

PRD 29



TASK FORCE



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



July 30, 1993

MEMORANDUM FOR: The Honorable
John Podesta
Assistant to the President and Staff Secretary

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

Michael Waguespack
Director for Counterintelligence Programs
National Security Council

FROM: Steven Garfinkel *Steve Garfinkel*
Director, Information Security Oversight Office

SUBJECT: Presidential Review Directive 29:
Current Status

Progress on the drafting of a new Executive order on national security information is right on schedule. Based on a tremendous variety of inputs and sources, ISOO has completed a first draft, dated today. We are prepared to submit the draft to the interested agencies as soon as you give us the okay. We are very pleased to note that, in our opinion at least, the process is working. The draft makes many significant changes that greatly increase openness and accountability, while maintaining a viable and rational system for protecting critically sensitive information.

Please find enclosed:

- Tab 1: Highlights of the major changes.
- Tab 2: A listing of all the major changes, presented in the order that they appear in the draft.
- Tab 3: A clean copy of the July 30 draft.
- Tab 4: A copy of the July 30 draft in legislative drafting style, showing the changes from the current Order.

Enclosures



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.

1

Divider Title: _____

HIGHLIGHTS OF MAJOR CHANGES

- Sets a positive tone by stressing the Administration's commitment to the democratic principle of open government.

FOIA

- Emphasizes the opportunity for original classifiers to weigh the public interest in keeping information unclassified that otherwise meets the standards for classification.

FOIA

- Emphasizes the opportunity for a declassification authority to weigh the public interest by declassifying information that otherwise continues to meet the standards for classification.

- Requires heads of agencies to demonstrate personal and senior management commitment for the effective implementation of this program.

- Abolishes the indefinite duration of classification, or "Originating Agency's Determination Required" (OADR).

- Establishes a maximum life span for all national security protected information.

*

- Curbs excessive classification by reducing the number of classification categories from 10 to 5 and narrowing their range of application.

- Prohibits classification when there is a reasonable doubt about the need to classify.

- Eliminates the presumption that any category of information is automatically classified.

- Requires the prompt removal of classification authority from an individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of the Order.

*

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

- Reduces the levels of classification to two, **Top Secret** and **Secret**.

- Curbs excessive classification by requiring original classifiers to be able to identify or describe the damage to the national security that could result from the unauthorized disclosure of the information.
- Limits special access programs to meet narrow and specific criteria.
- Establishes an Information Security Policy Advisory Council consisting of Government and non-Government representatives.
- Requires agencies to account for all costs associated with the security classification program and to submit those costs to the Information Security Oversight Office for publication.
- ✕• Eliminates portion marking waivers.
 - Requires that derivative classification authorities be designated in writing and be trained and certified.
 - Eliminates waivers of the requirement to produce classification guides.
- ✕• Requires all originating agencies to establish a systematic declassification review program for all records that are 25 years old.

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.

2

Divider Title: _____

MAJOR CHANGES
CONTAINED IN JULY 30, 1993, DRAFT EXECUTIVE ORDER ON
NATIONAL SECURITY PROTECTED INFORMATION
(IN ORDER OF APPEARANCE IN THE DRAFT)

- Sets a positive tone by stressing the Administration's commitment to the democratic principle of open government. [Preamble]
- Acknowledges the need to balance the protection of critically sensitive information in the interest of the national security with that of promoting the flow of information essential for the nation's progress. [Preamble]
- Underscores the fact that dramatic geopolitical changes have altered the nature of security threats and that corresponding changes in classification policies are required. [Preamble]
- Promotes understanding of the Order by providing clear definitions of key terms at the beginning of each major section. [1.1; 2.1; 3.1; 4.1; and 5.1]
- Introduces a new term, "national security protected information," narrower in scope than the current "national security information." [1.1(c)]
- Promotes more reasoned classification decisions by grouping under one section the standards for original classification that are scattered throughout the current Order. [1.2(a)]
- Delineates clearly the conditions that original classifiers must meet in order to classify information in the first instance. [1.2(a)]
- Curbs excessive classification by requiring original classifiers to be able to identify or describe the damage to the national security that could result from the unauthorized disclosure of the information. [1.2(a)(4)]
- Emphasizes the opportunity for original classifiers to weigh the public interest in keeping information unclassified that otherwise meets the standards for classification. [1.2(b)]
- Prohibits classification when there is a reasonable doubt about the need to classify. [1.2(c)]
- Reduces the levels of classification to two, **Top Secret** and **Secret**. [1.3(a)]

- Requires original classifiers to classify information at the lower level when in doubt about the appropriate level of classification. [1.3(c)]
- Directs that information classified **Confidential** under predecessor orders be declassified no later than six years from the effective date of this Order. Continued classification requires a new original classification decision to upgrade such information to **Secret**. [1.3(d)]
- Specifies that an original classification authority may not exercise such authority until the individual is trained and certified as provided in the Order and its implementing directives. [1.4(d)]
- Curbs excessive classification by reducing the number of classification categories from 10 to 5, and narrowing their range of application. [1.5]
- Eliminates the presumption that any category of information is automatically classified.
- Abolishes the indefinite duration of classification, or "Originating Agency's Determination Required" (OADR).
- Eliminates portion marking waivers.
- Establishes a timetable for automatic declassification when original classifiers cannot determine a date or event for declassification. [1.6 (b), (c) and (d)]
- Encourages automatic declassification by restricting extensions of the duration of classification. [1.6(e)]
- Requires that the name or personal identifier of the original classification authority be included as one of the essential classification markings. [1.7(a)(2)]
- Requires that a concise reason for classification be included as one of the essential classification markings. [1.7(a)(5)]
- Instructs original classifiers to consider the use of a classified addendum when national security protected information constitutes a small portion of an otherwise unclassified document. [1.7(g)]
- Prohibits the reclassification of information after it has been declassified and released to the public under proper authority. [1.8(c)]

- Restricts the use of classification by compilation and delineates clearly the conditions that must be met for such classifications. [1.8(e)]
- Requires individuals to challenge classification decisions that they believe to be improper. [1.9(a)]
- Directs agencies to establish procedures for processing challenges to classification and ensuring that challengers are not subject to retribution. [1.9(b)]
- Requires that derivative classification authorities be designated in writing and be trained and certified. [2.2(a)]
- Requires that the name or personal identifier of the derivative classifier be included as one of the essential classification markings. [2.2(c)(2)(A)]
- Requires that classification guides conform to standards contained in directives issued by the Information Security Oversight Office. [2.3(a)]
- Requires periodic review and update of classification guides. [2.3(c)]
- Eliminates waivers of the requirement to produce classification guides. [2.3]
- Emphasizes the opportunity for a declassification authority to weigh the public interest by declassifying information that otherwise continues to meet the standards for classification. [3.2(b)]
- Requires agencies to declassify records of permanent historical value before they may be accessioned into the National Archives. [3.3(d)]
- Establishes a maximum life span for all national security protected information. [3.4(a)]
- Permits, after justification and approval, the exemption of four very narrow categories of information from the 45-year automatic declassification requirement. [3.4(b)]
- Requires that any exempted information remain subject to mandatory and systematic declassification review provisions. [3.4(d)]
- Requires the Secretary of State to renegotiate any treaties or international agreements that extend classification beyond 45 years. [3.4(e)]
- Requires all originating agencies to establish a systematic declassification review program for all records that are 25 years old. [3.5(a)]

- Requires agencies to prioritize the systematic declassification review program based upon researcher interest and likelihood of declassification. [3.5(a)]
- Requires the Information Security Oversight Office to assure that the declassification guides developed by the agencies and furnished to the National Archives are adequate and current. [3.5(b)]
- Excuses agencies from the requirement to conduct a mandatory declassification review when the same information has been reviewed within the prior two years. [3.6(a)(3)]
- Requires the Archivist, in conjunction with the agencies and the Information Security Oversight Office, to explore the feasibility of a Government-wide declassification database. [3.8]
- Requires the Archivist to explore further uses of technology to assist the declassification process. [3.8]
- Prevents departing Government officials from removing national security protected information from the agency's control. [4.2(b)]
- Emphasizes the requirement to safeguard national security protected information in automated information systems. [4.2(e)]
- Permits an originating agency to waive the requirement that another agency receive permission before it can disclose the first agency's information to a third agency. [4.2(g)]
- Requires the annual update of any automatic, routine or recurring distribution lists of national security protected information. [4.3(b)]
- Limits, generally, the establishment of special access programs to the Secretaries of State, Defense and Energy, and the Director of Central Intelligence or their principal deputies. [4.4(a)]
- Limits special access programs to meet narrow and specific criteria. [4.4(a)(b)]
- Requires internal oversight and oversight by the Information Security Oversight Office for all special access programs. [4.4(3)]
- Requires that any special access program be revalidated annually. [4.4(b)(4)]

- Requires unanimous approval of an executive committee of agency heads in order to continue any special access program beyond five years. [4.4(b)(5)]
- Requires the agency head or principal deputy to review for revalidation any special access program that predates this Order. [4.4(c)]
- Directs an agency to submit a written justification to the National Security Council when seeking to deny access to the Information Security Oversight Office. [5.3(b)(4)]
- Requires the Director of the Information Security Oversight Office, through directives, to establish uniform standards for safeguarding; security education and training programs; agency self-inspection programs; and classification and declassification guides. [5.3(c)4]
- Establishes an Information Security Policy Advisory Council consisting of Government and Non-Government representatives. [5.4]
- Requires heads of agencies to demonstrate personal and senior management commitment for the effective implementation of this program. [5.5(a)]
- Increases individual accountability by tying performance contracts to the effective implementation of this program. [5.5(c)(7)]
- Requires agencies to account for all costs associated with the security classification program and to submit those costs to the Information Security Oversight Office for publication. [5.5(c)(8)]
- Requires sanctions when an individual creates or continues a special access program contrary to the requirements of the Order. [5.6 (b)(3)]
- Requires the prompt removal of classification authority from an individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of the Order. [5.6(d)]

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.

3

Divider Title: _____

Title 3

Executive Order of ...

The President

National Security Protected Information

TABLE OF CONTENTS

Preamble

Part 1. Original Classification

1.1	Definitions	1
1.2	Classification Standards	2
1.3	Classification Levels	4
1.4	Classification Authority	5
1.5	Classification Categories	7
1.6	Duration of Classification	9
1.7	Identification and Markings	10
1.8	Classification and Prohibitions and Limitations	12
1.9	Classification Challenges	14

Part 2. Derivative Classification

2.1	Definitions	16
2.2	Use of Derivative Classification	18
2.3	Classification Guides	19

Part 3. Declassification and Downgrading

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	26
3.6	Mandatory Declassification Review	28
3.7	Processing Requests	30
3.8	Declassification Database	31

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	Information Security Policy Advisory Council	43
5.5	General Responsibilities	45
5.6	Sanctions	47

Part 6. General Provisions

6.1	General Provisions.....	48
-----	-------------------------	----

DRAFT
July 30, 1993

Executive Order
National Security Protected Information

This Order prescribes a uniform system for classifying, safeguarding and declassifying national security protected 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 critically sensitive information remains a national priority. In recent years, however, dramatic geopolitical changes have altered the national security threats that we confront. These changes also 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) "National security protected information" means information that has been determined pursuant to this Order or any predecessor order to require protection against unauthorized disclosure or uncontrolled dissemination.

(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.

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

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

(g) "Original classification authority" means an individual designated 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 national security protected information to an unauthorized recipient.

(i) "Uncontrolled dissemination" means the distribution, reproduction or transmittal of information outside the control of the originating agency.

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

(k) "Senior agency official" means the official designated by the agency head under Section 5.5(c) of this Order to direct and administer the agency's program under which national security protected information is classified, safeguarded and declassified.

Section 1.2 *Classification Standards.*

(a) Information may be classified in the first instance under the terms of this Order only if 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

(1) **Top Secret** shall be applied to information, the unauthorized disclosure or uncontrolled dissemination 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 or uncontrolled dissemination 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 national security protected information.

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

(d) Information classified **Confidential** under Executive Order 12356 or its predecessors may remain classified for a period not to exceed six years from the effective date of this Order. An original classification authority may upgrade specific **Confidential** information to **Secret** only in accordance with the classification standards and procedures for original classification established by this Order.

(4) the original classification authority determines that the release of the information, either by itself or in the context of other 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) At the discretion of the original classification authority, information that meets the standards for classification may 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) Information classified in accordance with this Order 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 protected information shall be classified at one of the following two levels:

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 the **Top Secret** level are also authorized to classify information at the **Secret** 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; 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.

(3) **Secret** original classification authority may be delegated only by the President; an agency head or official designated pursuant to paragraph (a)(2), above; an official with **Top Secret** original classification authority; or the senior agency official, provided that official has been delegated **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 are trained and certified 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 or uncontrolled dissemination reasonably could be expected to:

- (a) Impair the ability of the United States military to defend the nation from armed aggression, or wage war or other armed conflict; or increase the vulnerability of the United States military, its personnel, installations, weapons, technology, and related systems;
- (b) damage relations between the United States and another country or international organization of governments; impede current diplomatic negotiations; or reveal foreign government information;

- (c) reveal intelligence sources, methods and activities, including special activities and cryptologic activities;
- (d) impair United States Government programs for safeguarding nuclear materials or facilities; or
- (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.

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 frames in paragraphs (b) and (c), below.
- (b) If the original classification authority cannot determine a specific date or event, information classified **Secret** shall be marked for declassification no later than ten years from the date of the original decision.

(c) If the original classification authority cannot determine a specific date or event, information classified **Top Secret** shall be marked for declassification no later than fifteen years from the date of the original decision.

(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 as follows:

(1) Information classified at the **Confidential** level shall be declassified in accordance with Section 1.3(d) of this Order.

(2) Information classified at the **Secret** level shall be declassified no later than ten years from the effective date of this Order.

(3) Information classified at the **Top Secret** level shall be declassified no later than fifteen years from the effective date of this Order.

(e) No earlier than 180 days before information is to be declassified in accordance with paragraphs (b), (c), and (d), above, an original classification authority may extend the duration of classification. Such extensions must conform with the standards and procedures for original classification established by this Order. An extension shall not exceed ten years. Additional extensions must conform with the requirements of this paragraph.

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 two 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) the date or event for declassification; 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 national security protected 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 and shall be provided 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 Order 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 refer it to an appropriate original classification authority for the application of omitted markings.

(g) The original classification authority shall consider the use of a classified addendum whenever national security protected 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) 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.
- (d) Information that has not previously been disclosed to the public under proper authority may be classified 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 through the personal participation and authority and on a

document-by-document basis by 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 may challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall assure that individuals are not subject to retribution for bringing such actions.

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 national security protected 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 describes 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 national security protected 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 national security protected 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. An authorized agency official shall identify 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 and certified 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 the 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 periodically. A guide must be updated or reissued in accordance with the standards of Section 1.6(e) of this Order in order to extend the duration of classification of any information classified derivatively pursuant to the guide.

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 national security protected 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 national security protected 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 national security protected information contained in records that have been determined by the Archivist of the United States to have permanent historical value.

(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 the **Top Secret** level shall be classified and safeguarded at the **Secret** 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 national security protected information with other agencies that have a direct interest in the subject matter.

(b) At the discretion of the agency head or the senior agency official, information that continues to meet the standards for classification may be declassified if it is determined that the public interest in declassifying the information outweighs the need for continued classification.

(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 national security protected 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 national security protected 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) National security protected 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) National security protected information that has been determined by the Archivist of the United States to have permanent historical value shall not be accessioned into the National Archives of the United States until that information has been declassified in accordance with this Order. 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) National security protected information classified under this or any predecessor order shall be automatically declassified 45 years from the date of its creation. This provision shall go into effect two years from the issuance of this Order.

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

- (1) Identify a confidential human intelligence source;
- (2) reveal information not publicly available that would clearly assist in the development or use of weapons of mass destruction;
- (3) reveal information not publicly available that would clearly impair United States cryptologic systems or activities; or
- (4) 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 shall provide the Director of the Information Security Oversight Office with a copy of such a justification at least 180 days before the information is

subject to automatic declassification. The Director may direct the agency not to exempt the information or to designate the information for automatic declassification at an earlier date than recommended. The Director's decision may be appealed to the National Security Council. The information will remain classified while the appeal is pending.

(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 45 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 45 years under this Section.

Section 3.5 *Systematic Declassification Review.*

(a) Each agency that has originated national security protected information under this Order or its predecessors shall establish and conduct a program

for systematic declassification review. This program shall apply to pertinent records no later than 25 years from the date of their creation. Agencies shall prioritize the systematic review of records based upon 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 national security protected information accessioned into the National Archives of the United States as of the effective date of this Order; information 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 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 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. Any decision by the Archivist may be appealed to the Director of the Information Security Oversight Office. Agencies with primary subject matter interest shall be notified promptly of the Director's decision on such appeals and may further appeal to the National Security Council. 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 national security protected 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.

(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 national security protected information, shall explore the feasibility and establish, if feasible, 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 national security protected information.
- (b) "Access" means the ability or opportunity to gain knowledge of national security protected information.
- (c) "Need-to-know" means a determination made by an authorized holder of national security protected information that a prospective recipient requires access to national security protected 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 authorized by an agency head for a specific class of national security protected 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 national security protected 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) National security protected 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 national security protected information from the agency's control.

(c) National security protected information may not be removed from official premises without proper authorization.

(d) Authorized disseminations of national security protected 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 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 national security protected information have controls that:

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

(f) In accordance with national policy directives, each agency head or senior agency official shall establish controls to ensure that national security protected 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, national security protected 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 national security protected 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 5.5(c)(1) 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 by the review panel shall be reviewed by the interagency review panel at each five year interval. 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 his or her principal deputy shall review all existing special access programs under the agency's jurisdiction and continue them only in accordance with the provisions of this Order. Each existing special access program that an agency head or his or her principal deputy continues 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) of this Order that access to national security protected 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 national security protected 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 national security protected 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 implementing its 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 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 national security protected 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 national security protected information;
- (2) agency security education and training programs;
- (3) agency self-inspection programs; and
- (4) classification and declassification guides.

Section 5.4 *Information Security Policy Advisory Council.*

(a) *Establishment.* There is established an Information Security Policy Advisory Council ("Council"). The Director of the Information Security Oversight Office shall serve as Chairman of the Council. The Director shall designate the initial agencies and organizations whose representatives shall comprise the Council. Government representatives shall rotate among the agencies most affected by the program established under this Order and shall be selected by the agency head or senior agency official of those agencies. Non-Government representatives shall rotate among organizations concerned with the classification and declassification of national security protected

information and shall be selected by the governing bodies of those organizations. The Council's by-laws shall establish standards for length of service and rotation among agencies and organizations.

(b) *Functions.*

(1) The Council and its members shall advise the Chairman on all matters concerning the policies established under this Order, including recommended changes to those policies as reflected in this Order or its implementing directives; and

(2) the Council shall serve as a forum to discuss policy issues in dispute.

(c) The Council shall meet at the request of the Chairman, but at least once each calendar year.

(d) *Administration.*

(1) Members of the Council shall serve without compensation for their work on the Council. However, non-government 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. 5701-5707).

(2) 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 5.5 *General Responsibilities.*

Heads of agencies that originate or handle national security protected information shall:

- (a) Demonstrate personal commitment and commit senior management to the successful implementation of the program established under this Order;
- (b) commit necessary resources to the effective implementation of the program established under this Order;
- (c) designate a senior agency official to direct and administer the program, whose responsibilities shall include:
 - (1) Overseeing the agency's program established under this Order, including any authorized special access programs;
 - (2) promulgating implementing regulations, which shall be published in the *Federal Register* to the extent that they affect members of the public;

(3) establishing and maintaining security education and training programs, which shall include the certification of original and derivative classifiers;

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

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

(6) developing special contingency plans for safeguarding national security protected information used in or near hostile or potentially hostile areas;

(7) assuring that the performance contract or other system used to rate civilian or military personnel performance includes the management of national security protected information as a critical element or item to be evaluated in the rating of: (A) original and derivative classification authorities; (B) security managers or security specialists; and (C) all other personnel whose duties significantly involve the creation or handling of national security protected information; and

(8) 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.

Section 5.6 *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.

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.

4

Divider Title: _____

This Order prescribes a uniform system for classifying, safeguarding, and declassifying, ~~and safeguarding~~ national security protected 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 critically sensitive information remains a national priority. In recent years, however, dramatic geopolitical changes have altered the national security threats that we confront. These changes also 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.~~

~~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 I

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) "National security protected information" means information that has been determined pursuant to this Order or any predecessor order to require protection against unauthorized disclosure and uncontrolled dissemination.

(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.

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

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

(g) "Original classification authority" means an individual designated 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 national security protected information to an unauthorized recipient.

(i) "Uncontrolled dissemination" means the distribution, reproduction or transmittal of information outside the control of the originating agency.

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

(k) "Senior agency official" means the official designated by the agency head under Section 5.5(c) of this Order to direct and administer the agency's program under which national security protected information is classified, safeguarded and declassified.

Section 1.2 Classification Standards

(a) Information may be classified in the first instance under the terms of this Order only if 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 release of the information, either by itself or in the context of other 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) At the discretion of the original classification authority, information that meets the standards for classification may 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) Information classified in accordance with this Order 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 protected information (~~hereinafter "classified information"~~) shall be classified at one of the following ~~three~~ two levels:

(1) **Top Secret** shall be applied to information, the unauthorized disclosure or uncontrolled dissemination 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 or uncontrolled dissemination 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.~~

(b) Except as otherwise provided by statute, no other terms shall be used to identify United States national security protected 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 ~~Secret~~higher level, ~~of classification pending a determination by an original classification authority, who shall make this determination within thirty (30) days.~~

(d) Information classified **Confidential** under Executive Order 12356 or its

predecessors may remain classified for a period not to exceed six years from the effective date of this Order. An original classification authority may upgrade specific **Confidential** information to **Secret** only in accordance with the classification standards and procedures for original classification established by this Order.

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*; ~~or~~ and

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

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

____(3) ~~Original~~ **Secret** original classification authority may be delegated only by the President; an agency head or official designated pursuant to ~~paragraph~~ Sections (a)(2) above, 1.2(a)(2); an official with ~~original~~ **Top Secret**

original classification authority; ~~or~~ and the senior agency official ~~designated~~
~~under Section 5.3(a)(1)~~, provided that official has been delegated ~~original~~
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. ~~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), 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 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 are trained and certified 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 or uncontrolled dissemination reasonably could be expected to:~~concerns:~~

(a) impair the ability of the United States military to defend the nation from armed aggression, or wage war or other armed conflict; or increase the

vulnerability of the United States military, its personnel, installations,
weapons technology, and related systems;

(b) damage relations between the United States and another country or
international organization of governments; impede current diplomatic
negotiations; or reveal foreign government information;

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

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

(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.

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

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

~~installations, projects;~~

~~(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 paragraphs (b) and (c), 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, information classified **Secret** shall be marked for declassification no later than ten years from the date of the original decision. ~~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.~~

~~(c) If the original classification authority cannot determine a specific date or event, information classified **Top Secret** shall be marked for declassification no later than fifteen years from the date of the original decision. Information classified under predecessor orders and is 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 as follows:~~

~~_____ (1) Information classified at the **Confidential** level shall be declassified in accordance with Section 1.3(d) of this Order;~~

~~_____ (2) information classified at the **Secret** level shall be declassified no later than ten years from the effective date of this Order; and~~

~~_____ (3) information classified at the **Top Secret** level shall be declassified no later than fifteen years from the effective date of this Order.~~

~~(e) No earlier than 180 days before information is to be declassified in accordance with paragraphs (b), (c), and (d), above, an original classification authority may extend the duration of classification. Such extensions must~~

conform with the standards and procedures for original classification established by this Order. An extension shall not exceed ten years. Additional extensions must conform with the requirements of this paragraph.

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 ~~two~~~~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; ~~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) the date or event for declassification; and, ~~or the notation "Originating Agency's Determination Required."~~

(5) a concise reason for classification, in accordance with instructions contained in the implementing directives instructions 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 national security protected 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.~~

(de) 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 Information Security Oversight Office.

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

(fe) 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 refer it to an appropriate original classification authority for the application of omitted markings.

(gf) The original classification authority shall consider the use of a classified addendum whenever national security protected 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. ~~Only 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 or reclassify information previously declassified and disclosed 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 through the personal participation and authority and on a document-by-document basis by the agency head, the deputy agency head, or the senior agency official, designated under Section 5.6.3(a), 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 may challenge the classification of information that they believe
is improperly classified or unclassified. These procedures shall assure that
individuals are not subject to retribution for bringing such actions.

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 national security protected 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 describes 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 national security protected 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 national security protected 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. An authorized agency official shall identify 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 and certified 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 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.~~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.~~

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)~~; 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 periodically. A guide must be updated or reissued in accordance with the standards of Section 1.6(e) of this Order in order to extend the duration of classification of any information classified derivatively pursuant to the guide. ~~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 national security protected 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 national security protected 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 national security protected information contained in records that have
been determined by the Archivist of the United States to have permanent
historical value.

(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 the **Top Secret** level shall be
classified and safeguarded at the **Secret** 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 national security protected~~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) At the discretion of the agency head, or the senior agency official information that continues to meet the standards for classification may be declassified if it is determined that the public interest in declassifying the information outweighs the need for continued classification. ~~(b) 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 national security protected~~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 national security protected~~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) National security protected~~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 guidelines.

(d) National security protected information that has been determined by the Archivist of the United States to have permanent historical value shall not be accessioned into the National Archives of the United States until that information has been declassified in accordance with this Order. 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) National security protected information classified under this or any predecessor order shall be automatically declassified 45 years from the date of its creation. This provision shall go into effect two years from the issuance of this Order.

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

- _____ (1) Identify a confidential human intelligence source;
- _____ (2) reveal information not publicly available that would clearly assist in the development or use of weapons of mass destruction;
- _____ (3) reveal information not publicly available that would clearly impair United States cryptologic systems or activities; or
- _____ (4) 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 shall provide the Director of the Information Security Oversight Office with a copy of such a justification at least 180 days before the information is subject to automatic declassification. The Director may direct the agency not to exempt the information or to designate the information for automatic declassification at an earlier date than recommended. The Director's decision may be appealed to the National Security Council. The information will remain classified while the appeal is pending.

(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 45 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond years under this Section.

Section 3.53 *Systematic Declassification Review for Declassification.*

(a) Each agency that has originated national security protected information under this Order or its predecessors shall establish and conduct a program for systematic declassification review. This program shall apply to pertinent records no later than 25 years from the date of their creation. Agencies shall prioritize the systematic review of records based upon the degree of researcher interest and the likelihood of declassification upon review.~~(a) 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 national security protected information accessioned into the National Archives of the United States as of the effective date of this Order; information 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 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 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. ~~(a) agency heads may conduct internal systematic review programs for classified information originated by their agencies contained in records determined by the Archivist to be permanently valuable but that have which has 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 national security protected ~~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-

(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, 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. Any decision by the Archivist may be appealed to the Director of the Information Security Oversight Office. Agencies with primary subject matter interest shall be notified promptly of the Director's decision on such appeals and may further appeal to the National Security Council. 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 national security protected~~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.

(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 classifiable 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. In cases in which the originating agency determines in writing that a response under paragraphSection 3.4 (af), (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

national security protected information, shall explore the feasibility and establish, if feasible, 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 national security protected information.

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

(c) "Need-to-know" means a determination made by an authorized holder of

national security protected information that a prospective recipient requires access to national security protected 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 authorized by an agency head for a specific class of national security protected 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 national security protected 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 provide 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) National security protected 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 national security protected information from the agency's control.~~(b) 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) National security protected information may not be removed from official premises without proper authorization.

(d) Authorized disseminations of national security protected information outside the executive branch shall assure the protection of the information in a manner equivalent to that provided within the executive branch.~~(e)~~

~~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 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 national security protected information have controls that:

(1) Prevent access by unauthorized persons; and

(2) ensure the integrity of the information.

(f) In accordance with national policy directives, each agency head or senior agency official shall establish controls to ensure that national security protected 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, national security protected ~~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 national security protected 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 5.5(c)(1) 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 by the review panel shall be reviewed by the interagency review panel at each five year interval. An agency head may appeal the review panel's disapproval of a special access program to the President ~~(b) 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 6.2(b)(5), shall have non delegable access to all such accountings.~~

(c) Within 180 days after the effective date of this Order, each agency head or his or her principal deputy shall review all existing special access programs under the agency's jurisdiction and continue them only in accordance with the provisions of this Order. Each existing special access program that an agency head or his or her principal deputy continues 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) of this Order that access to national security protected~~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 national security ~~protected/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 national security protected 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 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, and by 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, information inspections, and other cooperation that may be necessary to fulfill ~~the Director's responsibilities. If granting~~ access to specific categories of national security protected~~classified~~ information would pose an exceptional national security risk, the affected agency head or the senior agency shall submit a written justification recommending the denial to the National Security Council within 60 days of the Director's request~~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 national security protected information;

(2) agency security education and training programs;

(3) agency self-inspection programs; and

(4) classification and declassification guides.

Section. 5.4 Information Security Program Policy Advisory Council.

(a) Establishment. There is established an Information Security Policy Advisory Council ("Council"). The Director of the Information Security Oversight Office shall serve as Chairman of the Council. The Director shall designate the initial agencies and organizations whose representatives shall

comprise the Council. Government representatives shall rotate among the agencies most affected by the program established under this Order and shall be selected by the agency head or senior agency official of those agencies. Non-Government representatives shall rotate among organizations concerned with the classification and declassification of national security protected information and shall be selected by the governing bodies of those organizations. The Council's by-laws shall establish standards for length of service and rotation among agencies and organizations.

(b) Functions.

____ (1) The Council and its members shall advise the Chairman on all matters concerning the policies established under this Order, including recommended changes to those policies as reflected in this Order or its implementing directives; and

____ (2) The Council shall serve as a forum to discuss policy issues in dispute.

(c) The Council shall meet at the request of the Chairman, but at least once each calendar year.

(d) Administration.

____ (1) Members of the Council shall serve without compensation for their work on the Council. However, non-government 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. 5701-5707).

(2) 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. 5.53 *General Responsibilities.*

Heads of Agencies that originate or handle national security protected classified information shall:

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

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

(ca) designate a senior agency official to direct and administer its information security the program, whose responsibilities which shall include

~~active oversight and security education programs to ensure effective implementation of this Order;~~

_____ (1) Overseeing the agency's program established under this Order, including any authorized special access programs;

_____ (2b) promulgating implementing regulations, which ~~Any unclassified regulations that establish agency information security policy~~ shall be published in the *Federal Register* to the extent that these regulations affect members of the public;

_____ (3) establishing and maintaining security education and training programs, which shall include the certification of original and derivative classifiers;

_____ (4) establishing and maintaining security education and training programs, which shall include the periodic review and assessment of the agency's classified product;

_____ (5e) establishing procedures to prevent unnecessary access to national security protected~~classified~~ information, including procedures that:

_____ (Ai) ~~r~~Require that a demonstrable need for access to national security protected~~classified~~ information is established before initiating administrative clearance procedures; and

_____ (Bii) ensure that the number of persons granted access to national security protected~~classified~~ information is limited to the minimum consistent with operational and security requirements and needs;

_____ (6d) developing special contingency plans for the safeguarding~~protection~~ of national security protected~~classified~~ information used in or near hostile or potentially hostile areas;

_____ (7) assuring that the performance contract or other system used to rate civilian or military personnel performance includes the management of national security protected information as a critical element or item to be evaluated in the rating of:

_____ (A) Original and derivative classification authorities;

_____ (B) security managers or security specialists; and (C) all other personnel whose duties significantly involve the creation or handling of national security protected information; and

_____ (8) 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.

Section 5.64 *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 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 national security protected~~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~~
~~6.4(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 ~~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 issuance ~~on August 1, 1982.~~