

NATIONAL SECURITY COUNCIL

February 3, 1994

Paul Richards,

A new Draft Executive Order
on Classification for your review.

George TENET

Clinton Presidential Records Digital Records Marker

This is not a presidential record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

This marker identifies the place of a tabbed divider. Given our digitization capabilities, we are sometimes unable to adequately scan such dividers. The title from the original document is indicated below.

CLEAN VERSION

Divider Title: _____

Title 3 Executive Order of ...

The President Classified National Security Information

TABLE OF CONTENTS

Preamble	1
<i>Part 1. Original Classification</i>	
1.1 Definitions	2
1.2 Classification Standards	4
1.3 Classification Levels	5
1.4 Classification Authority	7
1.5 Classification Categories	9
1.6 Duration of Classification	10
1.7 Identification and Markings	12
1.8 Classification Prohibitions and Limitations	14
1.9 Classification Challenges	16
<i>Part 2. Derivative Classification</i>	
2.1 Definitions	17
2.2 Use of Derivative Classification	18
2.3 Classification Guides	19
<i>Part 3. Declassification and Downgrading</i>	
3.1 Definitions	20
3.2 Authority for Declassification	22
3.3 Transferred Information	23
3.4 Automatic Declassification	25
3.5 Systematic Declassification Review	27
3.6 Mandatory Declassification Review	29
3.7 Processing Requests	31
3.8 Declassification Database	32

Part 4. Safeguarding

4.1	Definitions	32
4.2	General Restrictions on Access	34
4.3	Distribution Controls	36
4.4	Special Access Programs	36
4.5	Access by Historical Researchers and Former Presidential Appointees	39

Part 5. Implementation and Review

5.1	Definitions	40
5.2	Policy Direction	41
5.3	Information Security Oversight Office	41
5.4	Interagency Security Classification Appeals Panel	43
5.5	Information Security Policy Advisory Council	45
5.6	General Responsibilities	47
5.7	Sanctions	49

Part 6. General Provisions

6.1	General Provisions	51
-----	------------------------------	----

Executive Order
Classified National Security Information

This Order prescribes a uniform system for classifying, safeguarding, and declassifying national security information.

Our democratic principles require that the American people be informed concerning the activities of their Government. Also, our nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national interest has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations. Protecting information critical to our nation's security remains a priority. In recent years, however, dramatic geopolitical changes have altered, although not eliminated, the national security threats that we confront. These changes provide a greater opportunity to emphasize our commitment to an open Government.

NOW, by the authority vested in me as President by the Constitution and laws of the United States of America, it is hereby ordered as follows:

Part 1

Original Classification

Section 1.1 Definitions.

As used in this Order, these terms are defined as follows:

(a) "National security" means the national defense or foreign relations of the United States.

(b) "Information" means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority and ability of the agency that originates information, or its successor in function, to regulate access to the information.

(c) "Classified national security information" (hereafter "classified information") means information that has been determined pursuant to this Order or any predecessor order to require protection against unauthorized disclosure.

(d) "Foreign government information" means:

(1) Information provided by a foreign government or governments, an international organization of governments, or any element thereof, with the expressed expectation that the information, the source of the information, or both, are to be held in confidence; or

(2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

(3) information received and treated as "Foreign Government Information" under the terms of a predecessor order.

(e) "Classification" means the act or process by which information is determined to be classified information.

(f) "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

(g) "Original classification authority" means an individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance.

(h) "Unauthorized disclosure" means a communication or physical transfer of classified information to an unauthorized recipient.

(i) "Agency" has the meaning provided at 5 U.S.C. § 552(f).

(j) "Senior agency official" means the official designated by the agency head under Section 5.6(a)(3) of this Order to direct and administer the agency's program under which national security information is classified, safeguarded and declassified.

Section 1.2 *Classification Standards*

(a) Information may be originally classified under the terms of this Order only if all of the following conditions are met:

- (1) An original classification authority classifies the information;
- (2) the information is owned by, produced by or for, or is under the control of the United States Government;
- (3) the information falls within one of the categories of information listed in Section 1.5 of this Order; and

(6) violate a statute, treaty, or international agreement.

(d) Information marked for an indefinite duration of classification under predecessor orders, ^{*[including but not limited to]*} for example, "Originating Agency's Determination Required," or information classified under predecessor orders that contains no declassification instructions shall be declassified in accordance with Part 3 of this Order.

Section 1.7 *Identification and Markings.*

(a) At the time of original classification, the following shall appear on the face of each classified document, or shall be applied to other classified media in an appropriate manner:

(1) One of the three classification levels defined in Section 1.3 of this Order;

(2) the identity, by name or personal identifier and position, of the original classification authority;

(3) the agency and office of origin, if not otherwise evident;

(4) declassification instructions, which shall indicate one of the following:

(4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and the original classifier is able to identify or describe the damage.

see p. 13
1.7 (a) (5)

(b) Information that meets the standards for classification shall be left unclassified if the original classification authority determines that the public interest in keeping the information unclassified outweighs the need for classification.

(c) If there is reasonable doubt about the need to classify information, it shall not be classified.

(d) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

Section 1.3 *Classification Levels.*

(a) Information may be classified at one of the following three levels:

(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 that the original classification authority is able to identify or describe.

(2) **Secret** shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) **Confidential** shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

(c) If there is reasonable doubt about the appropriate level of classification, it shall be classified at the lower level.

Section 1.4 *Classification Authority.*

(a) The authority to classify information originally may be exercised only by:

(1) The President;

(2) agency heads and officials designated by the President in the *Federal Register*; or

(3) United States Government officials delegated this authority pursuant to paragraph (c), below.

(b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

(c) *Delegation of Original Classification Authority.*

(1) Delegations of original classification authority shall be limited to the minimum required to administer this Order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) **Top Secret** original classification authority may be delegated only by the President; or an agency head or official designated pursuant to paragraph (a)(2), above.

(3) **Secret** or **Confidential** original classification authority may be delegated only by the President; an agency head or official designated pursuant to paragraph (a)(2), above; or the senior agency official, provided that official has been delegated **Top Secret** original classification authority by the agency head.

(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this Order. Each delegation shall identify the official by name or position title.

(d) Original classification authority may not be exercised by such authorities until they have received training in original classification as provided in this Order and its implementing directives.

(e) *Exceptional Cases.* When an employee, contractor, licensee, or grantee of an agency that does not have original classification authority originates information believed by that person 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 as provided under this Order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within thirty (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. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

Section 1.5 *Classification Categories.*

Information may be considered for classification only if its unauthorized disclosure reasonably could be expected to:

- (a) (1) impair the ability of the United States military to: (A) defend the nation from armed aggression; (B) engage in armed conflict;
or (C) participate in peacekeeping or multinational operations; or
 - (2) reveal or increase the vulnerability of the United States military, its personnel, installations, weapons technology, or related systems;
- (b) damage relations between the United States and another country or international organization of governments; impede diplomatic negotiations; impede the ability of the United States to engage in international economic policy; or reveal foreign government information;

- (c) reveal intelligence sources, methods and activities, including special activities or cryptologic activities;
- (d) impair United States Government programs for safeguarding nuclear materials or facilities;
- (e) damage the ability of the United States to relate or apply critical research or technology to the national defense or foreign relations of the United States; or
- (f) impair the ability of responsible United States Government officials to:
 - (1) protect the President, Vice President, and other authorized individuals; or
 - (2) maintain the continuity of the United States Government under emergency circumstances.

Section 1.6 *Duration of Classification.*

- (a) At the time of original classification, the original classification authority shall attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. The date or event shall not exceed the time frame in paragraph (b), below.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information originally classified under this Order shall be marked for automatic declassification **ten years** from the date of the original decision, except as provided in paragraph (c), below.

(c) At the time of original classification, the original classification authority may exempt from automatic declassification under paragraph (b), above, specific information, the release of which, even after the passage of ten years, could reasonably be expected to:

- (1) reveal an intelligence source, or an intelligence method that remains active;
- (2) reveal information that would clearly assist in the development or use of weapons of mass destruction;
- (3) reveal information that would clearly impair United States cryptologic systems or activities;
- (4) reveal information that would clearly impair the development or use of state of the art technology within a United States weapon system, intelligence gathering system, or counterintelligence system;
- (5) reveal foreign government information received by the United States with the clear expectation that the information would be protected for a period greater than ten years; or

(A) the date or event for declassification, as prescribed in Section 1.6(a);

(B) the date that is ten years from the date of original classification, as prescribed in Section 1.6(b); or

(C) the exemption from automatic declassification, as prescribed in Section 1.6(c); and

(5) a concise reason for classification, in accordance with instructions contained in the implementing directives issued by the Director of the Information Security Oversight Office.

(b) Specific information contained in paragraph (a), above, shall be excluded if it would unnecessarily reveal additional classified information.

(c) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are unclassified.

(d) Marking designations implementing the provisions of this Order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued by the Director of the Information Security Oversight Office.

(e) Foreign government information shall retain its original classification markings or shall be assigned a United States classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information.

(f) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.

(g) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document.

Section 1.8 *Classification Prohibitions and Limitations.*

(a) In no case shall information be classified in order to:

- (1) conceal violations of law, inefficiency, or administrative error;
- (2) prevent embarrassment to a person, organization, or agency;
- (3) restrain competition; or
- (4) prevent or delay the release of information that does not require protection in the interest of national security.

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

(c) Information may not be reclassified after it has been declassified and released to the public under proper authority.

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. § 552) or the Privacy Act of 1974 (5 U.S.C. § 552a), or the mandatory review provisions of Section 3.6 of this Order if such classification meets the requirements of this Order and is accomplished on a document-by-document basis under the personal participation or direction of the agency head, the deputy agency head, or the senior agency official.

(e) Compilations of items of information which are individually unclassified shall not be classified unless the compiled information reveals an additional association or relationship that:

- (1) Meets the standards for classification under this Order; and
- (2) is not otherwise revealed in the individual items of information.

As used in this Order, "compilation" means an arrangement of pre-existing unclassified items of information gathered together.

Section 1.9 *Classification Challenges.*

(a) Authorized holders of information who, in good faith, believe that its current status is improper, because it:

- (1) Should not be classified;
- (2) should be classified; or
- (3) should be classified at a different classification level;

shall challenge the classification status of the information in accordance with agency procedures established under paragraph (b), below.

(b) In accordance with implementing directives issued by the Director of the Information Security Oversight Office, an agency head or senior agency official shall establish procedures under which authorized holders of information shall challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall assure that:

- (1) individuals are not subject to retribution for bringing such actions;
- (2) an opportunity is provided for review by an impartial official or panel;
- and (3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel established by Section 5.4 of this Order.

Part 2

Derivative Classification

Section 2.1 Definitions.

As used in this Order, these terms are defined as follows:

(a) "Derivative classification" means the act of incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(b) "Derivative classification authority" means an individual designated in writing under Section 2.2(a) of this Order to classify information derivatively.

(c) "Classification guidance" means any instruction or source that prescribes the classification of specific information.

(d) "Classification guide" means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(e) "Source document" means an existing document which contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(f) "Multiple sources" means two or more sources which contain classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

Section 2.2 *Use of Derivative Classification.*

(a) An agency head or senior agency official shall identify those organizational units within an agency that may be required to classify information derivatively. A designated official of the United States Government shall authorize those organizational units within a contractor, licensee or grantee that may be required to classify information derivatively. The administrative head of each such unit shall designate at least one individual within that unit who shall be trained to serve as a derivative classification authority.

(b) A derivative classification authority will review and affirm each derivative classification action taken within the unit.

(c) Persons who apply derivative classification markings shall:

(1) Observe and respect original classification decisions; and
(2) carry forward to any newly created documents the pertinent classification markings, which shall be augmented by:

(A) The identity, by name or personal identifier and position, of the derivative classification authority; and

(B) for information derivatively classified based on multiple sources: (i) a date or event for declassification that corresponds to the longest period of classification among the sources; and (ii) on or attached to the official file or record copy, a listing of these sources.

Section 2.3 *Classification Guides.*

(a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this Order.

(b) Each guide shall be approved personally and in writing by an official who:

(1) Has program or supervisory responsibility over the information or is the senior agency official; and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agencies shall establish procedures to assure that classification guides are reviewed and updated as provided in directives issued under this Order.

Part 3

Declassification and Downgrading

Section 3.1 Definitions.

As used in this Order, these terms are defined as follows:

(a) "Declassification" means the authorized change in the status of information from classified information to unclassified information.

(b) "Automatic declassification" means the declassification of information based solely upon:

- (1) the occurrence of a specific date or event as determined by the original classification authority; or
- (2) the expiration of a maximum time frame for duration of classification established under this Order.

(c) "Declassification authority" means:

- (1) The official who authorized the original classification, if that official is still serving in the same position;
- (2) the originator's successor;
- (3) a supervisory official of either; or
- (4) officials delegated declassification authority in writing by the agency head or the senior agency official.

(d) "Mandatory declassification review" means the review for declassification of classified information in response to a request for declassification that meets the requirements under Section 3.6 of this Order.

(e) "Systematic declassification review" means the review for declassification of classified information contained in records that have been determined by the Archivist of the United States to have permanent historical value in accordance with chapter 33 of title 44, United States Code.

(f) "Declassification guide" means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

(g) "Downgrading" means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

Section 3.2 *Authority for Declassification.*

(a) Information shall be declassified or downgraded as soon as national security considerations permit. Agencies shall coordinate their review of classified information with other agencies that have a direct interest in the subject matter.

(b) If an agency head or senior agency official determines that the public interest in disclosure of specific information outweighs the national security interest in its continued classification, the information shall be declassified even though it continues to meet the standards for classification under this Order.

(c) 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 pending a prompt decision on the appeal.

(d) The provisions of this Section shall also apply to agencies that, under the terms of this Order, do not have original classification authority, but had such authority under predecessor orders.

Section 3.3 *Transferred Information.*

(a) 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.

(b) In the case of classified information that is not officially transferred as described in paragraph (a), above, but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information 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 that has an interest in the subject matter of the information.

(c) Classified information accessioned into the National Archives of the United States as of the effective date of this Order 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 declassification guides.

(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that records containing classified information be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to information being transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or information for which the

National Archives and Records Administration serves as the custodian of the records of an agency or organization that goes out of existence.

Section 3.4 *Automatic Declassification.*

(a) Information classified under this or any predecessor order shall be automatically declassified 25 years from the date of its creation. Within three years from the date of the issuance of this Order, all classified information more than 25 years old shall be automatically declassified, subject to paragraph (b), below.

(b) An agency head may exempt from automatic declassification under paragraph (a), above, specific information, the release of which should be expected to:

- (1) identify a confidential human intelligence source, or reveal information about the application of an intelligence source or method that remains active;
- (2) reveal information that would clearly assist in the development or use of weapons of mass destruction;
- (3) reveal information that would clearly impair United States cryptologic systems or activities;

(4) reveal information that would clearly impair the application of state of the art technology within a United States weapon system, intelligence gathering system, or counterintelligence system; or

(5) violate a statute, treaty, or international agreement.

(c) Any exemption as provided in paragraph (b), above, requires a written justification that identifies the specific information, explains why the information must remain classified for a longer period of time, and establishes a specific date or event for automatic declassification. The agency head or senior agency official shall provide the Director of the Information Security Oversight Office, serving as executive secretary of the Interagency Security Classification Appeals Panel, with a copy of such a justification at least 180 days before the information becomes subject to automatic declassification under paragraph (a), above. The Panel may direct the agency not to exempt the information or to designate the information for automatic declassification at an earlier date than recommended.

(d) Information exempted from automatic declassification under this Section shall remain subject to the mandatory and systematic declassification review provisions of this Order.

(e) The Secretary of State shall commence negotiations with the appropriate officials of a foreign government or international organization of

governments to modify any treaty or international agreement that requires the classification of information longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this Section.

Section 3.5 *Systematic Declassification Review.*

(a) Each agency that has originated classified information under this Order or its predecessors shall establish and conduct a program for systematic declassification review. This program shall apply to historically valuable records excepted from automatic declassification under Section 3.4 of this Order. Agencies shall prioritize the systematic review of records based upon:

(1) recommendations of the Information Security Policy Advisory Council, established in Section 5.5 of this Order, on specific subject areas for systematic review concentration; or

(2) the degree of researcher interest and the likelihood of declassification upon review.

(b) The Archivist of the United States shall conduct a systematic declassification review program for classified information: (1) accessioned into the National Archives of the United States as of the effective date of this Order; (2) information transferred to the Archivist pursuant to section 2203

of title 44, United States Code; and (3) information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that has gone out of existence. This program shall apply to pertinent records no later than 25 years from the date of their creation. The Archivist shall prioritize the systematic review of these records based upon the recommendations of the Information Security Policy Advisory Council; or the degree of researcher interest and the likelihood of declassification upon review. These records shall be reviewed in accordance with the standards of this Order, its implementing directives, and declassification guides provided to the Archivist by each agency that originated the records. The Director of the Information Security Oversight Office shall assure that agencies provide the Archivist with adequate and current declassification guides.

(c) After consultation with affected agencies, 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 or methods.

Section 3.6 *Mandatory Declassification Review.*

(a) Except as provided in paragraph (b), below, all information classified under this Order or predecessor orders shall be subject to a review for declassification by the originating agency if:

- (1) The request is made by a United States citizen or permanent resident alien, a federal agency, or a state or local government;
- (2) the request describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort; and
- (3) the information has not been reviewed for declassification within the past two years. If the agency has reviewed the information within the past two years, the agency shall inform the requester of this fact and of the requester's appeal rights.

(b) Information originated by a President, the White House Staff, by committees, commissions, or boards appointed by the President, or others specifically providing advice and counsel to a President or acting on behalf of a President is exempted from the provisions of paragraph (a), above. The Archivist of the United States shall have the authority to review, downgrade and declassify information under the control of the Archivist pursuant to sections 2107, 2111, 2111 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation

with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective presidential papers or records. Agencies with primary subject matter interest shall be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Interagency Security Classification Appeals Panel. The information shall remain classified pending a prompt decision on the appeal.

✓ NARA
Guidelines
to this is
previous EO?

(c) Agencies conducting a mandatory review for declassification shall declassify information no longer requiring protection under this Order. They shall release this information unless withholding is otherwise authorized and necessary under applicable law.

(d) In accordance with directives issued pursuant to this Order, agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They shall also provide a means for administratively appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency decision to the Interagency Security Classification Appeals Panel.

(e) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of 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. The Archivist shall develop special procedures for the review of information accessioned into the National Archives of the United States.

Section 3.7 *Processing Requests.*

In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this Order:

(a) 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 classified under this Order.

(b) When an agency receives any request for documents in its custody that were classified by another agency, it shall refer copies of the request and the requested documents to the originating agency for processing, and may, after consultation with the originating agency, inform the requester of the referral

unless such association is itself classified under this Order. In cases in which the originating agency determines in writing that a response under paragraph (a), above, is required, the referring agency shall respond to the requester in accordance with that paragraph.

Section 3.8 *Declassification Database.*

(a) The Archivist of the United States, in conjunction with the Director of the Information Security Oversight Office and those agencies that originate classified information, shall establish a Government-wide database of information that has been declassified. The Archivist shall also explore other possible uses of technology to facilitate the declassification process.

(b) Agency heads shall fully cooperate with the Archivist in these efforts.

Part 4

Safeguarding

Section 4.1 *Definitions.*

As used in this Order, these terms are defined as follows:

- (a) "Safeguarding" means protective measures and controls that are prescribed to secure classified information.
- (b) "Access" means the ability or opportunity to gain knowledge of classified information.
- (c) "Need-to-know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform a lawful and authorized function.
- (d) "Automated information system" means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.
- (e) "Integrity" means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.
- (f) "Network" means a system of two or more computers which can exchange data or information.
- (g) "Telecommunications" means the preparation, transmission, or communication of information by electronic means.

(h) "Special access program" means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Section 4.2 *General Restrictions on Access.*

(a) A person may have access to classified information provided that:

- (1) A determination of trustworthiness has been made by an agency head or the agency head's designee;
- (2) the person has signed an approved nondisclosure agreement; and
- (3) the person has a need-to-know the information.

(b) Classified information must remain in the custody or under the control of the originating agency or its successor in function. An official or employee leaving agency service may not remove classified information from the agency's control.

(c) Classified information may not be removed from official premises without proper authorization.

(d) Authorized dissemination of classified information outside the executive branch shall assure the protection of the information in a manner equivalent to that provided within the executive branch.

(e) Consistent with law, directives and regulation, an agency head or senior agency official shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, which collect, create, communicate, compute, disseminate, process, or store classified information have controls that:

- (1) Prevent access by unauthorized persons; and
- (2) ensure the integrity of the information.

(f) Consistent with law, directives and regulation, each agency head or senior agency official shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.,

(g) Except as provided by statute or 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. An agency head or senior agency official may waive this requirement for specific

information originated within that agency. For purposes of this Section, the Department of Defense shall be considered one agency.

Section 4.3 *Distribution Controls.*

(a) Each agency shall establish controls over the distribution of classified information to assure that it is distributed only to organizations or individuals eligible for access who also have a need-to-know the information.

(b) Each agency shall update, at least annually, the automatic, routine or recurring distribution of information that they classify. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

Section 4.4 *Special Access Programs.*

(a) *Establishment of special access programs.* Unless otherwise authorized by the President, only the Secretaries of State, Defense and Energy, and the Director of Central Intelligence, or the principal deputy of each, may create a special access program. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only upon a specific finding that:

(1) The vulnerability of, or threat to, specific information is exceptional; or

(2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure.

(b) Requirements and limitations.

(1) Special access programs shall be limited to programs in which the number of persons who will have access will be reasonably small and commensurate with the objective of providing extra protection for the information involved.

(2) Each agency head shall establish and maintain a system of accounting for special access programs consistent with directives promulgated by the Director of the Information Security Oversight Office.

(3) Special access programs shall be subject to the oversight program established under Section 5.6(a)(3) of this Order. In addition, the Director of the Information Security Oversight Office, or specific designees of the Director, shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this Order.

(4) The agency head or principal deputy shall review annually each special access program to determine whether it continues to meet the requirements of this Order.

(5) No special access program shall continue beyond five years from the date of its establishment except upon the unanimous approval of an interagency review panel composed of the Secretaries of State, Defense, and Energy, the Director of Central Intelligence, and the Attorney General, or the principal deputy of each. A special access program approved for continued operation shall be re-reviewed by the interagency review panel at five year intervals. An agency head may appeal the review panel's disapproval of a special access program to the President.

(c) Within 180 days after the effective date of this Order, each agency head or principal deputy shall review all existing special access programs under the agency's jurisdiction. These officials shall terminate any special access programs that do not clearly meet the provisions of this Order. Each existing special access program that an agency head or principal deputy revalidates shall be treated as if it were established on the effective date of this Order.

(d) Nothing in this Order shall supersede any requirement made by or under 10 U.S.C. § 119.

Section 4.5 *Access by Historical Researchers and Former Presidential Appointees.*

(a) The requirement in Section 4.2(a)(3) of this Order that access to classified information may be granted only to individuals who have a need-to-know the information may be waived for persons who:

- (1) Are engaged in historical research projects; or
- (2) previously have occupied policy-making positions to which they were appointed by the President.

(b) Waivers under this Section may be granted only if the agency head or senior agency official of the originating agency:

- (1) Determines in writing that access is consistent with the interest of national security;
- (2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this Order; and
- (3) limits the access granted to former presidential appointees to items that the person originated, reviewed, signed, or received while serving as a presidential appointee.

Part 5

Implementation and Review

Section 5.1 Definitions.

(a) "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this Order and its implementing directives.

(b) "Violation" means:

(1) Any knowing, willful or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;

(2) any knowing, willful or negligent action to classify or continue the classification of information contrary to the requirements of this Order or its implementing directives; or

(3) any knowing, willful or negligent action to create or continue a special access program contrary to the requirements of this Order.

(c) "Infraction" means any knowing, willful or negligent action contrary to the requirements of this Order or its implementing directives that does not comprise a "violation," as defined above.

Section 5.2 *Policy Direction.*

(a) The National Security Council shall provide overall policy direction for the program established under this Order.

(b) [Reserved]

Section 5.3 *Information Security Oversight Office.*

(a) [Reserved]

(b) The Director shall:

(1) 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;

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

(3) review agency implementing regulations and agency guides for systematic declassification review. The Director shall require any regulation or guide to be changed if inconsistent with this Order or its implementing

directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation or guide shall remain in effect pending a prompt decision on the appeal;

(4) have the authority to conduct on-site reviews of each agency's program established under this Order, and to require of each agency, those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the National Security Council within 60 days of the Director's request for access. Access shall be denied pending a prompt decision by the National Security Council;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend presidential approval;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this Order;

(7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this Order;

(8) report at least annually to the President through the National Security Council on the implementation of this Order; and

(9) have the authority to convene and chair interagency or other meetings to discuss matters pertaining to the program established under this Order.

(c) Directives issued by the Director of the Information Security Oversight Office shall establish uniform standards for:

- (1) Safeguarding classified information;
- (2) agency security education and training programs;
- (3) agency self-inspection programs; and
- (4) classification and declassification guides.

Section 5.4 *Interagency Security Classification Appeals Panel.*

(a) *Establishment and Administration.*

(1) There is established an Interagency Security Classification Appeals Panel ("Panel"). The Associate Attorney General shall serve as Chairman of the Panel. The Secretaries of State and Defense, the Director of Central Intelligence, the Archivist of the United States, and the Executive Secretary of the National Security Council shall each appoint a senior level representative to serve as a member of the Panel.

(2) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (1), above.

(3) The Director of the Information Security Oversight Office shall serve as the Executive Secretary. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.

(4) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel's functions.

(5) The Panel shall meet at the call of the Chairman. The Chairman shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.

(6) The Information Security Oversight Office shall include in its reports to the President a summary of the Panel's activities.

(b) *Functions.* The Panel shall:

(1) Take final administrative action on appeals by persons who have filed classification challenges under Section 1.9 of this Order;

(2) approve, deny or amend agency exemptions from automatic declassification as provided in Section 3.4 of this Order; and

(3) take final administrative action on appeals by persons or entities who have filed requests for mandatory declassification review under Section 3.6 of this Order.

(c) *Rules and Procedures.* The Panel shall issue by-laws, which shall be published in the *Federal Register* no later than 120 days from the effective date of this Order. The by-laws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that:

(1) The Panel will consider appeals only on actions in which the appellant has exhausted his or her administrative remedies within the responsible agency, and there is no current action pending on the issue within the federal courts and the information has not been the subject of review by the federal courts or the Panel within the past two years;

(2) the Panel will assure compliance with the safeguarding requirements established by this Order and its implementing directives;

(3) agency heads will cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner; and

(4) the Panel will report to the President through the National Security Council any instance in which it believes that an agency head is not cooperating fully with the Panel.

Section 5.5 *Information Security Policy Advisory Council.*

(a) *Establishment.* There is established an Information Security Policy Advisory Council ("Council"). The Council shall be comprised of seven members appointed by the President, from among interested persons who are

*historians,
librarians
etc.*

not otherwise employees of the Federal Government. The members shall elect the Council Chairman. The Council's by-laws shall establish standards for length of member service and rotation of the chair.

(b) *Functions.* The Council shall:

(1) Advise the President, the National Security Adviser, the Director of the Information Security Oversight Office, or such other officials as it deems appropriate, on policies established under this Order or its implementing directives, including recommended changes to those policies;

(2) recommend to agency heads specific subject areas for systematic declassification review; and

(3) serve as a forum to discuss policy issues in dispute.

(c) The Council shall meet at least once each calendar year, and as otherwise provided in its by-laws.

(d) *Administration.*

(1) Each Council member may be compensated at a rate of pay not to exceed the daily equivalent of the annual rate of basic pay in effect for grade GS-18 of the general schedule under section 5332 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Council.

(2) While away from their homes or regular place of business in the actual performance of the duties of the Council, members may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government service (5 U.S.C. 5703(b)).

(3) The staff of the Information Security Oversight Office shall provide operational and administrative support for the Council.

(4) Notwithstanding any other Executive order, the functions of the President under the Federal Advisory Committee Act, as amended, except that of reporting to the Congress, which are applicable to the Council, shall be performed by the Administrator of General Services in accordance with the guidelines and procedures established by the General Services Administration.

Section 5.6 *General Responsibilities.*

(a) Heads of agencies that originate or handle classified information shall:

(1) Demonstrate personal commitment and commit senior management to the successful implementation of the program established under this Order;

(2) commit necessary resources to the effective implementation of the program established under this Order;

(3) designate a senior agency official to direct and administer the program, whose responsibilities shall include:

(A) Overseeing the agency's program established under this Order, including any authorized special access programs;

(B) promulgating implementing regulations, which shall be published in the *Federal Register* to the extent that they affect members of the public;

(C) establishing and maintaining security education and training programs;

(D) establishing and maintaining an ongoing self-inspection program, which shall include the periodic review and assessment of the agency's classified product;

(E) establishing procedures to prevent unnecessary access to classified information, including procedures that: (i) require that a need for access to classified information is established before initiating administrative clearance procedures; and (ii) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs;

(F) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

(G) assuring that the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element or item to be

evaluated in the rating of: (i) Original and derivative classification authorities; (ii) security managers or security specialists; and (iii) all other personnel whose duties significantly involve the creation or handling of classified information; and

(H) accounting for the costs associated with the implementation of this Order, which shall be reported to the Director of the Information Security Oversight Office for publication.

(b) The Inspector General of each agency shall conduct periodic evaluations of the implementation and administration of the program established under this Order. Copies of each Inspector General's reports shall be provided to the agency head and the Director of the Information Security Oversight Office.

Section 5.7 *Sanctions.*

(a) If the Director of the Information Security Oversight Office finds that a violation of this Order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

- (1) Disclose to unauthorized persons information properly classified under this Order or predecessor orders;
- (2) classify or continue the classification of information in violation of this Order or any implementing directive;
- (3) create or continue a special access program contrary to the requirements of this Order; or
- (4) contravene any other provision of this Order or its implementing directives.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this Order.

(e) The agency head or senior agency official shall:

(1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b), above, occurs; and

(2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2) or (3), above, occurs.

Part 6

General Provisions

Section 6.1 *General Provisions.*

(a) Nothing in this Order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947. "Restricted Data" and "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 under that Act.

(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this Order with respect to any question arising in the course of its administration.

- (c) Nothing in this Order limits the protection afforded any information by other provisions of law.
- (d) Executive Order No. 12356 of April 6, 1982, is revoked as of the effective date of this Order.
- (e) This Order shall become effective 180 days from the date of its issuance.



Information Security Oversight Office
750 17th Street, NW., Suite 530
Washington, DC 20006



Date

DRAFT

MEMORANDUM FOR: The Honorable Anthony Lake
Assistant to the President
for National Security Affairs

THROUGH: The Honorable George Tenet
Special Assistant to the President and
Senior Adviser for Intelligence Programs

FROM: Steven Garfinkel
Director, Information Security Oversight Office

SUBJECT: Draft Executive Order to Replace E.O. 12356,
"National Security Information"

As chair of an interagency task force established by Presidential Review Directive 29 of April 26, 1993, and as Director of the Information Security Oversight Office, I am pleased to submit a draft of a proposed Executive Order to replace E.O. 12356, "National Security Information." The draft, dated January 1994, includes substantive changes, discussed between our staffs, from a previous draft dated November 10, 1993. The draft appears in both a clean version, and in legislative drafting style, which highlights its differences from the language of E.O. 12356.

I believe that the draft Order, if implemented and enforced, would result in achieving the objectives of the Presidential Review Directive, e. g., to reduce overclassification; to declassify enormous quantities of previously classified information; and to increase individual accountability while reducing the costs of the security classification system. The draft includes approximately 70 significant substantive changes from the current system. A number of major provisions have never before appeared in a security classification system. We highlight these new ideas in Attachment I.

Many of the ideas incorporated into this draft represent, in my view, reasonable compromise positions between those endorsed by some advocates of greater openness and some advocates of greater protection. Nonetheless, if experience is our guide, we should expect both public and internal criticism of a number of provisions. Attachment II briefly describes the more controversial provisions of the draft Order and the likely criticisms from advocates of greater openness and advocates of greater protection.

To facilitate your review, we also enclose a chart which compares salient provisions of the draft with the current system and its two immediate predecessors.

Attachments and enclosures

**ATTACHMENT I:
NEW PROVISIONS TO THE CLASSIFICATION SYSTEM
FEATURED IN DRAFT**

- Stresses openness and impact of geopolitical changes on classification policies.
- Balances public interest in disclosure with need for classification at both the time of classification and at the review for declassification.
- Limits the duration of classification to 10 years for much information.
- Requires declassification of almost all information at 25 years.
- Designates both original and derivative classification authorities and mandates training.
- Requires classifiers to identify why information is classified.
- Eliminates presumption that any category of information is automatically classified.
- Specifies sanctions for overclassification.
- Establishes a Government-wide declassification database.
- Establishes an interagency panel as the last appellate authority for classification challenges and mandatory review appeals.
- Establishes a council of non-Government representatives to recommend subject areas for systematic declassification review and to advise on classification system policies.
- Limits the establishment and continuation of special access programs and increases both internal and external oversight of them.
- Calls upon Inspectors General to conduct periodic evaluations of programs established under this Order.
- Requires accounting and reporting of security classification costs.
- Requires challenge of improper classification decisions and establishes processing procedures that ensure non-retribution.

- Ensures complete portion marking of classified documents.
- Prevents removal of classified information by departing Government officials.
- Requires renegotiation of most treaties or international agreements that extend classification beyond 25 years.
- Requires the annual update of any automatic, routine or recurring distribution lists of classified information.
- Emphasizes requirement to safeguard classified information in automated information systems.
- Requires personal commitment of agency heads and senior management to the effective implementation of the Order.
- Ties performance appraisals to effective implementation of the Order.

ATTACHMENT II -- ANTICIPATED CRITICISM

ISSUE: DURATION OF CLASSIFICATION

January 1994 Draft Language	Anticipated Criticism: Advocates of Greater Openness	Anticipated Criticism: Advocates of Greater Protection
- Requires classifiers to establish a date or event for declassification when possible. - Establishes a 10-year rule for classification of most information. - Exempts 6 narrow categories of information from 10-year rule. - Does not apply 10-year rule to information created under prior orders.	10 years exceeds general 6-yr. rule in Carter Order, 10-yr./8-yr./6-yr. rule in Nixon Order. - Exemption categories are too broad and open-ended. - Authorizes reclassification of undisclosed information following an access demand. - Does not apply short automatic time-frames to information classified under prior orders.	10 years is not long enough to protect most information adequately. - Far more exemption categories are necessary. (Many agencies will insist information that they create must be exempted.) - Automatic duration periods are arbitrary and capricious.

ISSUE: DECLASSIFICATION OF OLDER INFORMATION

January 1994 Draft Language	Anticipated Criticism: Advocates of Greater Openness	Anticipated Criticism: Advocates of Greater Protection
- Requires automatic declassification (without review) of most 25-yr. old information. - Establishes 5 very narrow categories of information exempted from automatic declassification at 25 years. - Requires agencies to systematically review for declassification historically valuable records exempted from automatic declassification.	- The maximum classification lifetime is too long, and exceeds the Carter Order. - The exemption categories are too broad and open-ended. - Systematic review is unrealistic, expensive and wasteful.	25 years is not long enough to protect some information adequately. - No information should be declassified without document-by-document review. - Far more exemption categories are necessary. (Many agencies will insist information that they create must be exempted.)

ATTACHMENT II -- ANTICIPATED CRITICISM

ISSUE: DECLASSIFICATION OF OLDER INFORMATION (CONT.)		
January 1994 Draft Language	Anticipated Criticism: Advocates of Greater Openness	Anticipated Criticism: Advocates of Greater Protection
- Requires mandatory review for declassification of information, no matter what its age, when the subject of an access demand. - Provides an interagency appeals mechanism for denials of mandatory declassification review requests. - Establishes a declassification database.		- Automatic declassification is arbitrary and capricious. - Systematic review is unrealistic, expensive and wasteful. - A declassification database is too expensive and risky.
ISSUE: BALANCING TEST		
January 1994 Draft Language	Anticipated Criticism: Advocates of Greater Openness	Anticipated Criticism: Advocates of Greater Protection
- Requires the non-classification of information when the public interest in disclosure outweighs the public interest in protection. - Requires the declassification of information when the public interest in disclosure outweighs the public interest in continued protection.	- Does not go far enough to mandate a balancing process - Original classifier unlikely to be objective.	- Balancing tests invite unnecessary litigation. - If included, the balancing test language should be fully discretionary. - Balancing test needlessly slows and makes the classification process more costly.

ATTACHMENT II -- ANTICIPATED CRITICISM

ISSUE: OVERSIGHT		
January 1994 Draft Language	Anticipated Criticism: Advocates of Greater Openness	Anticipated Criticism: Advocates of Greater Protection
• Maintains oversight duties assigned to the National Security Council, the Information Security Oversight Office (ISOO), and the senior agency officials. • Establishes a Council of non-Government representatives to recommend subject areas for declassification review and to advise on the Order's policies. • Establishes an Interagency Security Classification Appeals Panel as the final appellate authority for classification challenges and mandatory review appeals. • Calls for agency Inspectors General to conduct periodic evaluations of the program. • Requires accounting for and reporting of costs associated with the program.	• Reliance on so much internal oversight is ineffective • Legislation and Congressional oversight are needed. • The Appeals Panel should be comprised, at least in part, of non-Government individuals.	• Layered external and internal oversight is costly, unnecessary and runs contrary to the National Performance Review. • External panels lack expertise and infringe on the agency head's authority. • Accounting for costs is expensive and will result in inaccurate figures.

ATTACHMENT II -- ANTICIPATED CRITICISM

ISSUE: SPECIAL ACCESS PROGRAMS (SAPs)		
January 1994 Draft Language	Anticipated Criticism: Advocates of Greater Openness	Anticipated Criticism: Advocates of Greater Protection
- Limits the number of agencies authorized to establish SAPs. - Requires annual revalidation by agency head or deputy agency head. - Requires revalidation by an interagency panel for SAPs to be continued beyond five years. - Increases significantly internal and external oversight of SAPs.	- SAPs (or acquisition SAPs) should be eliminated completely. - SAPs are used to hide the costs of classified programs. - SAPs are used to hide embarrassing or controversial programs	- Increased oversight is costly and unnecessary. - Highly sensitive programs are jeopardized by external limitations on the agencies.
ISSUE: FOREIGN GOVERNMENT INFORMATION (FGI)		
January 1994 Draft Language	Anticipated Criticism: Advocates of Greater Openness	Anticipated Criticism: Advocates of Greater Protection
- Defines FGI as information expressly received in confidence from a foreign government. - Requires renegotiation of treaties that extend classification of FGI beyond 25 years.	Definition doesn't extend to information treated as FGI under prior systems.	- Limits ability of U.S. officials to deal with foreign governments. - May limit the amount of information foreign governments are willing to share. - Restricts flexibility of the Secretary of State.

ATTACHMENT II -- ANTICIPATED CRITICISM

ISSUE: DESIGNATION OF DERIVATIVE CLASSIFIERS		
January 1994 Draft Language	Anticipated Criticism: Advocates of Greater Openness	Anticipated Criticism: Advocates of Greater Protection
- Requires designation of derivative classifiers. - Requires training before a derivative classifier can exercise his authority. - Requires that management of classified information by derivative classifiers be an element of annual performance evaluation. - Requires that the identity of the derivative classifier be shown on the face of a document	Designating derivative classifiers does not limit the number of people who can classify.	- Designation of derivative classifiers is an administrative burden. - Additional required training will be too costly.
ISSUE: PORTION MARKING		
January 1994 Draft Language	Anticipated Criticism: Advocates of Greater Openness	Anticipated Criticism: Advocates of Greater Protection
- Requires portion marking of each classified document. - Eliminates portion marking waivers.	Some may want markings for units smaller than paragraphs.	- Portion markings threaten release of properly classified information. - Portion marking is a burden, especially in crisis situations.

Clinton Presidential Records Digital Records Marker

This is not a presidential record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

This marker identifies the place of a tabbed divider. Given our digitization capabilities, we are sometimes unable to adequately scan such dividers. The title from the original document is indicated below.

COMPARISON CHART

Divider Title: _____

COMPARISON CHART

OF

JANUARY 1994 DRAFT EXECUTIVE ORDER

WITH

EXECUTIVE ORDER 12356 (CURRENT ORDER -- REAGAN ORDER),

EXECUTIVE ORDER 12065 (CARTER ORDER)

AND

EXECUTIVE ORDER 11652 (NIXON ORDER)

TABLE OF CONTENTS

<i>ISSUE</i>	<i>PAGE</i>
DURATION OF ORIGINAL CLASSIFICATION	1
DECLASSIFICATION OF OLDER INFORMATION	2
BALANCING TEST	3
OVERSIGHT	4
SPECIAL ACCESS PROGRAMS	5
TONE	6
FOREIGN GOVERNMENT INFORMATION	7
CLASSIFICATION STANDARDS	8
CLASSIFICATION LEVELS	9
DESIGNATION OF ORIGINAL CLASSIFIERS	10
DESIGNATION OF DERIVATIVE CLASSIFIERS	11
CLASSIFICATION CATEGORIES	12
PORTION MARKING	13
RECLASSIFICATION PROHIBITIONS	14
CHALLENGES TO CLASSIFICATION	15
CLASSIFICATION GUIDES	16
DECLASSIFICATION DATABASE	17
ACCOUNTING AND REPORTING OF SECURITY COSTS	18
SANCTIONS	19

ISSUE: DURATION OF CLASSIFICATION

January 1994 Draft	E.O. 12356 (Current Order--Reagan Order)
• Requires classifiers to establish a date or event for declassification when possible. • Establishes a 10 year rule for classification of most information. • Exempts 6 narrow categories of information from 10 year rule. • Does not apply 10 year rule to information created under prior orders.	• Requires classifiers to establish a date or event for declassification when possible. • Establishes indefinite duration of classification when a date or event cannot be determined.
E.O. 12065 (Carter Order)	E.O. 11652 (Nixon Order)
• Establishes a 6 year rule for classification of most information. • Allows Top Secret classification authorities to exempt any information from the 6 year rule.	• Establishes a general declassification schedule for duration based on classification level: <u>Top Secret</u> 10 years <u>Secret</u> 8 years <u>Confidential</u> 6 years • Allows classification authorities broad discretion to exempt information from general declassification schedule.

ISSUE: DECLASSIFICATION OF OLDER INFORMATION

January 1994 Draft

- Requires automatic declassification (without review) of most 25 year old information.
- Establishes 5 very narrow categories of information exempted from automatic declassification at 25 years.
- Requires agencies to systematically review for declassification historically valuable records exempted from automatic declassification.
- Requires mandatory review for declassification of information, no matter what its age, when it is the subject of an access demand.
- Provides an interagency appeal mechanism for denials of mandatory declassification review requests.

E.O. 12356 (Current Order--Reagan Order)

- Does not automatically declassify older information.
- Requires the National Archives to systematically review for declassification historically valuable records when 30 years old.
- Encourages other agencies to conduct systematic review programs.
- Requires mandatory review for declassification of information, no matter what its age, when it is the subject of an access demand.

E.O. 12065 (Carter Order)

- Requires agencies to systematically review for declassification historically valuable records that are 20 years old.
- Requires mandatory review for declassification of information, no matter what its age, when it is the subject of an access demand.

E.O. 11652 (Nixon Order)

- Requires agencies to systematically review for declassification historically valuable records that are 30 years old.
- Requires mandatory review for declassification of information, no matter what its age, when it is the subject of an access demand.
- Requires automatic declassification of 30 year old information classified under this Order with broad discretion by agency heads to continue classification.

ISSUE: BALANCING TEST

January 1994 Draft	E.O. 12356 (Current Order--Reagan Order)
• Prohibits the classification of information when the public interest in disclosure outweighs the public interest in protection. • Requires the declassification of information when the public interest in disclosure outweighs the public interest in continued protection.	• Does not address balancing of interests.
E.O. 12065 (Carter Order)	E.O. 11652 (Nixon Order)
• Requires the declassification of information when the public interest in disclosure outweighs the public interest in continued protection.	• Does not address balancing of interests.

ISSUE: OVERSIGHT

January 1994 Draft	E.O. 12356 (Current Order--Reagan Order)
• Maintains oversight duties assigned to the National Security Council (NSC), the Information Security Oversight Office (ISOO), and the senior agency officials. • Establishes a Council of non-Government representatives to recommend subject areas for declassification review and to advise on the Order's policies. • Establishes an Interagency Security Classification Appeals Panel as the final appellate authority for classification challenges and mandatory review appeals. • Calls for agency Inspectors General to conduct periodic evaluations of the program.	• Maintains the National Security Council (NSC), as the provider of overall policy direction for the program. • Maintains the Information Security Oversight Office to oversee the program on behalf of the NSC. • Maintains the oversight duties assigned to the senior agency official.
E.O. 12065 (Carter Order)	E.O. 11652 (Nixon Order)
• Designates the National Security Council (NSC) as the provider of overall policy direction for the program. • Establishes the Information Security Oversight Office (ISOO) to oversee the program on behalf of the NSC. • Requires a senior agency official to conduct oversight duties. • Establishes an Interagency Security Committee, chaired by ISOO, to advise on implementation of the Order.	• Establishes an Interagency Classification Review Committee to assist the National Security Council in monitoring implementation of the Order. • Requires agency heads to designate senior agency officials to oversee the implementation of the program.

ISSUE: SPECIAL ACCESS PROGRAMS (SAPs)

January 1994 Draft	E.O. 12356 (Current Order--Reagan Order)
• Limits the number of agencies authorized to establish SAPs. • Requires annual revalidation by agency head or deputy agency head. • Requires revalidation by an interagency panel for SAPs to be continued beyond 5 years. • Increases significantly internal and external oversight of SAPs.	• Gives agencies broad authority to create and maintain SAPs. • Provides minimal external monitorship of SAPs.
E.O. 12065 (Carter Order)	E.O. 11652 (Nixon Order)
• Specifies intra-agency mechanisms to limit proliferation of SAPs. • Provides minimal external monitorship of SAPs.	• Makes no explicit reference to SAPs.

ISSUE: TONE

January 1994 Draft

- Makes a commitment to open Government in the preamble and provides enforcement mechanisms throughout.

E.O. 12356 (Current Order--Reagan Order)

- Emphasizes in the preamble and throughout the need to protect classified information.

E.O. 12065 (Carter Order)

- Makes a commitment to open Government in the preamble and in some of the sections, but does not provide enforcement mechanisms.

E.O. 11652 (Nixon Order)

- Makes a commitment to open Government in the preamble and in some of the sections, but does not provide enforcement mechanisms.

ISSUE: FOREIGN GOVERNMENT INFORMATION (FGI)

January 1994 Draft

- Defines FGI as information expressly received in confidence from a foreign government.
- Requires renegotiation of treaties that extend classification of FGI beyond 25 years.

E.O. 12356 (Current Order--Reagan Order)

- Defines FGI as information expressly or impliedly received in confidence from a foreign government.

E.O. 12065 (Carter Order)

- Defines FGI as information received in confidence from a foreign government.

E.O. 11652 (Nixon Order)

- Defines FGI as information received by the United States from a foreign government with the understanding that it be kept in confidence.

ISSUE: CLASSIFICATION STANDARDS

January 1994 Draft

- Requires classifiers to identify or describe the damage to the national security.
- Specifies that no category of information warrants presumptive classification.
- Provides that instances of doubt be resolved in favor of non-classification.

E.O. 12356 (Current Order--Reagan Order)

- Does not require classifiers to identify or describe the damage to the national security.
- Provides several categories of information requiring presumptive classification.
- Requires that instances of doubt be referred to higher authority for review.

E.O. 12065 (Carter Order)

- Introduces "identifiable damage" as the threshold for classification.
- Provides that instances of doubt be resolved in favor of non-classification.
- Provides several categories of information requiring presumptive classification.

E.O. 11652 (Nixon Order)

- No comparable provisions.

ISSUE: CLASSIFICATION LEVELS

January 1994 Draft

- Establishes 3 classification levels:

Top Secret - unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security that the classifier is able to identify or describe.

Secret - . . . serious damage to the national security that the classifier is able to identify or describe.

Confidential - . . . damage to the national security that the classifier is able to identify or describe.

E.O. 12356 (Current Order--Reagan Order)

- Establishes 3 classification levels:

Top Secret - unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.

Secret - . . . serious damage to the national security.

Confidential - . . . damage to the national security.

E.O. 12065 (Carter Order)

- Establishes 3 classification levels:

Top Secret - unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.

Secret - . . . serious damage to the national security.

Confidential - . . . *identifiable* damage to the national security.

E.O. 11652 (Nixon Order)

- Establishes 3 classification levels:

Top Secret - unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.

Secret - . . . serious damage to the national security.

Confidential - . . . damage to the national security.

ISSUE: DESIGNATION OF ORIGINAL CLASSIFIERS

January 1994 Draft	E.O. 12356 (Current Order--Reagan Order)
• Limits the authority to delegate original classification authority. • Training is required before an original classifier can exercise his authority. • Management of classified information by an original classifier to be an element of annual performance evaluation.	• Limits the authority to delegate original classification authority. • No training is required before an original classifier can exercise his authority. • No performance accountability for management of classified information by original classifiers.
E.O. 12065 (Carter Order)	E.O. 11652 (Nixon Order)
• Limits the authority to delegate original classification authority. • No training is required before an original classifier can exercise his authority. • No performance accountability for management of classified information by original classifiers.	• Limits the authority to delegate original classification authority. • No training is required before an original classifier can exercise his authority. • No performance accountability for management of classified information by original classifiers.

ISSUE: DESIGNATION OF DERIVATIVE CLASSIFIERS

January 1994 Draft	E.O. 12356 (Current Order--Reagan Order)
• Requires designation of derivative classifiers. • Requires training before a derivative classifier can exercise his authority. • Requires that management of classified information by derivative classifiers be an element of annual performance evaluation. • Requires that the identity of the derivative classifier be shown on the face of a document.	• Does not require designation of derivative classifiers. • Does not require training of derivative classifiers before they can exercise their authority. • Does not require performance accountability for management of classified information by derivative classifiers. • Does not require that the identity of the derivative classifier be shown on the face of a document.
E.O. 12065 (Carter Order)	E.O. 11652 (Nixon Order)
• Does not require designation of derivative classifiers. • Does not require training before derivative classifiers can exercise their authority. • Does not require performance accountability for management of classified information by derivative classifiers. • Does not require that the identity of the derivative classifier be shown on the face of a document.	• Does not require designation of derivative classifiers. • Does not require training before derivative classifiers can exercise their authority. • Does not require performance accountability for management of classified information by derivative classifiers. • Does not require that the identity of the derivative classifier be shown on the face of a document.

ISSUE: CLASSIFICATION CATEGORIES

January 1994 Draft	E.O. 12356 (Current Order--Reagan Order)
• Provides 6 categories of information that may be classified, each with a narrower range of application than in prior orders. • Eliminates an all inclusive "other" category.	• Provides 10 categories of information that may be classified, each broad in scope. • Includes an "other" category for national security information requiring protection.
E.O. 12065 (Carter Order)	E.O. 11652 (Nixon Order)
• Provides 7 categories of information that may be classified, each broad in scope. • Includes an "other" category for national security information.	• Establishes no specific categories of information that may be classified.

ISSUE: PORTION MARKING

January 1994 Draft

- Requires portion marking of each classified document.
- Eliminates portion marking waivers.

E.O. 12356 (Current Order--Reagan Order)

- Requires portion marking of each classified document.
- Allows portion marking waivers by agency head without Information Security Oversight Office approval.

E.O. 12065 (Carter Order)

- Requires portion marking of each classified document.
- Allows portion marking waivers by agency head with the approval of the Information Security Oversight Office.

E.O. 11652 (Nixon Order)

- Suggests that classifiers portion mark documents when practicable.

ISSUE: RECLASSIFICATION PROHIBITIONS

January 1994 Draft

- Prohibits the reclassification of information after it has been declassified and released to the public under proper authority.

E.O. 12356 (Current Order--Reagan Order)

- Allows the reclassification of information previously declassified and disclosed under certain limited conditions.

E.O. 12065 (Carter Order)

- Prohibits the reclassification of information after it has been declassified and released to the public under proper authority.

E.O. 11652 (Nixon Order)

- Does not address nor necessarily prohibit reclassification actions.

ISSUE: CHALLENGES TO CLASSIFICATION

January 1994 Draft

- Requires authorized holders to challenge classification decisions that they believe to be improper.
- Directs agencies to establish procedures for processing challenges to classification.
- Ensures that challengers are not subject to retribution.

E.O. 12356 (Current Order--Reagan Order)

- Does not address challenges to classification.

E.O. 12065 (Carter Order)

- Encourages agency personnel to challenge classification decisions that they believe to be improper.
- Provides no mechanism for processing challenges or ensuring non-retribution.

E.O. 11652 (Nixon Order)

- Requires holders of classified information to inform originator of improper classification.
- Requires the originator to re-examine the classification.

ISSUE: CLASSIFICATION GUIDES

January 1994 Draft	E.O. 12356 (Current Order--Reagan Order)
• Requires agencies to prepare classification guides to facilitate derivative classification. • Requires uniform standards for classification guides. • Eliminates waivers from the requirement to produce classification guides.	• Requires agencies to prepare classification guides to facilitate derivative classification. • No standards required for classification guides. • Allows agency heads to waive the requirement to produce classification guides.
E.O. 12065 (Carter Order)	E.O. 11652 (Nixon Order)
• Requires, for the first time, classification guides to specifically identify the information to be classified.	• Does not address the issue of classification guides.

ISSUE: DECLASSIFICATION DATABASE

January 1994 Draft

- Establishes a Government-wide declassification database.

E.O. 12356 (Current Order--Reagan Order)

- Does not require a declassification database.

E.O. 12065 (Carter Order)

- Does not require a declassification database.

E.O. 11652 (Nixon Order)

- Does not require a declassification database.

ISSUE: ACCOUNTING AND REPORTING OF SECURITY COSTS

January 1994 Draft	E.O. 12356 (Current Order--Reagan Order)
Requires agencies to account for and report annually costs associated with the security classification program.	Does not require accounting for costs.
E.O. 12065 (Carter Order)	E.O. 11652 (Nixon Order)
Does not require accounting for costs.	Does not require accounting for costs.

ISSUE: SANCTIONS

January 1994 Draft	E.O. 12356 (Current Order--Reagan Order)
• Broadens sanctions to include: (1) the improper administration of special access programs; and (2) reckless disregard or pattern of error in applying the classification standards. • Specifies knowing, willful or negligent violations as deserving of sanctions.	• Does not address sanctions for improper administration of special access programs or a reckless disregard or pattern of error in applying classification standards. • Specifies knowing, willful or negligent violations as deserving of sanctions.
E.O. 12065 (Carter Order)	E.O. 11652 (Nixon Order)
• Does not address sanctions for improper administration of special access programs or a reckless disregard or pattern of error in applying classification standards. • Specifies knowing, willful or negligent violations as deserving of sanctions.	• Does not address sanctions for improper administration of special access programs or a reckless disregard or pattern of error in applying classification standards. • Establishes a general framework for administrative actions as a result of violating the Order.

Clinton Presidential Records Digital Records Marker

This is not a presidential record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

This marker identifies the place of a tabbed divider. Given our digitization capabilities, we are sometimes unable to adequately scan such dividers. The title from the original document is indicated below.

LEGISLATIVE VERSION

Divider Title: _____

Executive Order
Classified National Security Information

This Order prescribes a uniform system for classifying, safeguarding, and declassifying, ~~and safeguarding~~ national security information.

Our democratic principles require that the American people be informed concerning the activities of their Government. Also, our nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national interest has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations. Protecting information critical to our nation's security remains a priority. In recent years, however, dramatic geopolitical changes have altered, although not eliminated, the national security threats that we confront. These changes provide a greater opportunity to emphasize our commitment to an open Government.

~~It recognizes that it is essential that the public be informed concerning the activities of its Government, but that the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure.~~

DRAFT
January 1994

~~Information may not be classified under this Order unless its disclosure reasonably could be expected to cause damage to the national security.~~

NOW, by the authority vested in me as President by the Constitution and laws of the United States of America, it is hereby ordered as follows:

Part 1

Original Classification

Section 1.1 ~~Classification Levels~~ Definitions.

As used in this Order, these terms are defined as follows:

(a) "National security" means the national defense or foreign relations of the United States.

(b) "Information" means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority and ability of the agency that originates information, or its successor in function, to regulate access to the information.

(c) "Classified national security information" (hereafter "classified information") means information that has been determined pursuant to this Order or any predecessor order to require protection against unauthorized disclosure.

(d) "Foreign government information" means:

(1) Information provided by a foreign government or governments, an international organization of governments, or any element thereof, with the expressed expectation that the information, the source of the information, or both, are to be held in confidence; or

(2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

(3) information received and treated as "Foreign Government Information" under the terms of a predecessor order.

(e) "Classification" means the act or process by which information is determined to be classified information.

(f) "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

(g) "Original classification authority" means an individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance.

(h) "Unauthorized disclosure" means a communication or physical transfer of classified information to an unauthorized recipient.

(i) "Agency" has the meaning provided at 5 U.S.C. § 552(f).

(j) "Senior agency official" means the official designated by the agency head under Section 5.6(a)(3) of this Order to direct and administer the agency's program under which national security information is classified, safeguarded and declassified.

Section 1.2 Classification Standards.

(a) Information may be originally classified under the terms of this Order only if all of the following conditions are met:

- (1) An original classification authority classifies the information;
- (2) the information is owned by, produced by or for, or is under the control of the United States Government;
- (3) the information falls within one of the categories of information listed in Section 1.5 of this Order; and

(4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and the original classifier is able to identify or describe the damage.

(b) Information that meets the standards for classification shall be left unclassified if the original classification authority determines that the public interest in keeping the information unclassified outweighs the need for classification.

(c) If there is reasonable doubt about the need to classify information, it shall not be classified.

(d) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

Section 1.3 Classification Levels.

(a) National security information (hereinafter "classified information") may
shall be classified at one of the following three levels:

(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 that the original classification authority is able to identify or describe.

(2) **Secret** shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) **Confidential** shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

~~(c) If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by an original classification authority, who shall make this determination within thirty (30) days. If there is reasonable doubt about the appropriate level of classification, it shall be classified safeguarded at the lower higher level, of classification pending a determination by an original classification authority, who shall make this determination within thirty (30) days.~~

Section 1.42 *Classification Authority.*

(a) ~~Top Secret.~~ The authority to classify information originally as ~~Top Secret~~ may be exercised only by:

- (1) The President;
- (2) agency heads and officials designated by the President in the *Federal Register*; ~~and~~
- (3) United States Government officials delegated this authority pursuant to paragraph (c), below ~~Section 1.2(d).~~

~~(b) Secret.~~ The authority to classify information originally as ~~Secret~~ may be exercised only by:

- ~~(1) agency heads and officials designated by the President in the **Federal Register**;~~
- ~~(2) officials with original **Top Secret** classification authority; and~~
- ~~(3) officials delegated such authority pursuant to Section 1.2(d).~~

~~(c) Confidential.~~ The authority to classify information originally as ~~Confidential~~ may be exercised only by:

- ~~(1) agency heads and officials designated by the President in the **Federal Register**;~~

- ~~(2) officials with original **Top Secret** or **Secret** classification authority; and~~
~~(3) officials delegated such authority pursuant to Section 1.2(d).~~

(b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

~~(cd)~~ *Delegation of Original Classification Authority.*

(1) Delegations of original classification authority shall be limited to the minimum required to administer this Order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) ~~Original **Top Secret** original~~ classification authority may be delegated only by the President; or an agency head or official designated pursuant to paragraph (a)(2), above ~~Section 1.2(a)(2), and the senior official designated under Section 5.3(a)(1), provided that official has been delegated original **Top Secret** classification authority by the agency head.~~

(3) ~~Original **Secret** or **Confidential** original~~ classification authority may be delegated only by the President; an agency head or official designated pursuant to paragraph (a)(2), above; 1.2(a)(2) and 1.2(b)(1); an official with original **Top Secret** classification authority; or ~~and the senior agency official designated under Section 5.3(a)(1), provided that official has been delegated original **Top Secret** original~~ classification authority by the agency head.

~~(4) Original **Confidential** classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2); 1.2(b)(1) and 1.2(c)(1); an official with original **Top Secret** classification authority; and the senior official designated under Section 5.3(a)(1), provided that official has been delegated original classification authority by the agency head. (5) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this Order. It shall identify the official delegated the authority. Each delegation shall identify the official by name or position title. Delegated classification authority includes the authority to classify information at the level granted and lower levels of classification.~~

(d) Original classification authority may not be exercised by such authorities until they have received training in original classification as provided in this Order and its implementing directives.

(e) *Exceptional Cases.* When an employee, contractor, licensee, or grantee of an agency that does not have original classification authority originates information believed by that person 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 as provided under this Order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with

respect to this information. That agency shall decide within thirty (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. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

Section 1.53 *Classification Categories.*

~~(a)~~ Information ~~may~~shall be considered for classification only if its unauthorized disclosure reasonably could be expected to concern:

- (a) (1) impair the ability of the United States military to: (A) defend the nation from armed aggression; (B) engage in armed conflict; or (C) participate in peacekeeping or multinational operations; or
(2) reveal or increase the vulnerability of the United States military, its personnel, installations, weapons technology, or related systems;

(b) damage relations between the United States and another country or international organization of governments; impede diplomatic negotiations; impede the ability of the United States to engage in international economic policy; or reveal foreign government information;

(c) reveal intelligence sources, methods and activities, including special activities or cryptologic activities;

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

(e) damage the ability of the United States to relate or apply critical research or technology to the national defense or foreign relations of the United States; or

(f) impair the ability of responsible United States Government officials to:

(1) protect the President, Vice President, and other authorized individuals; or

(2) maintain the continuity of the United States Government under emergency circumstances.

~~(1) military plans, weapons, or operations;~~

~~(2) the vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;~~

~~(3) foreign government information;~~

~~(4) intelligence activities (including special activities), or intelligence sources or methods;~~

~~(5) foreign relations or foreign activities of the United States;~~

- ~~(6) scientific, technological, or economic matters relating to the national security;~~
 - ~~(7) United States Government programs for safeguarding nuclear materials or facilities;~~
 - ~~(8) cryptology;~~
 - ~~(9) a confidential source; or~~
 - ~~(10) other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President or by agency heads or other officials who have been delegated original classification authority by the President. Any determination made under this subsection shall be reported promptly to the Director of the Information Security Oversight Office.~~
- ~~(b) Information that is determined to concern one or more of the categories in Section 1.3(a) shall be classified when an original classification authority also determines that its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security.~~
- ~~(c) Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security.~~

~~(d) Information classified in accordance with Section 1.3 shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information.~~

Section 1.64 *Duration of Classification.*

(a) At the time of original classification, the original classification authority shall attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. The date or event shall not exceed the time frames in paragraph (b), below. ~~Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified.~~

(b) If the original classification authority cannot determine a specific date or event for declassification, information originally classified under this Order shall be marked for automatic declassification ten years from the date of the original decision, except as provided in paragraph (c), below.

(c) At the time of original classification, the original classification authority may exempt from automatic declassification under paragraph (b), above, specific information the release of which, even after the passage of ten years, could reasonably be expected to:

- (1) reveal an intelligence source, or an intelligence method that remains active;
- (2) reveal information that would clearly assist in the development or use of weapons of mass destruction;
- (3) reveal information that would clearly impair United States cryptologic systems or activities;
- (4) reveal information that would clearly impair the development or use of state of the art technology within a United States weapon system, intelligence gathering system, or counterintelligence system;
- (5) reveal foreign government information received by the United States with the clear expectation that the information would be protected for a period greater than ten years; or
- (6) violate a statute, treaty, or international agreement.

~~Automatic declassification determinations under predecessor orders shall remain valid unless the classification is extended by an authorized official of the originating agency. These extensions may be by individual documents or categories of information. The agency shall be responsible for notifying holders of the information of such extensions.~~

~~(d) Information classified under predecessor orders and marked for declassification review shall remain classified until reviewed for declassification under the provisions of this Order.~~

(d) Information marked for an indefinite duration of classification under predecessor orders, for example, "Originating Agency's Determination Required," or information classified under predecessor orders that contains no declassification instructions shall be declassified in accordance with Part 3 of this Order.

Section 1.75 *Identification and Markings.*

(a) At the time of original classification, the following ~~information~~ shall ~~appear~~~~be shown~~ on the face of ~~each~~~~all~~ classified documents, or ~~shall be applied to~~ clearly associated with other forms of classified ~~media~~~~information~~ in an ~~appropriate~~ manner; ~~appropriate to the medium involved, unless this information itself would reveal a confidential source or relationship not otherwise evident in the document or information:~~

(1) One of the three classification levels defined in Section ~~1.43~~ 1.43 of this Order;

(2) the identity, by name or personal identifier and position, of the original classification authority; ~~if other than the person whose name appears as the approving or signing official;~~

(3) the agency and office of origin, if not otherwise evident; ~~and~~

(4) declassification instructions, which shall indicate one of the following:

~~(4)(A)~~ the date or event for declassification as prescribed in Section 1.6(a); or the notation "Originating Agency's Determination Required."

(B) the date that is ten years from the date of original classification, as prescribed in Section 1.6(b); or

(C) the exemption from automatic declassification, as prescribed in Section 1.6(c); and

(5) a concise reason for classification, in accordance with instructions contained in the implementing directives issued by the Director of the Information Security Oversight Office.

(b) Specific information contained in paragraph (a), above, shall be excluded if it would unnecessarily reveal additional classified information.

~~(cb)~~ Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are unclassified not classified. ~~Agency heads may, for good~~

~~cause, grant and revoke waivers of this requirement for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.~~

(~~d~~e) Marking designations implementing the provisions of this Order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued by the Director of the Information Security Oversight Office.

(~~e~~d) Foreign government information shall ~~either retain its original classification markings or shall or~~ be assigned a United States classification that ~~shall ensure provides~~ a degree of protection at least equivalent to that required by the entity that furnished the information.

(~~f~~e) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. ~~Omitted markings may be inserted on a document by an official specified in Section 3.1(b).~~ Holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.

(g) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document.

Section 1.86 *Classification Prohibitions and Limitations*~~on Classification.~~

(a) In no case shall information be classified in order to:

- (1) conceal violations of law, inefficiency, or administrative error;
- (2) to prevent embarrassment to a person, organization, or agency;
- (3) to restrain competition; or
- (4) to prevent or delay the release of information that does not require protection in the interest of national security.

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

(c) Information may not be reclassified after it has been declassified and released to the public under proper authority. ~~The President or an agency head or official designated under Section 1.2(a)(2), 1.2(b)(1), or 1.2(c)(1) may reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of~~

~~national security; and (2) the information may reasonably be recovered. These reclassification actions shall be reported promptly to the Director of the Information Security Oversight Office.~~

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. § 552) or the Privacy Act of 1974 (5 U.S.C. § 552a), or the mandatory review provisions of this Section 3.6 of this Order (~~Section 3.4~~) if such classification meets the requirements of this Order and is accomplished ~~personally and~~ on a document-by-document basis under the personal participation or direction of by the agency head, the deputy agency head, or the senior agency official, ~~designated under Section 5.3(a)(1) or an official with original Top Secret classification authority.~~

(e) Compilations of items of information which are individually unclassified shall not be classified unless the compiled information reveals an additional association or relationship that:

- (1) Meets the standards for classification under this Order; and
- (2) is not otherwise revealed in the individual items of information.

As used in this Order, "compilation" means an arrangement of pre-existing unclassified items of information gathered together.

Section 1.9 Classification Challenges.

(a) Authorized holders of information who, in good faith, believe that its current status is improper, because it:

(1) Should not be classified;

(2) should be classified; or

(3) should be classified at a different classification level;

shall challenge the classification status of the information in accordance with agency procedures established under paragraph (b), below.

(b) In accordance with implementing directives issued by the Director of the Information Security Oversight Office, an agency head or senior agency official shall establish procedures under which authorized holders of information shall challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall assure that:
(1) individuals are not subject to retribution for bringing such actions; (2) an opportunity is provided for review by an impartial official or panel; and
(3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel established by Section 5.4 of this Order.

Part 2

Derivative Classification

Section 2.1 Definitions.

As used in this Order, these terms are defined as follows:

(a) "Derivative classification" means the act of incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(b) "Derivative classification authority" means an individual designated in writing under Section 2.2(a) of this Order to classify information derivatively.

(c) "Classification guidance" means any instruction or source that prescribes the classification of specific information.

(d) "Classification guide" means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(e) "Source document" means an existing document which contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(f) "Multiple sources" means two or more sources which contain classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

Section 2.21 *Use of Derivative Classification.*

(a) An agency head or senior agency official shall identify those organizational units within an agency that may be required to classify information derivatively. A designated official of the United States Government shall authorize those organizational units within a contractor, licensee or grantee that may be required to classify information derivatively. The administrative head of each such unit shall designate at least one individual within that unit who shall be trained to serve as a derivative classification authority. Derivative classification is (1) the determination

~~that information is in substance the same as information currently classified, and (2) the application of the same classification markings. 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.~~

(b) A derivative classification authority will review and affirm each derivative classification action taken within the unit.

~~(bc)~~ Persons who apply derivative classification markings shall:

(1) Observe and respect original classification decisions; and
(2) carry forward to any newly created documents ~~any assigned~~
~~authorized markings. The declassification date or event that provides the~~
~~longest period of classification shall be used for documents classified on the~~
~~basis of multiple sources.~~the pertinent classification markings, which shall
be augmented by:

(A) The identity, by name or personal identifier and position, of the derivative classification authority; and

(B) for information derivatively classified based on multiple sources: (i) a date or event for declassification that corresponds to the longest period of classification among the sources; and (ii) on or attached to the official file or record copy, a listing of these sources.

Section. 2.23 *Classification Guides.*

(a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this Order.

(b) Each guide shall be approved personally and in writing by an official who:

(1) Has program or supervisory responsibility over the information or is the senior agency official ~~designated under Section 5.3(a)(1); and~~

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agencies shall establish procedures to assure that classification guides are reviewed and updated as provided in directives issued under this Order.
~~Agency heads may, for good cause, grant and revoke waivers of the requirement to prepare~~

~~classification guides for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.~~

Part 3

Declassification and Downgrading

Section 3.1 Definitions.

As used in this Order, these terms are defined as follows:

(a) "Declassification" means the authorized change in the status of information from classified information to unclassified information.

(b) "Automatic declassification" means the declassification of information based solely upon:

(1) the occurrence of a specific date or event as determined by the original classification authority; or

(2) the expiration of a maximum time frame for duration of classification established under this Order.

(c) "Declassification authority" means:

- (1) The official who authorized the original classification, if that official is still serving in the same position;
- (2) the originator's successor;
- (3) a supervisory official of either; or
- (4) officials delegated declassification authority in writing by the agency head or the senior agency official.

(d) "Mandatory declassification review" means the review for declassification of classified information in response to a request for declassification that meets the requirements under Section 3.6 of this Order.

(e) "Systematic declassification review" means the review for declassification of classified information contained in records that have been determined by the Archivist of the United States to have permanent historical value in accordance with chapter 33 of title 44, United States Code.

(f) "Declassification guide" means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

(g) "Downgrading" means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

Section 3.2-1 Authority for Declassification Authority.

(a) Information shall be declassified or downgraded as soon as national security considerations permit. Agencies shall coordinate their review of classified information with other agencies that have a direct interest in the subject matter. ~~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.~~

(b) If an agency head or senior agency official determines that the public interest in disclosure of specific information outweighs the national security interest in its continued classification, the information shall be declassified even though it continues to meet the standards for classification under this Order. ~~Information shall be declassified or downgraded by the official who authorized the original classification, if that official is still serving in the same position; the originator's successor; a supervisory official of either; or officials delegated such authority in writing by the agency head or the senior agency official designated pursuant to Section 5.3(a)(1).~~

(c) 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 pending a prompt decision on the appeal.

(d) The provisions of this Section shall also apply to agencies that, under the terms of this Order, do not have original classification authority, but ~~that~~ had such authority under predecessor orders.

Section 3.32 *Transferred Information.*

(a) 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.

(b) In the case of classified information that is not officially transferred as described in paragraph Section 3.2(a), above, but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information 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 that has an interest in the subject matter of the information.

(c) Classified information accessioned into the National Archives of the United States as of the effective date of this Order 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 declassification guidelines.

(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that records containing classified information be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to information being transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that goes out of existence.

Section 3.4 Automatic Declassification.

(a) Information classified under this or any predecessor order shall be automatically declassified 25 years from the date of its creation. Within three years from the date of the issuance of this Order, all classified information more than 25 years old shall be automatically declassified, subject to paragraph (b), below.

(b) An agency head may exempt from automatic declassification under paragraph (a), above, specific information, the release of which should be expected to:

(1) identify a confidential human intelligence source, or reveal information about the application of an intelligence source or method that remains active;

(2) reveal information that would clearly assist in the development or use of weapons of mass destruction;

(3) reveal information that would clearly impair United States cryptologic systems or activities;

(4) reveal information that would clearly impair the application of state of the art technology within a United States weapon system, intelligence gathering system, or counterintelligence system; or

(5) violate a statute, treaty, or international agreement.

(c) Any exemption as provided in paragraph (b), above, requires a written justification that identifies the specific information, explains why the information must remain classified for a longer period of time, and establishes a specific date or event for automatic declassification. The agency head or senior agency official shall provide the Director of the Information Security Oversight Office, serving as executive secretary of the Interagency Security Classification Appeals Panel, with a copy of such a justification at least 180 days before the information becomes subject to automatic declassification under paragraph (a), above. The Panel may direct the agency not to exempt the information or to designate the information for automatic declassification at an earlier date than recommended.

(d) Information exempted from automatic declassification under this Section shall remain subject to the mandatory and systematic declassification review provisions of this Order.

(e) The Secretary of State shall commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this Section.

Section 3.53 *Systematic Declassification Review for Declassification.*

(a) Each agency that has originated classified information under this Order or its predecessors shall establish and conduct a program for systematic declassification review. This program shall apply to historically valuable records excepted from automatic declassification under Section 3.4 of this Order. Agencies shall prioritize the systematic review of records based upon:

(1) recommendations of the Information Security Policy Advisory Council, established in Section 5.5 of this Order, on specific subject areas for systematic review concentration; or

(2) the degree of researcher interest and the likelihood of declassification upon review.

~~—The Archivist of the United States shall, in accordance with procedures and timeframes prescribed in the Information Security Oversight Office's directives implementing this Order, systematically review for declassification or downgrading (1) classified records accessioned into the National Archives of the United States, and (2) classified presidential papers or records under the Archivists control. Such information shall be reviewed by the Archivist for declassification or downgrading in accordance with systematic review guidelines that shall be provided by the head of the agency that originated~~

~~the information, or in the case of foreign government information, by the Director of the Information Security Oversight Office in consultation with interested agency heads.~~

(b) The Archivist of the United States shall conduct a systematic declassification review program for classified information: (1) accessioned into the National Archives of the United States as of the effective date of this Order; (2) information transferred to the Archivist pursuant to section 2203 of title 44, United States Code; and (3) information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that has gone out of existence. This program shall apply to pertinent records no later than 25 years from the date of their creation. The Archivist shall prioritize the systematic review of these records based upon the recommendations of the Information Security Policy Advisory Council; or the degree of researcher interest and the likelihood of declassification upon review. These records shall be reviewed in accordance with the standards of this Order, its implementing directives, and declassification guides provided to the Archivist by each agency that originated the records. The Director of the Information Security Oversight Office shall assure that agencies provide the Archivist with adequate and current declassification guides. Agency heads may conduct internal

~~systematic review programs for classified information originated by their agencies contained in records determined by the Archivist to be premanently valuable but that have not been accessioned into the National Archives of the United States.~~

(c) After consultation with affected agencies, 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 or methods.

Section 3.64 *Mandatory Declassification Review for ~~Declassification~~.*

(a) Except as provided in paragraph Section 3.4(b), below, all information classified under this Order or predecessor orders shall be subject to a review for declassification by the originating agency; if:

(1) ~~T~~the request is made by a United States citizen or permanent resident alien, a federal agency, or a state or local government; ~~and~~

(2) the request describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort; and ~~and~~.

(3) the information has not been reviewed for declassification within the past two years. If the agency has reviewed the information within the past two years, the agency shall inform the requester of this fact and of the requester's appeal rights.

(b) Information originated by a President, the White House Staff, by committees, commissions, or boards appointed by the President, or others specifically providing advice and counsel to a President or acting on behalf of a President is exempted from the provisions of paragraph Section 3.4(a), above. The Archivist of the United States shall have the authority to review, downgrade and declassify information under the control of ~~the Administrator of General Services or the~~ Archivist pursuant to sections 2107, 2111, 2111 note, 2107 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective presidential papers or records. Agencies with primary subject matter interest shall be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Interagency Security Classification Appeals Panel~~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.~~ The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information no longer requiring protection under this Order. They shall release this information unless withholding is otherwise authorized and necessary under applicable law.

(d) In accordance with directives issued pursuant to this Order, Agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They shall also provide a means for administratively appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency decision to the Interagency Security Classification Appeals Panel.

(e) After consultation with affected agencies, ~~The~~ Secretary of Defense shall develop special procedures for the review of 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 consultation with affected agencies.~~ The Archivist shall develop special procedures for the review of information accessioned into the National Archives of the United States.

Section 3.7 Processing Requests.

~~(f)~~ In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this Order:

~~(a1)~~ 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 classified ~~able~~ under this Order.

~~(b2)~~ When an agency receives any request for documents in its custody that were classified by another agency, it shall refer copies of the request and the requested documents to the originating agency for processing, and may, after consultation with the originating agency, inform the requester of the referral unless such association is itself classified under this Order. In cases in which the originating agency determines in writing that a response under paragraphSection 3.4(a1), (1) above, is required, the referring agency shall respond to the requester in accordance with that paragraphSection.

Section 3.8 Declassification Database.

(a) The Archivist of the United States, in conjunction with the Director of the Information Security Oversight Office and those agencies that originate classified information, shall establish a Government-wide database of information that has been declassified. The Archivist shall also explore other possible uses of technology to facilitate the declassification process.

(b) Agency heads shall fully cooperate with the Archivist in these efforts.

Part 4

Safeguarding

Section 4.1 Definitions.

As used in this Order, these terms are defined as follows:

(a) "Safeguarding" means protective measures and controls that are prescribed to secure classified information.

(b) "Access" means the ability or opportunity to gain knowledge of classified information.

(c) "Need-to-know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform a lawful and authorized function.

(d) "Automated information system" means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

(e) "Integrity" means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

(f) "Network" means a system of two or more computers which can exchange data or information.

(g) "Telecommunications" means the preparation, transmission, or communication of information by electronic means.

(h) "Special access program" means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Section 4.21 *General Restrictions on Access.*

(a) A person may have~~is eligible for~~ access to classified information provided that:

(1) a~~A~~ determination of trustworthiness has been made by an agency heads or the agency head's designee~~a designated official and provided that such access is essential to the accomplishment of lawful and authorized Government purposes.~~

(2) the person has signed an approved nondisclosure agreement; and

(3) the person has a need-to-know the information.

(b) Classified information must remain in the custody or under the control of the originating agency or its successor in function. An official or employee leaving agency service may not remove classified information from the agency's control. 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.

(c) Classified information may not be removed from official premises without proper authorization.

(ed) Authorized dissemination of classified information outside the executive branch shall assure the protection of the information in a manner equivalent to that provided within the executive branch.~~Classified information shall not be disseminated outside the executive branch except under conditions that ensure that the information will be given protection equivalent to that afforded within the executive branch.~~

(e) Consistent with law, directives and regulation, an agency head or senior agency official shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, which collect, create, communicate, compute, disseminate, process, or store classified information have controls that:

- (1) Prevent access by unauthorized persons; and
- (2) ensure the integrity of the information.

(f) Consistent with law, directives and regulation, each agency head or senior agency official shall establish controls to ensure that classified

information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

(gd) Except as provided by statute or 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. An agency head or senior agency official may waive this requirement for specific information originated within that agency. For purposes of this Section, the Department of Defense shall be considered one agency.

Section 4.3 Distribution Controls.

(a) Each agency shall establish controls over the distribution of classified information to assure that it is distributed only to organizations or individuals eligible for access who also have a need-to-know the information.

(b) Each agency shall update, at least annually, the automatic, routine or recurring distribution of information that they classify. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

Section 4.42 *Special Access Programs.*

(a) Establishment of special access programs. Unless otherwise authorized by the President, only the Secretaries of State, Defense and Energy, and the Director of Central Intelligence, or the principal deputy of each, may create a special access program. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only upon a specific finding that:

(1) The vulnerability of, or threat to, specific information is exceptional; or

(2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure.~~(a) Agency heads designated pursuant to Section 1.2(a) may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this Order or predecessor orders. Such programs may be created or continued only at the written direction of these agency heads. For special access programs pertaining to intelligence activities (including special activities but not including military operational, strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence.~~

(b) Requirements and limitations.

(1) Special access programs shall be limited to programs in which the number of persons who will have access will be reasonably small and commensurate with the objective of providing extra protection for the information involved.

(2) Each agency head shall establish and maintain a system of accounting for special access programs consistent with directives promulgated by the Director of the Information Security Oversight Office.

(3) Special access programs shall be subject to the oversight program established under Section 5.6(a)(3) of this Order. In addition, the Director of the Information Security Oversight Office, or specific designees of the Director, shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this Order.

(4) The agency head or principal deputy shall review annually each special access program to determine whether it continues to meet the requirements of this Order.

(5) No special access program shall continue beyond five years from the date of its establishment except upon the unanimous approval of an interagency review panel composed of the Secretaries of State, Defense, and Energy, the Director of Central Intelligence, and the Attorney General, or the principal deputy of each. A special access program approved for continued operation shall be re-reviewed by the interagency review panel at five year

intervals. An agency head may appeal the review panel's disapproval of a special access program to the President ~~Each agency head shall establish and maintain a system of accounting for special access programs. The Director of the Information Security oversight Office, consistent with the provisions of Section 5.2(b)(4), shall have non-delegable access to all such accountings.~~

(c) Within 180 days after the effective date of this Order, each agency head or principal deputy shall review all existing special access programs under the agency's jurisdiction. These officials shall terminate any special access programs that do not clearly meet the provisions of this Order. Each existing special access program that an agency head or principal deputy revalidates shall be treated as if it were established on the effective date of this Order.

(d) Nothing in this Order shall supersede any requirement made by or under 10 U.S.C. § 119.

Section 4.53 *Access by Historical Researchers and Former Presidential Appointees.*

(a) The requirement in Section 4.21(a)(3) of this Order that access to classified information may be granted only to individuals who have a need-

~~to know the information as is essential to the accomplishment of authorized and lawful Government purposes~~ may be waived ~~as provided in Section 4.3(b)~~ for persons who:

- (1) Are engaged in historical research projects; or
- (2) previously have occupied policy-making positions to which they were appointed by the President.

(b) Waivers under this Section ~~4.3(a)~~ may be granted only if the ~~originating agency head or senior agency official of the originating agency~~:

- (1) Determines in writing that access is consistent with the interest of national security;
- (2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this Order; and
- (3) limits the access granted to former presidential appointees to items that the person originated, reviewed, signed, or received while serving as a presidential appointee.

Part 5

Implementation and Review

Section 5.1 Definitions.

(a) "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this Order and its implementing directives.

(b) "Violation" means:

(1) Any knowing, willful or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;

(2) any knowing, willful or negligent action to classify or continue the classification of information contrary to the requirements of this Order or its implementing directives; or

(3) any knowing, willful or negligent action to create or continue a special access program contrary to the requirements of this Order.

(c) "Infraction" means any knowing, willful or negligent action contrary to the requirements of this Order or its implementing directives that does not comprise a "violation," as defined above.

Section 5.21 *Policy Direction.*

(a) The National Security Council shall provide overall policy direction for the program established under this Order~~information security program.~~

(b) ~~[Reserved] The Administrator of General Services shall be responsible for implementing and monitoring the programs established pursuant to this Order. The Administrator shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.~~

Section 5.32 *Information Security Oversight Office.*

(a) ~~[Reserved] 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 Director shall have the authority to appoint a staff for the Office.~~

(b) The Director shall:

(1) 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;

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

(3) 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~~ inconsistent with this Order or its 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 pending a prompt decision on the appeal;

(4) have the authority to conduct on-site reviews of each agency's~~the~~ information security program established under this Order, ~~of each agency that generates or handles classified information~~ and to require of each agency, those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities. ~~If these reports, inspections, or granting~~ access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the National Security Council within 60 days of the Director's request for access~~official designated under Section 5.3(a)(1) may deny access. Access shall be denied pending a prompt decision by the National Security Council; The Director may appeal denials to the National Security Council. The denial of access shall remain in effect pending a prompt decision on the appeal.~~

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend presidential approval;

(6) 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 established under this Order;

(7) have the authority to prescribe, after consultation with affected agencies, ~~standard~~ standardization of forms or procedures that will promote the implementation of the ~~information security~~ program established under this Order;

(8) report at least annually to the President through the National Security Council on the implementation of this Order; and

(9) have the authority to convene and chair interagency or other meetings to discuss matters pertaining to the ~~security~~ program established under this Order.

(c) Directives issued by the Director of the Information Security Oversight Office shall establish uniform standards for:

(1) Safeguarding classified information;

(2) agency security education and training programs;

(3) agency self-inspection programs; and

(4) classification and declassification guides.

Section 5.4 Interagency Security Classification Appeals Panel.

(a) Establishment and Administration.

(1) There is established an Interagency Security Classification Appeals Panel ("Panel"). The Associate Attorney General shall serve as Chairman of the Panel. The Secretaries of State and Defense, the Director of Central Intelligence, the Archivist of the United States, and the Executive Secretary of the National Security Council shall each appoint a senior level representative to serve as a member of the Panel.

(2) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (1), above.

(3) The Director of the Information Security Oversight Office shall serve as the Executive Secretary. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.

(4) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel's functions.

(5) The Panel shall meet at the call of the Chairman. The Chairman shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.

(6) The Information Security Oversight Office shall include in its reports to the President a summary of the Panel's activities.

(b) Functions. The Panel shall:

(1) Take final administrative action on appeals by persons who have filed classification challenges under Section 1.9 of this Order;

(2) approve, deny or amend agency exemptions from automatic declassification as provided in Section 3.4 of this Order; and

(3) take final administrative action on appeals by persons or entities who have filed requests for mandatory declassification review under Section 3.6 of this Order.

(c) Rules and Procedures. The Panel shall issue by-laws, which shall be published in the *Federal Register* no later than 120 days from the effective date of this Order. The by-laws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that:

(1) The Panel will consider appeals only on actions in which the appellant has exhausted his or her administrative remedies within the responsible agency, and there is no current action pending on the issue within the federal courts and the information has not been the subject of review by the federal courts or the Panel within the past two years;

(2) the Panel will assure compliance with the safeguarding requirements established by this Order and its implementing directives;

(3) agency heads will cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner;

(4) the Panel will report to the President through the National Security Council any instance in which it believes that an agency head is not cooperating fully with the Panel.

Section. 5.5 Information Security Policy Advisory Council.

(a) Establishment. There is established an Information Security Policy Advisory Council ("Council"). The Council shall be comprised of seven members appointed by the President, from among interested persons who are not otherwise employees of the Federal Government. The members shall elect the Council Chairman. The Council's by-laws shall establish standards for length of member service and rotation of the chair.

(b) Functions. The Council shall:

(1) Advise the President, the National Security Adviser, the Director of the Information Security Oversight Office, or such other officials as it deems appropriate, on policies established under this Order or its implementing directives, including recommended changes to those policies;

(2) recommend to agency heads specific subject areas for systematic declassification review; and

(3) serve as a forum to discuss policy issues in dispute.

(c) The Council shall meet at least once each calendar year, and as otherwise provided in its by-laws.

(d) Administration.

(1) Each Council member may be compensated at a rate of pay not to exceed the daily equivalent of the annual rate of basic pay in effect for grade GS-18 of the general schedule under section 5332 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Council.

(2) While away from their homes or regular place of business in the actual performance of the duties of the Council, members may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government service (5 U.S.C. 5703(b)).

(3) The staff of the Information Security Oversight Office shall provide operational and administrative support for the Council.

(4) Notwithstanding any other Executive order, the functions of the President under the Federal Advisory Committee Act, as amended, except that of reporting to the Congress, which are applicable to the Council, shall

be performed by the Administrator of General Services in accordance with the guidelines and procedures established by the General Services Administration.

Section 5.63 *General Responsibilities.*

(a) Heads of Agencies that originate or handle classified information shall:

(1) Demonstrate personal commitment and commit senior management to the successful implementation of the program established under this Order;

(2) commit necessary resources to the effective implementation of the program established under this Order;

(3a) designate a senior agency official to direct and administer its information security the program, whose responsibilities which shall include an active oversight and security education program to ensure effective implementation of this Order;

(A) Overseeing the agency's program established under this Order, including any authorized special access programs;

(Bb) promulgateing implementing regulations, which. Any unclassified regulations that establish agency information security policy shall be published in the *Federal Register* to the extent that theyse regulations affect members of the public;

(C) establishing and maintaining security education and training programs;

(D) establishing and maintaining an ongoing self-inspection program, which shall include the periodic review and assessment of the agency's classified product;

(Ee) establishing procedures to prevent unnecessary access to classified information, including procedures that: (i) require that a demonstrable need for access to classified information is established before initiating administrative clearance procedures;; and (ii) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs; and

(Fd) developing special contingency plans for the safeguardingprotection of classified information used in or near hostile or potentially hostile areas;;

(G) assuring that the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of: (i) Original and derivative classification authorities; (ii) security managers or security specialists; and (iii) all other personnel whose duties significantly involve the creation or handling of classified information; and

(H) accounting for the costs associated with the implementation of this Order, which shall be reported to the Director of the Information Security Oversight Office for publication.

(b) The Inspector General of each agency shall conduct periodic evaluations of the implementation and administration of the program established under this Order. Copies of each Inspector General's reports shall be provided to the agency head and the Director of the Information Security Oversight Office.

Section 5.74 *Sanctions.*

(a) If the Director of the Information Security Oversight Office finds that a violation of this Order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior agency official designated under Section 6.3(a) so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, and grantees shall be subject to appropriate sanctions if they: ~~(1)~~ knowingly, willfully, or negligently:

(1) Disclose to unauthorized persons information properly classified under this Order or predecessor orders;

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

(3) create or continue a special access program contrary to the requirements of this Order; or

(4) ~~knowingly and willfully violate~~ contravene any other provision of this Order or its implementing directives.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this Order.

(ed) ~~The~~ Each agency head or the senior agency official designated under Section 5.3(a)(1) shall:

(1) ~~ensure that take~~ appropriate and prompt corrective action when is taken whenever a violation or infraction under paragraph b, above, Section 5.4(b) occurs; and:

~~(2) notify~~ ~~Either shall ensure that the Director of the Information Security Oversight Office is promptly notified whenever a violation under paragraph Section 5.4(b)(1), or (2) or (3), above, occurs.~~

Part 6

General Provisions

Section 6.1 *General Provisions* ~~Definitions.~~

~~(a) "Agency" has the meaning provided at 5 U.S.C. 552 (e).~~

~~(b) "Information" means any information or material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government.~~

~~(c) "National security information" means information that has been determined pursuant to this Order or any predecessor order to require protection against unauthorized disclosure and that is so designated.~~

~~(d) "Foreign government information" means:~~

~~(1) information provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or~~

~~(2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.~~

~~(e) "National security" means the national defense or foreign relations of the United States.~~

~~(f) "Confidential source" means any individual or organization that has provided, or that 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.~~

~~(g) "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.~~

~~Sec. 6.2 General:~~

~~(a) Nothing in this Order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947. "Restricted Data" and "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 under that Act.

(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this Order with respect to any question arising in the course of its administration.

(c) Nothing in this Order limits the protection afforded any information by other provisions of law.

(d) Executive Order No. ~~12356~~~~12065~~ of ~~April 6, 1982~~~~June 28, 1978~~, as amended, is revoked as of the effective date of this Order.

(e) This Order shall become effective 180 days from the date of its issuance~~on August 1, 1982~~.



Information Security Oversight Office
750 17th Street, NW., Suite 530
Washington, DC 20006



November 10, 1993

Dear Mr. Richard:

On behalf of the Information Security Oversight, thank you for your outstanding presentation and contribution to our symposium, "National Security Information: The Future of Declassification." Your opening remarks set the proper tone for the symposium. It was just what we needed to make the attendees aware of the new challenges confronting the Government's declassification system.

The entire symposium was extremely successful. We have received nothing but favorable comments about your speech. In fact, many of our guests are requesting copies of our transcript of it. More importantly, we appreciate you spending an entire day with us. Our guests valued the opportunity to discuss their perspectives with you.

Once again, please accept our sincerest appreciation for your outstanding contribution to our symposium.

Sincerely,

A handwritten signature in dark ink, reading "Steve Garfinkel".

Steven Garfinkel
Director

Mr. R. Paul Richard
Deputy Staff Secretary
Ground Floor, West Wing
The White House
Washington, DC 20500

