executive Order No. 12065 of June 28, 1978, is revoked as of the effective date of this Order.

6-204. This Order shall become effective on _____, 1981.