

OGC 78-2661

25 April 1978

MEMORANDUM FOR: Deputy Director for Administration  
Deputy Director for Science & Technology  
Deputy Director for Operations  
Deputy to the DCI for National Intelligence  
Deputy to the DCI for Resource Management  
Deputy to the DCI for Collection Tasking  
Legislative Counsel  
Inspector General  
Comptroller  
Executive Secretary


FROM



Office of General Counsel

SUBJECT

: Executive Order on National Security Information

Attached for your information is a copy of the most recent draft, dated 20 April 1978, of the proposed Executive order on classification. With the possible exception of section 4(e)(3), which is being discussed with the Department of Defense, this version is to be sent to OMB for review and editing before submission to the President for approval. In addition, efforts are now under way to draft a directive to implement this Order. Please do not hesitate to contact me  if you have any questions or comments.

STATINTL



Attachment

NSC review(s) completed.

MORI/CDF Pages 1 thru 27

EXECUTIVE ORDER

-----

NATIONAL SECURITY INFORMATION

By virtue of the authority vested in me by the Constitution 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

Section	Description	
1.	Definitions .....	2
2.	Original Classification .....	3
	(a) Classification Designation .....	3
	(b) Classification Authority .....	4
	(c) Classification Requirements .....	6
	(d) Classification Criteria .....	7
	(e) Limitation on Duration of Classification .....	8
	(f) Classification Identification and Marking .....	8
	(g) Prohibitions .....	9
3.	Derivative Classification of Information .	10
4.	Declassification and Downgrading .....	11
	(a) Declassification Authority .....	12
	(b) Authority Over Transferred Information .....	12
	(c) Declassification Policy .....	13
	(d) Declassification Requirements .....	14
	(e) Systematic Review for Declassification .....	14
	(f) Mandatory Review for Declassification.	16
	(g) Downgrading .....	17

5.	Safeguarding .....	17
	(a) General Restrictions on Access .....	17
	(b) Special Access Programs .....	18
	(c) Access by Historical Researchers and Former Presidential Appointees .....	19
	(d) Reproduction Controls .....	20
6.	Implementation and Review .....	20
	(a) Information Security Oversight Office .....	20
	(b) Interagency Information Security Committee .	22
	(c) Agencies with Original Classification Authority.....	22
	(d) Agencies without Original Classification Authority .....	24
7.	Administrative Sanctions .....	24
8.	Atomic Energy Information or Material .....	24
9.	Interpretation of the Order .....	25
10.	Revocation of Prior Orders and Directives .....	25
11.	Effective Date .....	25

Section 1. Definitions.

(a) "Agency" has the meaning used in 5 U.S.C. 552(e).

(b) "Classified information" means information or material owned by, produced for or by (hereinafter collectively termed "information") that is/in the possession of or under the control of the United States Government that has been determined by proper authority to require protection against unauthorized disclosure in the interest of national security and is so designated.

(c) "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 joint arrangement with, a foreign government or international organization of governments or an official of either.

(d) "National security information" means information that concerns the national defense or foreign relations of the United States.

Section 2. Original Classification.

(a) Classification Designation. National security information that requires protection against unauthorized disclosure may be classified in one of the three designations listed below. If the classifying official has reasonable doubt which designation is appropriate, or whether the information should be classified at all, the less restrictive treatment should be designated or guidance should be sought from an appropriate senior agency official.

(1) "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.

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause identifiable damage to the national security.

(b) Classification Authority.

(1) 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 the provisions of subsection (4) below:

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 of the United States

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, General Services Administration (delegable only to the Director, Federal Preparedness Agency and to the Director, Information Security Oversight Office.)

(2) 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 so authorized in accordance with the provisions of subsection (4):

The Secretary of Commerce

The Secretary of Transportation

The Administrator, Agency for International Development

The Director, International Communication Agency

(3) 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 so authorized in accordance with subsection (4):

The President and Chairman, Export-Import Bank of the United States

The President and Chief Executive Officer, Overseas Private Investment Corporation

(4) Limitations on Delegation of Classification Authority.

(i) Authority for original classification of information as "Top Secret" may be delegated only in writing and only to principal subordinate officials determined by the President or by Agency heads listed in subsection (1) above to have a frequent need to exercise such authority. Authority so delegated may not be redelegated.

(ii) Authority for original classification of information as "Secret" may be delegated only in writing and only to those subordinates determined by the President, by Agency heads listed in subsections (1) and (2) above and by officials with "Top Secret" classification authority to have frequent need to exercise such authority. Authority so delegated may not be redelegated.

(iii) Authority for original classification of information as "Confidential" may be delegated only in writing and only to those subordinates determined by the President, by Agency heads listed in subsections (1), (2) and (3) above and by officials with "Top Secret" classification authority to have frequent need to exercise such authority. Authority so delegated may not be redelegated.

(iv) Each delegation of original classification authority shall be in writing by name or title of position held or as prescribed in directives implementing this Order.

(v) Delegations of original classification authority shall be held to an absolute minimum. Administrative convenience is not a valid basis for such delegations. Periodic review of such delegations shall be made to ensure that the officials so designated have demonstrated a continuing need to exercise such authority.

(vi) Agencies or officials not granted original classification authority in this section may request such authority from the President through the Information Security Oversight Office, established herein. Approval of such requests shall be published in the Federal Register.

(5) Exceptional Cases. When an employee of an Agency that does not have original classification authority, or a contractor of such an Agency, originates information that is believed to require classification, the person or contractor shall protect that information in the manner prescribed by this Order and implementing directives. The information shall be transmitted promptly through established channels and under appropriate safeguards to the Agency having primary interest in the subject matter and appropriate original classification authority with a request that a determination be made as to classification. Such requests shall be acted upon within 30 days. Where such Agency cannot be identified, the information shall be sent to the Director of the Information Security Oversight Office for a <sup>determination.</sup> a/...

(c) Classification Requirements. Information may not be classified unless an original classification authority determines:

- (1) that the information falls into one or more of the criteria set forth in subsection (d) below, which apply equally to all three authorized classification designations; and
- (2) that the unauthorized disclosure of such information reasonably could be expected to cause at least identifiable damage to the national security.

The 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.

(d) Classification Criteria. Information may not be considered for classification unless its disclosure reasonably could be expected to:

(1) Make the United States or its allies vulnerable to attack by a foreign power, or weaken the ability of the United States or its allies to conduct armed operations or defend themselves, or diminish the military or operational effectiveness of the United States' armed forces; or

(2) Lead to hostile political, economic, or military action against the United States or its allies by a foreign power; or

(3) Reveal, in whole or in part, the defense or foreign policy plans or posture of the United States or its allies; provide a foreign nation with information upon which to develop effective countermeasures to such plans or posture; weaken or nullify the effectiveness of a United States military, foreign policy, foreign intelligence, or foreign counterintelligence plan, operation, project, or activity; or

(4) Aid a foreign nation to develop or improve its military capability; or

(5) Reveal, jeopardize, or reduce the effectiveness of an intelligence or cryptologic source, method, device, or system; or

(6) Disclose to other nations or foreign groups that the United States has, or is capable of obtaining, certain information concerning those nations or groups without their knowledge or consent; or

(7) Deprive the United States of a diplomatic, military, scientific, engineering, technical, economic, or intelligence advantage related to the national security; or

(8) Create or increase international tensions; cause or contribute to political or economic instability or civil disorder in a foreign country; or otherwise impair the foreign relations of the



- (9) Disclose or impair the position of the United States or its allies in international negotiations; or
- (10) Disclose the identity of a confidential foreign source; or
- (11) Disclose foreign government information; or
- (12) Diminish the effectiveness of United States Government programs for safeguarding nuclear materials or facilities; or
- (13) Place a person's life in jeopardy.

(e) Limitation on Duration of Classification.

(1) Except as permitted in paragraph (2) below, each original classification authority at the time of original classification shall set a date or event for automatic declassification no more than six years later. Alternatively, the original classification authority may set a date or event not more than six years later for review to determine whether there is a continued need to protect the information. Only officials with Top Secret classification authority may extend classification of the information beyond six years and only then in accordance with paragraph (2) below.

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

(f) Classification Identification and Marking.

(1) The following shall be shown on the face of paper copies of all documents at the time of original classification: (i) the identity of the original classification authority; (ii) the office of origin; (iii) the date of the document's origin; (iv) the date or event for declassification or review; and (v) one of the three classification designations defined herein. When the individual who signs or otherwise authenticates a document or item also is authorized to classify it, no further annotation of identity is required. Documents classified for more than six years shall also be marked with the identity of the official who authorized the prolonged classification and the justification for it. This justification may be by reference to criteria set forth in agency implementing directives.

(2) Markings such as "For Official Use Only" and "Limited Official Use" may not be used to identify information requiring protection pursuant to this Order. Nor may terms such as "Conference," or "Agency" be used in conjunction with classification designations prescribed by this Order; e.g., "Agency Confidential," or "Conference Confidential."

(3) 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, in order to facilitate excerpting and other uses. Agency heads may seek a waiver of this requirement from the Director of the Information Security Oversight Office for specified classes of information. The Director of the Oversight Office may, for good cause, grant and revoke such a waiver.

(4) Foreign government information shall either retain its original classification designation or be assigned a United States classification designation that shall assure a degree of protection equivalent to that required by the entity that furnished the information.

(5) Classified documents that contain or reveal information that the originator has determined is subject to special dissemination and reproduction limitations shall be marked clearly so as to place the user on notice of the restrictions.

(g) Prohibitions.

(1) 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.

(2) Basic scientific research information not clearly related to the national security may not be classified.

(3) A product of non-government research and development that does not incorporate or reveal classified information to which

Approved For Release 2006/11/17 : CIA-RDP86-00674R000300040008-5  
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).

(4) References to classified documents that individually, or in aggregate, do not disclose classified information may not be classified or used as a basis for classification.

(5) 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.

(6) No document may be classified after an Agency has received a request for such document under the Freedom of Information Act or the Mandatory Review provision of this Order

Section 4(f) 7, unless such document requires the protection authorized by this Order and such classification is authorized personally, and in writing, by the head of the Agency concerned, by the senior official designated to oversee the Agency information security program, or by an agency official with original Top Secret classification authority.

(7) Classification may not be restored to documents already declassified and released to the public under this or prior Orders.

### Section 3. Derivative Classification of Information.

(a) Original classification authority shall not be given to persons who only reproduce, extract or summarize classified information or who only apply to information classification markings derived from source material or as directed by a security classification guide. Persons who apply derivative classification markings shall (i) respect classifications assigned by originators; (ii) to the maximum extent practicable verify the current level of classification of the information prior to applying such markings; (iii) in accordance with subsections (b) <sup>and (c)</sup> below, carry forward to any newly created documents the assigned dates or events for declassification or review and any additional authorized markings.

Documents based on multiple classified sources may use a single marking.

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

(c) New material that derives its classification from information classified under prior Orders shall be treated as follows:

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

(2) When the source material bears no date or event for declassification or is marked for declassification beyond twenty years, the new material shall be marked with a date for review for declassification <sup>at</sup> twenty years from the date of original classification of the source material.

(3) When the source material is foreign government information bearing no date or event for declassification or 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 4. Declassification and Downgrading

(a) Declassification Authority. The authority to declassify or downgrade information classified under this or prior Executive orders shall be exercised as follows:

(1) 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.

(2) Agency heads named in Section 2(b) shall designate additional officials at the lowest practicable echelons to exercise declassification and downgrading authority.

(3) When the Director of the Information Security Oversight Office determines that information is classified in violation of this Order, or that information considered in the exercise of the Director's appellate function pursuant to Section 4(f)(2) should be declassified or downgraded, the Director shall promptly notify the affected Agency of such a determination. The Agency shall have 20 working days to contest the determination. In the event agreement on the classification of the information in question cannot be reached between the Director of the Information Security Oversight Office and the Agency, they will appeal the case to the National Security Council. Contested information shall remain classified until the appeal is resolved.

(4) The provisions of this Order relating to the declassification of national security information 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 Executive orders.

(b) Authority Over Transferred Information.

(1) For classified information transferred in conjunction with a transfer of function -- not merely for storage purposes -- the receiving Agency shall be deemed to be the originating Agency for all purposes under this Order.

(2) For classified information not transferred in accordance with subsection (1) above, 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) Classified information transferred to the General Services Administration for accession into the Archives of the United States shall be declassified or downgraded by the Archivist of the United States in accordance with this Order, the directives of the Information Security Oversight Office, and Agency guidelines.

(4) After the termination of a Presidential administration, the Archivist of the United States shall have the authority to review and declassify or downgrade all information classified by the President, the White House staff, or committees or commissions appointed by the President or others acting on the President's behalf. This authority shall be exercised only after consultation with the agencies having primary subject matter interest. Disagreements on declassification of Presidential documents between the National Archives and agencies having primary subject matter interest may be appealed to the Director of the Information Security Oversight Office.

(c) Declassification Policy.

(1) 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 the occurrence of an event which would make continued classification unnecessary.

(2) Whenever information is reviewed for declassification pursuant to this Order, it shall be declassified unless the declassification authority established in Section 4(a) determines that the information continues to meet the standards for classification pre-

(3) It is presumed that information which continues to meet the standards for classification in Section 2(c) 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 a question arises, it shall be referred to the agency head, an official with Top Secret classification authority, or the Archivist of the United States in the case of material covered in Section 4(f)(2). That official will determine whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure.

(d) Declassification Requirements.

(1) Except as provided in Section 4(e)(4) below, information classified on or after the effective date of this Order shall be declassified or reviewed in accordance with the date or event set pursuant to Section 2(e).

(i) Information not marked with such a date or event shall be declassified automatically six years after the date of original classification, unless the head or deputy head of the agency extends its classification personally and in writing in accordance with Section 2(e)(2).

(ii) When information is marked for review <sup>Section 2</sup> within six years of original classification, pursuant to Section 2(e)(1), and that review is not conducted by the end of the sixth year, the information is automatically declassified. However, the head of the agency or officials with Top Secret classification authority may restore and extend the classification personally and in writing, in accordance with Section 2(e)(2). Ab

(2) Except as provided in Section 4(e)(4) below, information which was classified before the effective date of this Order and already marked with a date or event directing declassification in 20 years or less from date of origin, shall be declassified automatically in accordance with such date or event unless declassified earlier. Information not so marked shall be reviewed for declassification in accordance with Section 4(e) and (f) below.

(c) Systematic Review for Declassification.

(1) 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 20 years old. Agency heads listed in Section 2(b) and officials designated by the President pursuant to Section 2(b)(1) of this Order may extend classification beyond 20 years, but only in accordance with Sections 4(c) and 4(e)(2). This authority may not be delegated. When classification is extended beyond 20 years, a date for declassification or the next review no more than 10 years later shall be set and marked on the document. Subsequent reviews for declassification shall be set at no more than 10 year intervals. The Director of the Information Security Oversight Office may extend the period between subsequent reviews for specific categories of information.



the Agency heads listed in Section 2(b) 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 20-year old classified information under their jurisdiction. These guidelines shall state specific, limited categories of information which, because of their national security sensitivity, should not be declassified automatically but should be reviewed item-by-item to determine whether continued protection beyond 20 years is needed. 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 20 years from the date of original classification. These guidelines shall be authorized for use by the Archivist of the United States and by any Agency having custody of the information.

(3) Notwithstanding Section 4(e)(1) and (2), the Secretary of Defense may establish special procedures for systematic review and declassification of classified cryptologic information produced by units of the Department of Defense. These procedures shall be consistent, so far as practicable, with the objectives of Section 4(e)(1) and (2) and shall be reviewed and approved by the Director of the Information Security Oversight Office prior to implementation. Any decision by the Director in this regard may be appealed to the National Security Council. In case of an appeal, the information will remain classified until the appeal is resolved.

(4) Foreign government information shall be exempt from the automatic declassification and 20 year systematic review provisions of this Section. Unless declassified earlier, such information shall be reviewed for declassification 30 years from its date of origin. Such review shall be in accordance with the provisions of Section 4(c) 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.

(5) Transition to systematic review at twenty years shall be implemented as rapidly as practicable but shall be completed no more than ten years from the effective date of this Order.

(f) Mandatory Review for Declassification.

(1) Except as provided in (2) below, information classified pursuant to this or prior Executive orders shall be reviewed for possible declassification upon request of a member of the public, a government employee or an Agency, provided the request is sufficiently specific to permit location of the information with reasonable effort. Requests for declassification under this provision shall be acted upon within 60 days. Requests for declassification under the Freedom of Information Act shall be processed in accordance with the provisions of the Act.

(2) Information less than ten years old originated by the President or a President's White House staff or Committees or Commissions appointed by the President or 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 subsection (1) above. Such information over ten years old, however, shall be subject to mandatory declassification review upon the request of a member of the public, a government employee or an Agency. The processing of such requests shall accord with procedures developed by the Archivist of the United States which shall include consultations with agencies having primary subject matter interest. Denial by the Archivist of such a request for declassification may be appealed to the Director of the Information Security Oversight Office who may order declassification. In such cases, the Director of the Information Security Oversight Office shall promptly notify agencies with primary subject matter interest, which may follow the appeals process set forth in Section 4(a)(3).

(3) 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 subsection (1) above and for direct response to the requester. The Archivist shall inform requesters of such referrals.

(4) No Agency in possession of a document classified under the provisions of this or prior Orders may, in response to a request made under the Freedom of Information Act or the Mandatory Review provision of this Order (Section 4(f)) for such document, refuse to confirm the existence or non-existence of such document, unless the fact of its existence or non-existence would itself be classifiable under this Order.

(g) Downgrading. Information classified under this or prior Orders and marked for automatic downgrading is downgraded accordingly without notification to holders. Other information classified under this or prior Orders may be assigned a lower classification designation by the originator or other officials authorized to downgrade or to declassify when such downgrading serves a useful purpose. Notice of such downgrading shall be provided to holders of the information to the extent practicable.

#### Section 5. Safeguarding.

##### (a) General Restrictions on Access.

(1) No person may be given access to classified information unless such person has been determined to be trustworthy and unless access to such information is necessary for the performance of official duties.

(2) 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.

(3) Controls shall be established by each Agency to assure 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) 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 governing disposition of federal records.

(5) Classified information disseminated outside the executive branch shall be given protection equivalent to that afforded within the executive branch.

(b) Special Access Programs.

(1) Agency heads listed in Section 2(b)(1) may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this or prior Orders. Such programs may be created or continued only by written direction and only by these Agency heads or, 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 4. Special access programs may be created or continued only on a specific showing that:

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

(ii) 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

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

(2) All such special access programs except those required by treaty or international agreement shall terminate automatically every five years unless renewed in accordance with the procedures in this subsection.

(3) Within 180 days after the effective date of this Order, the Agency heads listed in Section 2(b)(1) shall review all existing special access programs under their jurisdiction and continue them only in accordance with the procedures in this subsection. Each of those Agency heads shall also establish and maintain a system of accounting for all special access programs they create or continue.

The Director of the Information Security Oversight Office shall have non-delegable access to all such accountings.

(c) Access by Historical Researchers and Former Presidential Appointees. The requirement in Section 5(a)(1) that access to classified information be granted only as is necessary for the performance of official duties shall not apply to persons who are engaged in historical research projects or who previously have occupied policy-making positions to which they were appointed by the President provided that the Agency with jurisdiction over the information:

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

(2) takes appropriate steps to ensure that classified information is not disclosed or published without prior review and declassification;

(3) takes reasonable action to ensure that access is limited to specific categories of information over which that Agency has classification jurisdiction;

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

(d) Reproduction Controls.

(1) Top Secret documents may not be reproduced without the consent of the originating Agency unless otherwise marked by the originating office.

(2) Reproduction of Secret and Confidential documents may be restricted by the originating Agency.

(3) Reproduced copies of classified documents are subject to the same accountability and controls as the original documents.

(4) 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; all documents covered by special access programs distributed outside the originating agency; and all Secret and Confidential documents marked in accordance with Section 2(f)(5).

(5) Subsections (1) and (2) above 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 6. Implementation and Review.

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.

(a) Information Security Oversight Office.

(1) The Administrator of General Services shall be responsible for implementing and monitoring the program established pursuant to this Order. This responsibility shall be performed through an Information Security Oversight Office.

(2) This Office shall have a full-time Director appointed by the Administrator of General Services subject to approval by the President. The Director shall have authority to appoint a staff. The Director shall:

(i) oversee Agency actions to ensure compliance with this Order and implementing directives;

(ii) 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 denials of declassification requests pursuant to Section 4(g)(2);

(iii) exercise the authority to declassify information provided by Sections 4(a)(3) and 4(f)(2);

(iv) 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;

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

(vi) review all Agency implementing regulations and guidelines for systematic review to ensure their consistency with the provisions of the Order and implementing directives. If the Director finds any regulation or guideline inconsistent with this Order or implementing directives, the Director may require it to be changed. The Agency head may appeal such a decision to the National Security Council, which shall have final decision-making authority. Pending resolution of the appeal, the Agency regulation or guideline shall remain in effect.

(vii) exercise case-by-case classification authority in accordance with Section 2(b)(5) and review requests for original classification authority in accordance with Section 2(b)(4)(vi);

(viii) 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 the above 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. In such a case, the Agency head shall report the decision and the reason to the National Security Council, which may overrule the decision.

(b) Interagency Information Security Committee. 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 Staff, the Domestic Policy Staff, and the Archivist of the United States. Representatives of other agencies may be invited to meet with the Committee on matters of particular interest to those agencies. 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.

(c) Agencies with Original Classification Authority. Each Agency granted original classification authority pursuant to this Order shall:

(1) Submit to the Information Security Oversight Office a copy of the regulations and guidelines for systematic review adopted pursuant to this Order and implementing directives. Subsequent changes to Agency regulations and guidelines for systematic review shall also be forwarded to the Oversight Office.

(2) Publish in the Federal Register the unclassified regulations implementing this Order or changes thereto.



(3) Designate a senior Agency official to conduct an active oversight program to ensure effective implementation of this Order.

(4) 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.

(5) Establish a process to decide appeals from denials of declassification requests, pursuant to Section 4(f).

(6) Establish and maintain a program to familiarize Agency personnel and others with access to classified information with the provisions of this Order and implementing directives; to impress upon each individual his or her responsibility for exercising vigilance and care in complying with the provisions of this Order; and, to encourage him or her to challenge classification decisions believed to be improper.

(7) Ensure the preparation and promulgation of guidelines for security classification that will facilitate the identification and uniform classification of information requiring protection under the provisions of this Order.

(8) Develop and promulgate guidelines for systematic review in accordance with Section 4(e)(2).

(9) Take necessary action to ensure that:

(i) a demonstrable need for access to classified information is established prior to the initiation of administrative clearance procedures, and

(ii) the number of people granted access to classified information is reduced to and maintained at the minimum, consistent with operational requirements and needs.

(10) Ensure that safeguarding practices are reviewed continuously and eliminate those that are duplicative or unnecessary.

(11) 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.

(d) Agencies Without Original Classification Authority.

Each Agency that has not been granted original classification authority but that handles classified information shall comply with appropriate subsections above 17(c)(1), (2), (3), (4), (5), (6), (8), (9), (10) and (11) 7.

Section 7. Administrative Sanctions.

In any case in which the Information Security Oversight Office finds that a violation of this Order or any implementing directive has occurred, it shall make a report to the head of the Agency concerned so that corrective steps may be taken.

(a) Officers and employees of the United States shall be subject to appropriate administrative sanctions if they:

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

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

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

(b) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, or other sanction in accordance with applicable law and Agency regulations.

(c) Agency heads shall make provision to ensure that appropriate and prompt corrective action is taken whenever a violation under subsection (a) occurs. They shall also inform the Director of the Information Security Oversight Office when such violations occur.

(d) Agency heads shall report to the Attorney General evidence of possible violations of federal criminal law by an employee of their department or agency to the extent any such information may be reflected in classified information and report to the Attorney General evidence of possible violations by any other person of those federal criminal laws specified in guidelines adopted by the Attorney General;

Section 8. Atomic Energy Information or Material.

Nothing in this Order shall supersede any requirements 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 such Atomic Energy Act and the regulations of the Department of Energy.

Section 9. Interpretation of the Order.

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.

Section 10. Revocation of Prior Orders and Directives.

Executive Order No. 11652 of March 8, 1972, as amended by Executive Order No. 11714 of April 24, 1973, and No. 11862 of June 11, 1975, and the National Security Council Directive of May 17, 1972 [3 C.F.R. 1085 (1971-75 Comp.)7] are revoked.

Section 11. Effective Date.

This Order shall become effective on October 1, 1978, except that the functions of the Information Security Oversight office specified in Section 6(a)(1)(iv) and 6(a)(1)(vi) shall be effective immediately and shall be performed in the interim by the Interagency Classification Review Committee established pursuant to Executive Order 11652.

Approved For Release 2006/11/17 : CIA-RDP86-00674R000300040008-5

**Page Denied**