

Executive Order
Classified National Security Information

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

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

AID Comment: Revise the second line of the title as follows:

~~Classified National Security Information~~ Classified in the National Interest

RATIONALE: Eliminate redundancy since the terms "classified" and "national security information" are commonly used interchangeably. The original text is also misleading because it implies the existence of unclassified national security information.

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 of the agency that originates information, or its successor in function, to regulate access to the information.*

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

(d) *"Foreign Government Information" means:*

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

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

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

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

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

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

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

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

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

(k) *"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 that the information or relationship, or both, be held in confidence.*

(l) *"Damage to the national security" means harm to the national defense or foreign relations of the United States from the disclosure of information, to include the sensitivity, value, and utility of that information.*

AID Comment: General Comment on the definition sections throughout the Order: Move all definitions to the end of the Order, and eliminate the word "means" in defining terms. For example, 1.1(a) should read: *"National Security."* The national defense or foreign relations of the United States.

RATIONALE: Placing the definitions at the end helps identify the substance of the Order, and facilitates its reading.

NRC Comment: General comment: Add the NRC to the list of agencies having original classification authority.

RATIONALE: NRC has a need to classify information dealing with the national defense and foreign relations.

STATE Comment: General comment: Define "foreign government" in section 1.1.

RATIONALE: Seeks to include international organizations in definition of foreign government. The addition is also consistent with the definition of Foreign Government Information provided in the Order.

TREASURY General Comment: Make a separate entry for the definition of "control" (1.1(b)).

RATIONALE: None provided.

DOD Comment: Revise paragraph 1.1(b) as follows:

(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 of the United States

Government ~~agency that originates information, or its successor in function,~~
to regulate access to the information.

RATIONALE: Clarity. Also, defining "control" in terms of the U.S.

Government recognizes that classified information is shared and accessed by various agencies.

AID Comment: Revise paragraph 1.1(c) as follows:

(c) "Classified ~~national security~~ information," (hereafter "~~classified information~~") which also may be referred to as "national security information" means information that has been determined pursuant to this Order or any predecessor order to require protection against disclosure.

RATIONALE: Eliminate redundancy since the terms "classified" and "national security information" are commonly used interchangeably.

DOT Comment: Revise paragraph 1.1(c) as follows:

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

RATIONALE: Clarity and completeness.

CIA Comment: Revise paragraph 1.1(c) as follows:

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

RATIONALE: Clarity, completeness and consistency.

DOD Comment: Revise paragraph 1.1(c) as follows:

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

RATIONALE: Completeness; the key word in this context is "unauthorized."

TREASURY Comment: Revise paragraph 1.1(c) as follows:

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

RATIONALE: Completeness; the key word in this context is "unauthorized."

AID Comment: Revise paragraph 1.1(e) as follows:

(e) "Classification" means the act or process by which information is determined to ~~be classified information~~ require protection in the interests of national security.

RATIONALE: Clarity.

CIA Comment: Revise paragraph 1.1(f) as follows:

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

RATIONALE: Clarity, completeness and consistency.

DOD Comment: Revise paragraph 1.1(f) as follows:

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

RATIONALE: Completeness; the key word in this context is "unauthorized."

TREASURY Comment: Revise paragraph 1.1(f) as follows:

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

RATIONALE: Completeness.

NSC Comment: Revise paragraph 1.1(i) as follows:

(i) "Agency" has the meaning provided at 5 U.S.C. § 552(f). The provisions of this Order also apply to those entities within the Executive Branch that are not agencies within the meaning of 5 U.S.C. § 552(f).

RATIONALE: Make clear that the provisions of the Order apply to executive branch agencies that are not agencies within the meaning of 5 U.S.C. § 552(f).

DOT Comment: Revise paragraph 1.1(i) as follows:

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

RATIONALE: 5 U.S.C. § 552(e) is the proper citation.

DOD Comment: Revise paragraph 1.1(k) as follows:

(k) "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 that the information or relationship, or both, are to be held in confidence.

RATIONALE: Consistency with the text of paragraph 1.1(d)(2).

CIA Comment: Revise paragraph 1.1(l) as follows:

(l) "Damage to the national security" means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

RATIONALE: Clarity, completeness and consistency.

DOD Comment: Revise paragraph 1.1(l) as follows:

(l) "Damage to the national security" means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

RATIONALE: Clarity and completeness.

TREASURY Comment: Revise paragraph 1.1(l) as follows:

(l) "Damage to the national security" means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

RATIONALE: Completeness.

Section 1.2 Classification Standards

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

- (1) An original classification authority classifies the information;*
- (2) the information is owned by, produced by or for, or is under the control of the United States Government;*
- (3) the information falls within one or more of the categories of information listed in Section 1.5 of this Order; and*
- (4) the original classification authority determines that the disclosure of the information reasonably could be expected to result in damage to the national security and the original classifier is able to identify or describe the damage.*

(b) If there is significant doubt about the need to classify information, it shall not be classified. This provision does not:

- (1) Amplify or modify the substantive criteria or procedures for classification; and*
- (2) create any substantive or procedural rights subject to judicial review.*

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

DOD Comment: Revise paragraph 1.2(a)(4) as follows:

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

RATIONALE: Clarity and completeness.

DOT Comment: Revise paragraph 1.2(a)(4) as follows:

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

RATIONALE: Clarity and completeness.

TREASURY Comment: Revise paragraph 1.2(a)(4) as follows:

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

RATIONALE: Completeness.

AID Comment: Revise paragraph 1.2(b) as follows:

(b) If ~~there is significant doubt~~ exists about the need to classify information, it shall be ~~not be~~ classified.

RATIONALE: In doubtful cases, it's best to err on the side of caution and classify the information.

DOT Comment: Revise paragraph 1.2(b) as follows:

If there is a reasonable ~~significant~~ doubt about the need to classify information, it shall not be classified. . . .

RATIONALE: Removes the confusion associated with the term "significant."

Section 1.3 *Classification Levels.*

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

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

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

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

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

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

AID Comment: Revise paragraphs 1.3(a)(1), (a)(2) and (a)(3) as follows:

(1) **Top Secret** shall be applied to information, the disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security ~~that the original classification authority is able to identify or describe.~~

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

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

RATIONALE: The provision for challenges in Section 1.9 makes this requirement unnecessary.

DOT Comment: Revise paragraphs 1.3(a)(1), (a)(2) and (a)(3) as follows:

(1) **Top Secret** shall be applied to information, the disclosure of which ~~reasonably~~ could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

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

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

RATIONALE: None provided.

CIA Comment: Revise paragraph 1.3(a)(1), (a)(2) and (a)(3) as follows:

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

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

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

RATIONALE: Clarity, completeness and consistency.

DOD Comment: Revise paragraph 1.3(b) as follows:

(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information. "FOREIGN GOVERNMENT RESTRICTED" may be used to identify foreign government information that is classified as Restricted and which ordinarily requires less protection than United States Confidential information.

RATIONALE: Paragraph 4.2(g) of the draft affords less protection for certain Foreign Government information marked RESTRICTED. This change remedies that weakness.

AID Comment: Revise paragraph 1.3(c) as follows:

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

RATIONALE: Caution recommends to err on the side of the higher classification.

DOT Comment: Revise paragraph 1.3(c) as follows:

(c) If there is reasonable ~~significant~~ doubt about the appropriate level of classification, it shall be ~~classified~~ safeguarded at the ~~lower~~ higher level pending a determination by an original classification authority.

RATIONALE: Basic risk principles dictate that when dealing with national security information is best to err on the side of protection.

Section 1.4 Classification Authority.

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

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

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

(c) *Delegation of Original Classification Authority.*

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

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

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

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

(d) *Original classification authorities must receive training in original classification as provided in this Order and its implementing directives.*

(e) *Exceptional Cases. When an employee, contractor, licensee, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this Order and its implementing directives. The information shall be transmitted promptly as provided under this Order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within thirty (30) days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.*

CIA Comment: Revise paragraph 1.4(e) as follows:

(e) *Exceptional Cases. . . . 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 agencies having primary subject matter interest and forward the information, with appropriate recommendations, to ~~that~~ those agencies for a classification determination.*

RATIONALE: The change recognizes that more than one agency may have subject matter interest.

TREASURY Comment: Revise paragraph 1.4(e) as follows:

(e) *Exceptional Cases.* . . . 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~~ Security Policy Board. The ~~Director Board~~ shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

RATIONALE: The Security Policy Board established by PDD 29 is the proper entity.

NRC Comment: Revise paragraph 1.4(e) as follows:

(e) *Exceptional Cases.* When an employee, contractor, licensee, certificate holder, 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. . . .

RATIONALE: The Energy Policy Act of 1992 identifies certificate holders as a new category which should be included in this Order.

Section 1.5 *Classification Categories.*

Information may not be considered for classification unless it concerns:

- (a) Military plans, weapons, or operations;*
- (b) Foreign government information;*
- (c) Intelligence activities (including special activities), intelligence sources or methods, or cryptology;*
- (d) Foreign relations or foreign activities of the United States, including confidential sources;*
- (e) Scientific, technological, or economic matters relating to the national security;*
- (f) United States Government programs for safeguarding nuclear materials or facilities; or*
- (g) Vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.*

AID Comment: Revise the leading sentence of section 1.5 as follows:

Information, including but not limited to the following, may not be considered for classification unless it concerns:

RATIONALE: The categories listed do not allow classifying information such as travel plans of senior officials or schedules of meetings in high risk areas.

USN (Naval Reactors) Comment: Revise paragraph 1.5(a) as follows:

(a) Military plans, weapons systems, or operations;

RATIONALE: Ensure consistency with sections 1.6 and 3.4.

AID Comment: Revise paragraph 1.5(c) as follows:

(c) Intelligence activities (including special activities), intelligence sources or methods, including confidential sources or cryptology;

RATIONALE: "Confidential sources" applies more to intelligence activities than to foreign relations.

AID Comment: Revise paragraph 1.5(d) as follows:

(d) Foreign relations or foreign activities of the United States, ~~including confidential sources~~;

RATIONALE: The term "Confidential sources" applies to intelligence activities rather than to foreign relations.

DOD Comment: Revise paragraph 1.5(g) as follows:

(g) Vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security and national security emergency preparedness.

RATIONALE: Allows for the protection of plans related to the continuity of Government in national security emergencies. This change also promotes consistency with paragraph 1.6(d)(7).

Section 1.6 Duration of Classification.

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

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

(c) An original classification authority may extend the duration of classification or reclassify specific information for a period not to exceed ten additional years if such action is consistent with the standards and procedures established under this Order. This provision does not apply to information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.

(d) At the time of original classification, the original classification authority may exempt from automatic declassification specific information the disclosure of which could reasonably be expected to cause damage to the

national security for a period greater than that provided in paragraph (b), above, and the release of which could reasonably be expected to:

(1) Reveal an intelligence source, method, or activity, or a cryptologic system or activity;

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

(3) reveal information that would impair the development or use of technology within a United States weapon system;

(4) reveal United States military plans, or national security emergency preparedness plans;

(5) reveal foreign government information;

(6) damage relations between the United States and a foreign government, or reveal a confidential source;

(7) impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized; or

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

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

STATE Comment: Revise paragraph 1.6(c) as follows:

(c) An original classification authority may extend the duration of classification or reclassify specific information for ~~a~~ successive periods not to

exceed ten ~~additional~~ years at a time if such action is consistent with the standards and procedures established under this Order.

RATIONALE: Assuming that this provision would permit more than one 10 year extension, the proposed language provides clarity.

TREASURY Comment: Clarify the meaning of paragraph 1.6(c).

RATIONALE: Revise the paragraph to clarify whether this section allows extensions of duration of classification only once, or whether the authority can be repeatedly invoked.

NARA Comment: General comment on paragraph 1.6(d):

The exemptions from automatic declassification at the time of original classification will not provide significant change from the current Order.

RATIONALE: N/A.

CIA Comment: Revise paragraph 1.6(d) as follows:

(d) At the time of original classification, the original classification authority may exempt from automatic declassification specific information, the disclosure of which could reasonably be expected to cause damage to the

national security, for a period greater than that provided in paragraph (b), above, and the release of which could reasonably be expected to:

RATIONALE: Punctuation after the words "information" and "security" clarifies this section. The existing language, if taken literally, means that information could be exempted from automatic declassification if its disclosure reasonably could be expected to cause 10 years, or more, worth of damage to the national security.

CIA Comment: Revise paragraph 1.6(d) as follows:

(d) At the time of original classification, the original classification authority may exempt from automatic declassification specific information the unauthorized disclosure of which could reasonably be expected to cause damage to the national security for a period greater than that provided in paragraph (b), above, and the release of which could reasonably be expected to:

RATIONALE: Ensures consistency with paragraph 1.1(h).

DOT Comment: General comment on paragraph 1.6(d):

Amend to include a specific date or event for review of all documents exempted from the 10-year rule.

RATIONALE: An automatic exemption from declassification will become as over-used as "OADR" is in the current Order.

NRC Comment: Revise exemptions in paragraph 1.6(d) to use same exemptions used in paragraph 3.4(b).

RATIONALE: Exemptions should be consistent for both the 10-year and 25-year rules.

NRC Comment: Revise paragraph 1.6(d)(2) as follows:

(2) reveal information that would assist in the development or use of weapons of mass destruction, or reveal United States programs to protect nuclear materials;

RATIONALE: As written, the exemption does not appear to include protective measures for facilities which possess significant quantities of nuclear material which could be used in weapon production. Also, if the exemption criteria is not explicitly stated, the legal basis for NRC actions may be subject to litigation.

DOD Comment: Revise paragraph 1.6(d)(3) to read:

(3) reveal information that would impair the effectiveness of a United States weapon system, or the development or use of technology within a United States weapon system or assist in development of a foreign nuclear powered submarine weapon system which adversely would affect the national security;

RATIONALE: Operational characteristics within a weapon system may require added protection.

USN (Naval Reactors) Comment: Revise paragraph 1.6(d)(3) as follows:

(3) reveal information that would impair the development or use of technology within a United States weapon system, or assist in development of a foreign weapon system which would adversely impact the national security;

RATIONALE: Technology should be protected for as long as it might be useful in the development of a foreign weapon system, especially as that technology pertains to the nuclear propulsion of ships.

AID Comment: Revise paragraph 1.6(d)(6) as follows:

(6) damage relations between the United States and a foreign government, ~~or reveal a confidential source;~~

RATIONALE: "Confidential Source" is more applicable to intelligence activities than to foreign relations. Move the phrase "reveal a confidential source" to Paragraph 1.6(d)(1).

STATE Comment: Revise paragraph 1.6(d)(6) as follows:

Option 1. (6) ~~damage relations between the United States and a foreign government, or reveal a confidential source;~~ would damage current diplomatic negotiations or other ongoing official activities of the United States;

or

Option 2. (6) damage relations between the United States and a foreign government, ~~or reveal a confidential source,~~ or ongoing diplomatic activities of the United States;

RATIONALE: The exception should not be limited to impairing a bilateral relationship between the U.S. and a foreign government. Important U.S. foreign policy objectives may, for example, involve information regarding negotiation strategies, anti-terrorism, a non-governmental organization, or international organizations.

NRC Comment: Revise language in paragraph 1.6(d)(6) as follows:

(6) ~~damage relations between the United States and a foreign government,~~
~~or reveal a confidential source;~~

RATIONALE: As written, authorizes classification to prevent embarrassment. This is in conflict with paragraph 1.8(a)(2).

ACDA Comment: Revise paragraph 1.6(d)(6) as follows:

(6) damage ~~relations between the United States and a foreign government,~~
the foreign relations or impede the foreign activities of the United States, or
reveal a confidential source;

RATIONALE: Existing language appears inadequate to protect certain functions and activities abroad.

DOT Comment: Clarify paragraph 1.6(d)(7) and (8).

RATIONALE: These two paragraphs should coincide with Section 1.5.

STATE Comment: Clarify paragraphs 1.6(d)(7) and (8).

RATIONALE: Neither 1.6(d)(7) nor 1.6(d)(8) is mentioned in Section 1.5. State assumes that the information would have been originally classified under paragraph 1.5(g) dealing with plans relating to the national security or

Paragraph 1.5(d) dealing with foreign relations of the United States. If this is NOT the intention, the relationship to Section 1.5 should be clarified.

Section 1.7 Identification and Markings.

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

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

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

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

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

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

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

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

(5) a concise reason for classification which, at a minimum, cites the applicable classification categories in Section 1.5 of this Order.

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

(c) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, which portions are exempt from automatic declassification under Section 1.6(d) of this Order, and which portions are unclassified. In accordance with standards prescribed in directives issued under this Order, the Director of the Information Security Oversight Office may grant waivers of this requirement for specified classes of documents or information. The Director shall revoke any waiver upon a finding of abuse.

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

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

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

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

AID Comment: General comment: Revise paragraph 1.7(a) to provide additional time to accomplish this requirement.

RATIONALE: This explicitly requires automated information systems to incorporate required identification and markings. This may require modification of existing code. Code modification is time-consuming and labor intensive and unlikely all could be accomplished within 180 days.

DOD Comment: Change paragraph 1.7(a)(4)(A) to read:

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

RATIONALE: Avoid ambiguity about the relationship of the provisions.

COMMERCE Comment: General comment on paragraph 1.7(a)(5):

Allowing only the citing of the applicable classification category(ies) as a reason for classification seems to defeat the Order's purpose of requiring classifiers to make thoughtful and reasoned classification decisions.

RATIONALE: N/A.

DOD Comment: Revise paragraph 1.7(b) as follows:

(b) Specific information contained in paragraph (a), above, ~~shall~~ may be excluded if it would reveal additional classified information. Classified information may be included in the markings required by paragraph (a), above.

RATIONALE: There are instances when criteria listed in 1.7(a) need to be included on the face of a document and would not be subject to unauthorized disclosure.

DOD Comment: Revise paragraph 1.7(c) as follows:

(c) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, ~~which portions are exempt from automatic declassification under Section 1.6 (d) of this Order~~

RATIONALE: Eliminate a requirement that is unduly burdensome; agencies have no resources to allow strict observance of this requirement.

TREASURY Comment: Delete the reference to the ISOO Director in paragraph 1.7(d).

RATIONALE: PDD 29 gives the Security Policy Board responsibility for issuing implementing directives.

AID Comment: Delete paragraph 1.7(f).

RATIONALE: The requirement to coordinate with an appropriate original classification authority is burdensome and time-consuming.

CIA Comment: Revise paragraph 1.7(f) as follows:

(f) . . . Whenever such information is reviewed for possible declassification,
~~H~~holders of such information shall coordinate with an appropriate
classification authority for the application of omitted markings.

RATIONALE: Clarify that the requirement for coordination applies only
when such documents are reviewed for declassification.

DOE Comment: Revise paragraph 1.7(f) as follows:

(f) Information assigned a level of classification under this or predecessor
orders shall be considered as classified at that level of classification despite
the omission of other required markings. ~~Holders of such information shall
coordinate with an appropriate classification authority for the application of
omitted markings.~~ When a document is being transmitted outside of the
originator's or holder's organization, the document shall be coordinated with
an appropriate classification authority to assure the omitted markings are
applied. Any document retired to a repository prior to the date of this Order
is not required to be reviewed for applying omitted markings while in the
repository or when retrieved from the repository for reference, inventory, or
similar purposes.

RATIONALE: Limit the circumstances under which omitted markings are
applied. Agencies do not have the resources to review and remark existing
documents with omitted markings.

COMMERCE Comment: General comment on paragraph 1.7(f): Marking errors should be returned to the originator.

RATIONALE: Clarity. Only the originator is responsible for correcting mistakes. The reference to an appropriate classification authority could be interpreted to mean a derivative classifier.

Section 1.8 *Classification Prohibitions and Limitations.*

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

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

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

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

(d) *Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. § 552) or the Privacy Act of 1974 (5 U.S.C. § 552a), or the mandatory review provisions of Section 3.6 of this Order only if such classification meets the requirements of this Order and is accomplished on a document-by-document basis under the personal participation or direction of the agency head, the deputy agency head, or the senior agency official designated under Section 5.6 of this Order. This provision does not apply to classified information contained in records*

that are more than 25 years old and have been determined to have permanent historical value under title 44 United States Code.

(e) Compilations of items of information which are individually unclassified may be classified if 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.*

USN (JAG) Comment: General comment on paragraph 1.8(c): Delete this requirement.

RATIONALE: Allow reclassification of information in cases where declassification was approved in error and damage to national security is imminent, provided the information is reasonably retrievable and further dissemination could be prohibited.

USN (JAG) Comment: Revise paragraph 1.8(d) as follows:

(d) . . . only of such classification meets the requirements of this Order and is accomplished on a document-by-document basis under the personal participation or direction of the ~~agency head, the deputy agency head, or the senior agency official designated under Section 5.6 of this Order.~~ Original Classification Authorities and their legitimate delegees, as defined in paragraph 1.1(g), and as designated in accordance with section 1.4. This provision does not apply to classified information contained in records that

are more than 25 years old and have been determined to have permanent historical value under title 44 United States Code.

RATIONALE: Existing language would consume valuable time of senior government officials.

CIA Comment: Revise paragraph 1.8(e) as follows:

(e) ~~Compilations of~~ Items of information which are individually unclassified may be classified if, when compiled, the compiled information reveals ~~an~~ additional information 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~~" "compiled information" means an arrangement . . . gathered together.

RATIONALE: Ensure that each individual piece of intelligence information will not aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself.

DOE Comment: Revise paragraph 1.8(e) as follows:

(e) Compilations of items of information which are (1) individually unclassified or (2) classified at a lower level may (1) be classified or (2)

classified at a higher level if 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.~~

RATIONALE: Compilations at lower levels can also result in a higher classification level.

Section 1.9 Classification Challenges.

(a) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph (b), below.

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

USIA Comment: General comment on Section 1.9:

USIA is concerned about retrieving information which has been released to the public as unclassified and which is later determined to be classified.

RATIONALE: N/A.

DEA Comment: General Comment on paragraphs 1.9(a) & (b): Clarify the requirements of these paragraphs.

RATIONALE: Requires clarification to eliminate any confusion regarding whether there will be an affirmative duty to challenge improper classifications.

TREASURY Comment: Revise Paragraph 1.9(b) as follows:

In accordance with direction from the Director of the Information Security Oversight Office,

RATIONALE: PDD 29 assigns to the Security Policy Board responsibility for issuing implementing directives.

Section 2.1 Definitions.

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

(a) "Derivative classification" means the act of incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance.

The duplication or reproduction of existing classified information is not derivative classification.

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

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

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

(e) "Multiple sources" means two or more source documents, classification guides or a combination of both.

AID Comment: Revise paragraph 2.1(a) as follows:

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

RATIONALE: Use of the word "new" may be misinterpreted to apply to the information, vice the form or format.

AID Comment: Delete the requirement in paragraph 2.1(c) that each original classification authority produce a classification guide, or revise the paragraph to require only one standard guideline.

RATIONALE: Requiring each original classification authority to produce a classification guide fosters duplication of effort.

Section 2.2 Use of Derivative Classification.

(a) 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) 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. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward: (A) the date or event for declassification that corresponds to the longest period of classification among the sources; and (B) a listing of these sources on or attached to the official file or record copy.*

DOE Comment: Change paragraph 2.2(b) to paragraph 2.2(c), and add a new paragraph 2.2(b) as follows:

(b) Derivative classifiers shall be trained in derivative classification as provided in this Order and its implementing directive.

RATIONALE: Derivative classification often requires technical expertise to make subtle judgments. Requiring training would be the single most

effective tool in preventing overclassification and eliminating other classification problems.

Section 2.3 Classification Guides.

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

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

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

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

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

DOD Comment: Revise paragraph 2.2(b)(2) as follows:

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

RATIONALE: Provides a parallel to the concept of derivative classification.

Part 3

Declassification and Downgrading

Section 3.1 Definitions.

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

- (a) "Declassification" means the authorized change in the status of information from classified information to unclassified information.*
- (b) "Automatic declassification" means the declassification of information based solely upon:*
 - (1) The occurrence of a specific date or event as determined by the original classification authority; or*
 - (2) the expiration of a maximum time frame for duration of classification established under this Order.*
- (c) "Declassification authority" means:*
 - (1) The official who authorized the original classification, if that official is still serving in the same position;*
 - (2) the originator's successor;*
 - (3) a supervisory official of either; or*
 - (4) officials delegated declassification authority in writing by the agency head or the senior agency official.*
- (d) "Mandatory declassification review" means the review for declassification of classified information in response to a request for declassification that meets the requirements under Section 3.6 of this Order.*
- (e) "Systematic declassification review" means the review for declassification of classified information contained in records that have been determined by the Archivist of the United States to have permanent historical value in accordance with chapter 33 of title 44, United States Code.*
- (f) "Declassification guide" means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.*

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

(h) *"File series" means documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.*

CIA Comment: Revise paragraph 3.1(c)(2) as follows:

(2) the originator's successors;

RATIONALE: If the originator is succeeded more than once, everyone after the first successor loses his status as a declassification authority.

AID Comment: Revise paragraph 3.1(e) as follows:

(e) "Systematic declassification review" means the review for declassification of classified information no older than 5 years contained in records that have been determined by the originating Agency or the Archivist of the United States to have permanent historical value ~~in accordance with chapter 33 of title 44, United States Code.~~

RATIONALE: The proposed language does not reflect the declassification program which the Order requires of originating agencies in addition to the efforts of the Archivist (as stated in paragraph 3.3(d)).

NARA Comment: General comment on paragraph 3.1(e): Add a reference to Chapter 21 of the United States Code.

RATIONALE: Completeness, since Chapter 21 concerns the accession of historical records into the National Archives.

AID Comment: Delete the requirement in paragraph 3.1(f) that each agency produce a declassification guide, or revise the paragraph to require only one standard guideline.

RATIONALE: Requiring each agency to produce a declassification guide fosters duplication of effort.

DOD Comment: Revise paragraph 3.1(f) as follows:

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

RATIONALE: Recognizes that original classification authorities routinely issue declassification guidance as an integral part of classification guidance.

Section 3.2 Authority for Declassification.

(a) Information shall be declassified as soon as it no longer meets the standards for classification under this Order.

(b) It is presumed that information that continues to meet the classification requirements under this Order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or a senior agency official with responsibility for processing Freedom of Information Act requests or mandatory review requests under this Order. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure. This provision does not:

(1) Amplify or modify the substantive criteria or procedures for classification; and

(2) create any substantive or procedural rights subject to judicial review.

(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.

COMMERCE Comment: General comment on paragraph 3.2(b): Revise language to assure that an independent security review will be conducted prior to declassification of information.

RATIONALE: As written, the language only provides that an official with FOIA responsibilities review and determine public interest. This review does not strike sufficient balance between the public's right to access and the damage that might result from disclosure.

DEA Comment: General comment on paragraph 3.2(b): The paragraph permits, at each agency's discretion, the balancing of the public interest in disclosure against the damage to national security. Recommend that either (1) only agency heads may make these determinations, or (2) an interagency body make these determinations.

RATIONALE: Unless directives carefully address this discretionary responsibility, the provision could result in differing standards on when the public interest outweighs damage to the national security.

DOD Comment: Revise paragraph 3.2(b) as follows:

(b) . . . When such questions arise, they shall be referred to the agency head or athe senior agency official ~~with responsibility for processing Freedom of Information Act requests or mandatory review requests under this Order. . . .~~

RATIONALE: The FOIA official may not be of sufficient rank within the organization to make this determination. Also, use of the senior agency official term is consistent with remainder of the Order.

STATE Comment: Revise paragraph 3.2(b) as follows:

(b) . . . When such questions arise, they shall be referred to the agency head or a senior agency official ~~with responsibility for processing Freedom of Information Act requests or mandatory review requests under this~~ Order. . . .

RATIONALE: Eliminate confusion since the "Senior Agency Official" is not necessarily the official responsible for Freedom of Information Act requests.

NSC Comment: Revise paragraph 3.2(c) as follows:

(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 President through the Assistant to the President for National Security Affairs. The information shall remain classified pending a prompt decision on the appeal.

RATIONALE: Ensure consistency with the Government's position in Armstrong v. Executive Office of the President that the NSC is not an agency.

DOD Comment: Add a new paragraph to 3.2 as follows:

(e) Foreign government information shall not be declassified without the prior written consent of the originating government.

RATIONALE: Reciprocity and compliance with existing agreements.

Section 3.3 Transferred Information.

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

(b) In the case of classified information that is not officially transferred as described in paragraph (a), above, but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this Order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the information.

(c) Classified information accessioned into the National Archives of the United States as of the effective date of this Order shall be declassified or downgraded by the Archivist of the United States in accordance with this Order, the directives of the Information Security Oversight Office, and agency declassification guides.

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

2203 of title 44, United States Code, or information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that goes out of existence.

(e) To the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in Sections 1.6 and 3.4 of this Order.

FEMA Comment: General comment on paragraph 3.3(c):

Language does not adequately ensure that the Archivist will continue classification for information that FEMA identifies in declassification guides as requiring continued protection.

RATIONALE: N/A.

CIA Comment: Revise paragraph 3.3(c) as follows:

(c) Classified information accessioned into the National Archives of the United States as of the effective date of this Order shall be declassified or downgraded by the Archivist of the United States, in coordination with the originating agency, in accordance with this Order, the directives of the Information Security Oversight Office, and agency declassification guides.

RATIONALE: Information originated by one agency may be contained in records accessioned by another agency. The proposed revision provides opportunity for the originating agency to be consulted.

TREASURY Comment: Modify paragraph 3.3(c) so that directives referenced are those of the Security Policy Board.

RATIONALE: PDD 29 assigns to the Security Policy Board responsibility for issuing implementing directives.

NARA Comment: General comment on paragraph 3.3(d): Modify the paragraph to include a reference to 44 U.S.C. Section 2111.

RATIONALE: Allow exception for donated historical materials accessioned into the National Archives.

Section 3.4 Automatic Declassification.

(a) Subject to paragraph (b), below, within five years from the issuance of this Order, all classified information contained in records that (1) are more than 25 years old, and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. Subsequently, all classified information in such records shall be automatically declassified no longer than 25 years from the date of its original classification, except as provided in paragraph (b), below.

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

(1) Reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method;

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

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

(4) reveal information that would impair the application of state of the art technology within a United States weapon system;

(5) reveal actual United States military war plans that remain in effect;

(6) reveal information that would seriously and demonstrably impair relations between the United States and a foreign government; or

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

(c) No later than the effective date of this Order, an agency head shall notify the President through the National Security Council of any specific file series of records for which a review or assessment has determined that the information within those file series almost invariably falls within one or more of the exemption categories listed in paragraph (b), above, and which the agency proposes to exempt from automatic declassification. The notification shall include:

(1) A description of the file series;

(2) an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and

(3) except for the identity of a confidential human source, a specific date or event for declassification of the information.

The President may direct the agency head not to exempt the file series or to declassify the information within that series at an earlier date than recommended.

(d) At least 180 days before it becomes subject to automatic declassification under this Section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as executive secretary of the Interagency Security Classification Appeals Panel, of any specific information beyond that included in a notification to the President under paragraph (c), above, that the agency proposes to exempt from automatic declassification. The notification shall include:

(1) A description of the information;

(2) an explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time; and

(3) except for the identity of a confidential human source, a specific date or event for declassification of the information. The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than

recommended. The agency head may appeal such a decision to the President through the National Security Council. The information will remain classified while such an appeal is pending.

(e) No later than the effective date of this Order, the agency head or senior agency official shall provide the Director of the Information Security Oversight Office with a plan of action for compliance with the requirements of this Section, including the establishment of interim target dates. Each such plan of action shall include the requirement that the agency declassify at least 15 percent of the records affected by this Section no later than one year from the effective date of this Order, and similar commitments for subsequent years until the effective date for automatic declassification.

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

(g) The Secretary of State shall determine when the United States should 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 contained in records affected by this Section for a period longer than 25 years from the date of their creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this Section.

AID Comment: General comment on Section 3.4: Should not be titled "automatic declassification," since there are exceptions, and exceptions require review.

RATIONALE: N/A.

USN (JAG) Comment: General comment on Section 3.4: Navy action must commence immediately in order to meet with the time limits imposed in this section.

RATIONALE: N/A.

CIA Comment: General comment on Section 3.4: This provision conservatively will cost the agency in excess of \$60 million over 5 years. Without Administration support for additional funding, agency will be required to divert resources from intelligence programs.

RATIONALE: N/A.

TREASURY Comment: General comment on Section 3.4: Senior policy officials should review the decision to reduce the automatic declassification provision from 40 years to 25 years, as well as the decision to include foreign government information within the reach of this section.

RATIONALE: N/A.

COMMERCE Comment: General comment on Section 3.4: The Order requires agencies to develop a plan of action to meet the requirements of this

section within 180 days of its effective date. To develop such a plan, agencies will need implementing instructions either from ISOO or the Security Policy Board, which are unlikely to be available in time to permit agencies to meet the 180 day deadline.

RATIONALE: N/A.

NARA Comment: General comment on Section 3.4: The breadth of the exemptions in the current draft has destroyed the concept of automatic declassification. The exemptions will require far too much labor intensive page by page review. The effect will be no significant change from the current system. NARA will notify agencies that they must advise it of file series exempted as authorized in paragraph 3.4(c) and specific information exempted as authorized in paragraph 3.4(d).

RATIONALE: N/A.

DOD Comment: General comment on Section 3.4. The declassification provisions of the draft are complex and not conducive to efficient implementation. DOD conservatively estimates \$215.5 millions as the 5-year cost of implementing the automatic declassification provisions. This is for departmental non-intelligence activities. . . . Accordingly, DOD intends to seek Security Policy Board consideration of the declassification provisions of

the new order and requests that the Board develop a more efficient system for the declassification of permanently valuable records. DOD requests that this be done in a year.

RATIONALE: N/A.

DOD Comment: General comment on Section 3.4: Revise all references to 25 years to read 30 years. Make conforming changes throughout the Order.

RATIONALE: The later time frame will be more efficient and will result in the declassification of more information. Moreover, there is less likelihood of review errors leading to damage to the national security.

DOE Comment: Delete all of the current exemptions categories in paragraph 3.4(b) and substitute for them the exemption categories that currently exist in paragraph 1.6(d), the categories for exemption from 10 year automatic declassification.

RATIONALE: Consistency will avoid confusion that could result in the release of classified information.

CIA Comment: Revise paragraph 3.4(b)(1) as follows:

(1) Reveal the identity of a confidential human source, or a human intelligence source, or reveal information about the application of an intelligence source or method;

RATIONALE: The term "confidential human source" requires an expectation of confidentiality on the part of the source. Unlike State Department sources, human intelligence sources may be unwitting or unaware of their status, so that there is no expectation of confidentiality in that respect. Additional language assures their protection.

NRC Comment: Revise paragraph 3.4(b)(2) as follows:

(2) reveal information that would assist in the development or use of weapons of mass destruction, or reveal United States programs to protect nuclear materials;

RATIONALE: As currently written, this exemption does not appear to include protective measures for facilities which possess significant quantities of nuclear material which could be used in weapon production.

DOD Comment: Revise paragraph 3.4(b)(2) as follows:

(2) reveal information that would assist in the development or use of

weapons of mass destruction, or assist in development of a foreign nuclear powered submarine weapon system which adversely would affect the national security;

RATIONALE: The added language is intended to allow for the continued protections of such information including, especially, that associated with nuclear powered submarines.

USN (Naval Reactors) Comment: Revise paragraph 3.4(b)(4) as follows:

(4) reveal information that would impair the application of ~~state of the art~~ currently usable technology within used in a United States weapon system, or assist in development of a foreign weapon system which would adversely impact the United States national security;

RATIONALE: There are a number of technologies that are no longer state of the art, i.e., the latest version, that would assist in the development of weapons systems by foreign countries. The U.S. should be able to protect any technology that is currently usable in a U.S. or foreign weapon system.

FEMA Comment: Revise paragraph 3.4(b)(5) as follows:

(5) reveal actual United States military war plans or national security emergency preparedness plans that remain in effect;

RATIONALE: Vital ongoing national security programs relating to emergency preparedness contain information that is more than 25 years old.

DOD Comment: Revise paragraph 3.4(b)(5) as follows:

(5) reveal actual United States military war or national security emergency preparedness plans that remain in effect;

RATIONALE: The addition is needed to assure that such plans are not inadvertently subjected to premature declassification.

STATE Comment: Revise paragraph 3.4(b)(6) in either of the following two ways, although the first is preferred:

(6) reveal information that would ~~seriously and demonstrably impair relations between the United States and a foreign government~~ damage current diplomatic negotiations or other ongoing official activities of the United States;

or

(6) reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or ongoing diplomatic activities of the United States;

RATIONALE: The exception should not be limited to impairing a bilateral relationship between the U.S. and a foreign government. Important U.S.

foreign policy objectives may, for example, involve information regarding negotiation strategies, anti-terrorism, a non-governmental organization, or international organizations.

ACDA Comment: Revise paragraph 3.4(b)(6) as follows:

(6) reveal information that would seriously and demonstrably ~~impair relations between the United States and a foreign government~~ damage the foreign relations or impede the foreign activities of the United States;

RATIONALE: Same as State's rationale for broadening this provision.

DOD Comment: Revise paragraph 3.4(b)(6) as follows:

(6) reveal foreign government information or information that ~~would~~ seriously and demonstrably would impair relations between the United States and a foreign government;

RATIONALE: The addition is needed to assure that foreign government information is not subjected to premature declassification.

TREASURY Comment: Add a new paragraph 3.4(b)(8), as follows:

(8) reveal information that would impair the ability of United States Government officials to protect the President, Vice President, and other

officials for whom protection services, in the interest of national security, are authorized.

RATIONALE: Despite the passage of time, there is some information related to dwellings or Secret Service systems that remains sensitive beyond 25 years. This fact was recognized in the JFK Assassination Records Collection Act of 1992.

AID Comment: Add a new paragraph 3.4(c), as follows, renumbering subsequent paragraphs and making necessary reference revisions to reflect the new paragraph:

(c) An agency head may appeal the time limit provisions of paragraph (a), above, when extenuating circumstances prevent the agency from completing its review task on time, and where specific information of the type of (b)(1) through (7) is clearly in the unreviewed remnant.

RATIONALE: At a time of Government downsizing, lack of resources or other unforeseen problems may prevent the attainment of the five year goal. Such circumstances should not jeopardize the protection of information that is still sensitive.

STATE Comment: Revise paragraph 3.4(c) to delete the introductory phrase, "No later than the effective date of this Order"

RATIONALE: Since the Executive Order applies also to documents created in the future, dropping the introductory phrase maintains the requirement to notify the President about exempted file series created after the Order becomes effective.

NSC Comment: Revise paragraph 3.4(c) as follows:

(c) No later than the effective date of this Order, an agency head shall notify the President through the ~~National Security Council~~ Assistant to the President for National Security Affairs of any specific file series

RATIONALE: Ensure consistency with the Government's position in Armstrong v. Executive Office of the President that the NSC is not an agency.

CIA Comment: Revise paragraph 3.4(c)(3) as follows:

(3) except for the identity of a confidential human source, or a human intelligence source, a specific date or event for declassification of the information.

RATIONALE: Same as for CIA comment on paragraph 3.4(b)(1), above.

CIA Comment: Revise paragraph 3.4(d) as follows:

(d) At least 180 days before it becomes ~~subject to~~ automatically
declassified ~~ation~~ under this Section, an agency head

RATIONALE: Clarify that an agency has four and a half years under this section to locate exempt information.

TREASURY Comment: Revise paragraph 3.4(d) as follows:

(d) At least 180 days before it information would otherwise becomes subject to automatic declassification under this Section, an agency head

RATIONALE: This allows for sufficient time for responding rather than on the same date as the E.O. goes into effect.

STATE Comment: Revise paragraph 3.4(d) as follows:

(d) ~~At least 180 days before~~ Within 90 days after it becomes subject to automatic declassification under this Section, an agency head

RATIONALE: The current requirement will be difficult to administer and erodes the short period agencies have in which to review millions of documents.

NSC Comment: Revise paragraph 3.4(d)(3) as follows:

... The agency head may appeal such a decision to the President through the National Security Council. Assistant to the President for National Security Affairs.

RATIONALE: Ensure consistency with the Government's position in Armstrong v. Executive Office of the President that the NSC is not an agency.

CIA Comment: Revise paragraph 3.4(d)(3) as follows:

(3) except for the identity of a confidential human source, or a human intelligence source, a specific date or event for declassification of the information. ...

RATIONALE: Same as for CIA comment on paragraph 3.4(b)(1), above.

DOD Comment: Revise paragraph 3.4(e) as follows:

(e) No later than the effective date of this Order, the agency head or senior agency official shall provide the Director of the Information Security Oversight Office with a plan of action for compliance with the requirements of this Section, including the establishment of interim target dates. ~~Each such plan of action shall include the requirement that the agency declassify at least 15 percent of the records affected by this Section no later than one~~

~~year from the effective date of this Order, and similar commitments for subsequent years until the effective date for automatic declassification.~~

RATIONALE: The Department cannot be certain of adequate funding to meet these requirements.

Section 3.5 Systematic Declassification Review.

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

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

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

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

(c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

NARA Comment: General comment on Section 3.5: As NARA interprets the provisions of the section, the agencies are directed to conduct systematic review before accessioning. NARA policy regarding those records accessioned without agency review will be to notify agencies with equity in the records and allow limited time for their review, after which NARA will consider the records declassified.

RATIONALE: N/A.

DOD Comment: General comment on Section 3.5: Change all references to 25 years to read 30 years.

RATIONALE: Adding five years to the declassification time line will (1) result in more material being declassified; (2) lessen the potential for damage to the national security through errors; and (3) conserve limited declassification review resources.

TREASURY Comment: General comment on Section 3.5: Delete the requirement for systematic declassification review by agencies.

RATIONALE: In the absence of existing staff to support this requirement, and the unlikely prospect of acquiring additional staff, it is presumptive to assume such a goal.

DOD Comment: Revise paragraph 3.5(a) as follows:

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

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

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

RATIONALE: Agencies will not be able to perform local and genuinely systematic review of records if, as expected, they are required to change subject area emphasis frequently.

NARA Comment: General Comment on paragraph 3.5(b): Modify the paragraph to reference 44 U.S.C. Sections 2107, 2111 and 2111 note.

RATIONALE: Allows inclusion of other records transferred to the Archives, such as donated historical materials and the Nixon White House Records.

DOD Comment: Revise paragraph 3.5(b) to read:

(b) . . . These records shall be reviewed in accordance with the standards of this Order, its implementing directives, and classification/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 classification/declassification guides.

RATIONALE: Recognizes that original classifiers routinely issue declassification guidance as an integral part of classification guidance.

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 describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;

(2) the information is not exempted from search and review under the Central Intelligence Agency Information Act; 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

(1) the incumbent President;

(2) the incumbent President's White House Staff;

(3) committees, commissions, or boards appointed by the incumbent President; or

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

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

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

(e) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of cryptologic information, and the

Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods. The Archivist shall develop special procedures for the review of information accessioned into the National Archives of the United States.

COMMERCE Comment: Paragraph 3.6(a) refers to "The request," but does not make clear what this "request" is. The paragraph requires clarification.

RATIONALE: Self explanatory.

USN (JAG) Comment: Paragraph 3.6(a)(1) refers to "The request," but there is no antecedent text to explain what request is being referenced. The paragraph requires clarification.

RATIONALE: Self explanatory.

NRC Comment: Paragraph 3.6(a)(1) should include a preamble to define "the request."

RATIONALE: Self explanatory.

DOD Comment: Revise paragraph 3.6(a)(1) as follows:

(1) The request is made by a United States citizen or permanent resident alien, a federal agency, or a State or local government, and describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;

RATIONALE: There is no apparent reason to delete the U.S. citizen (etc.) requirement, and reinstating the language will help preserve an advantage held by U.S. researchers.

USN (JAG) Comment: Paragraph 3.6(b) exempts the President, White House Staff and special Presidential advisors from onerous declassification review requirements imposed on the rest of the Executive Branch in response to FOIA requests. "The rationale for the Presidential exemption, whatever it is, might justify a broader exemption."

RATIONALE: N/A

NARA Comment: General comment on paragraph 3.6(b): Modify this paragraph so that no distinctions are made between the incumbent and former Presidents, consistent with existing policy.

RATIONALE: This change may diminish the rights of a former President to claim privilege, particularly in the case of records subject to the Presidential Records Act.

NSC Comment: Revise paragraph 3.6(b)(4) as follows:

(4) ~~others specifically providing advice and counsel to the incumbent President or acting on behalf of the incumbent President~~ entities within the Executive Office of the President that solely advise and assist the President . . . are exempted

RATIONALE: Ensure consistency with the Government's position in Armstrong v. Executive Office of the President that the NSC is not an agency.

CIA Comment: Revise paragraph 3.6(e) to read:

(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., ~~and~~ and ~~The~~ The Archivist shall develop special procedures for the review of information accessioned into the National Archives of the United States.

RATIONALE: As originally drafted, this paragraph requires the DOD and CIA to consult with affected agencies, but allows the Archivist to develop procedures without consulting the agencies. The provision should require the Archivist to, when drafting procedures, consult with agencies so that they have the opportunity to protect their interests.

DOD Comment: Revise paragraph 3.6(e) as follows:

(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.~~

RATIONALE: The deleted sentence seems unnecessary, and this revision makes this section consistent with similar provisions of paragraph 3.5(c).

Section 3.7 Processing Requests and Reviews.

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, or pursuant to the automatic declassification or systematic review provisions of this Order:

(a) An agency may 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 contain information that was originally classified by another agency, or comes across such documents in the process of the automatic declassification or systematic review provisions of this Order, it shall refer copies of any request and the pertinent documents to the originating agency for processing, and may, after consultation with the originating agency, inform any 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.

NO COMMENTS RECEIVED ON SECTION 3.7.

Section 3.8 Declassification Database.

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

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

(c) Except as otherwise provided by law, all declassified information contained within the database established under paragraph (a), above, shall be available to the public.

USN (JAG) Comment: Delete Section 3.8.

RATIONALE: A Government-wide declassification database will be very expensive and time-consuming. It is difficult to understand imposing this requirement when there does not currently exist a government-wide database for information that was never classified. Participation in the database will consume Navy manpower and financial resources.

NARA Comment: Delete Section 3.8:

RATIONALE: While NARA believes this is a worthwhile endeavor, a study conducted to assess feasibility revealed that the project would require resources that NARA does not have and does not expect to receive in the future.

AID Comment: Revise paragraph 3.8(c) as follows:

(c) Except as otherwise provided by law, all declassified information contained within the database established under paragraph (a), above, shall be available to the public and protected from inadvertent or intentional modification.

RATIONALE: None provided.

Section 4.1 Definitions.

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

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

DOD Comment: Revise paragraph 4.1(c) as follows:

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

RATIONALE: The proposed change will ensure that only authorized persons performing official government business are granted access to classified information.

Section 4.2 General Restrictions on Access.

- (a) A person may have access to classified information provided that:*
 - (1) A determination of trustworthiness has been made by an agency head or the agency head's designee;*
 - (2) the person has signed an approved nondisclosure agreement; and*
 - (3) the person has a need-to-know the information.*
- (b) Classified information shall remain under the control of the originating agency or its successor in function. An agency shall not disclose information originally classified by another agency without its authorization. An official or employee leaving agency service may not remove classified information from the agency's control.*
- (c) Classified information may not be removed from official premises without proper authorization.*
- (d) Authorized dissemination of classified information outside the executive branch shall assure the protection of the information in a manner equivalent to that provided within the executive branch.*
- (e) Consistent with law, directives and regulation, an agency head or senior agency official shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, which collect, create, communicate, compute, disseminate, process, or store classified information have controls that:*
 - (1) Prevent access by unauthorized persons; and*
 - (2) ensure the integrity of the information.*
- (f) Consistent with law, directives and regulation, each agency head or senior agency official shall establish controls to ensure that classified information is*

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

*(g) Consistent with directives issued pursuant to this Order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to United States **Confidential** information, including allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.*

(h) Except as provided by statute or directives issued by the President through the National Security Council, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information originated within that agency. For purposes of this Section, the Department of Defense shall be considered one agency.

TREASURY Comment: Revise paragraph 4.2(a)(1) as follows:

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

(1) A determination of ~~eligibility~~trustworthiness has been made by an agency head or the agency head's designee;

RATIONALE: A determination of trustworthiness is only one of several criteria evaluated by agencies in order to grant access to classified information. Further, the current language is inconsistent with the proposed Executive Order on Access to Classified Information.

DOD Comment: Revise paragraph 4.2(b) as follows:

(b) Classified information shall remain under the control of the originating agency, ~~or its successor in function, or another agency of the U.S.~~

~~Government. An agency shall not disclose information originally classified by another agency without its authorization.~~ An official or employee leaving agency service may not remove classified information from the agency's control.

RATIONALE: This provision would impair the ability of agencies to conduct classified inter-governmental functions. Further, the proposed language is inconsistent with paragraph 4.2(d) and (h).

AID Comment: Revise paragraph 4.2(c) as follows:

Classified information and material may not be removed from official premises without proper authorization, justification, and safeguarding capability, in accordance with implementing directives issued by the Director of the Information Security Oversight Office.

RATIONALE: Authorization given without regard to safeguarding capabilities may lead to a compromise of the information.

CIA Comment: Revise paragraph 4.2(d) as follows:

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

RATIONALE: The sentence needs an actor to provide the assurance that information is properly protected outside the executive branch.

DOD Comment: Substitute the following language in paragraph 4.2(d):

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

RATIONALE: "Authorized dissemination" cannot "assure the protection." The proposed change reverts back to the language contained in E.O 12356.

AID Comment: Add the following language to paragraph 4.2(e).

(3) ensure availability of the information to authorized persons.

RATIONALE: Both the integrity and availability of information is paramount.

DOE Comment: General comment on paragraph 4.2(g).
Strongly support the provision as written.

RATIONALE: N/A.

DEA Comment: General comment on paragraph 4.2(g): Clarify the provision.

RATIONALE: The provision seems to permit less restrictive standards for certain "foreign government information" than those established for Confidential.

DOD Comment: Revise paragraph 4.2(g) as follows:

(g) Consistent with directives issued pursuant to this Order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. Such ~~When adequate to achieve equivalency, these~~ standards may be less restrictive than the safeguarding standards that ~~ordinarily~~ apply to United

States **Confidential** information, ~~including~~. This includes allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.

RATIONALE: None provided.

DOD Comment: Revise paragraph 4.2(h) as follows:

(h) Except as provided by statute or directives issued by the President through the National Security Council, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the other agency determining that the prospective recipient agency has a need-to-know the information and is able to safeguard the information ~~the consent of the originating agency.~~

Notwithstanding, Aan agency head or senior agency official may require that permission be obtained prior to third agency dissemination of ~~waive this requirement for specific information originated within that agency.~~ For purposes of this Section, the Department of Defense shall be considered one agency.

RATIONALE: The proposed changes apply the need-to-know principle and the appropriate safeguarding requirements while permitting application of the third agency rule on a case by case basis.

NSC Comment: Revise paragraph 4.2(h) as follows:

(h) Except as provided by statute or directives issued by the President ~~through the National Security Council~~, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information originated within that agency. For purposes of this Section, the Department of Defense shall be considered one agency.

RATIONALE: Presidential directives are not issued through the National Security Council.

Section 4.3 Distribution Controls.

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

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

NO COMMENTS RECEIVED ON SECTION 4.3.

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. 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. 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; and*
- (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; or*
- (3) the program is required by statute.*

(b) Requirements and limitations.

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

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

(3) Special access programs shall be subject to the oversight program established under Section 5.6(a)(3) of this Order. In addition, the Director of the Information Security Oversight Office 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. An agency head may limit access to a special access program to the Director and no more than one other employee of the Information Security Oversight Office; or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only.

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

(c) Within 180 days after the effective date of this Order, each agency head or principal deputy shall review all existing special access programs under the

agency's jurisdiction. These officials shall terminate any special access programs that do not clearly meet the provisions of this Order. Each existing special access program that an agency head or principal deputy revalidates shall be treated as if it were established on the effective date of this Order.

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

FEMA Comment: Revise paragraph 4.4(a) as follows:

Option 1.

(a) *Establishment of special access programs.* Unless otherwise authorized by the Executive Secretary of the National Security Council, acting on behalf of 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. . . .

or

Option 2.

(a) *Establishment of special access programs.* Unless otherwise authorized by the President, only the Secretaries of State, Defense and Energy, the Director of the Federal Emergency Management Agency, and the Director of Central Intelligence, or the principal deputy of each, may create a special access program. . . .

RATIONALE: FEMA needs the authority to create special access programs in order to adequately protect the agency's emergency preparedness programs.

NASA Comment: Revise paragraph 4.4(a) as follows:

(a) *Establishment of special access programs.* Unless otherwise authorized by the President, only the Secretaries of State, Defense and Energy, the Administrator of the National Aeronautics and Space Administration, and the Director of Central Intelligence, or the principal deputy of each, may create a special access program. . . .

RATIONALE: NASA needs the authority to create special access programs in order to adequately protect time sensitive programs.

DOD Comment: Revise paragraph 4.4(a)(1) as follows:

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

RATIONALE: Allows the creation of special access programs where the threat or vulnerability has not been established; e.g., new technologies that are unknown by hostile intelligence collectors.

DOD Comment: Revise paragraph 4.4(b)(1) as follows:

(1) Special access programs shall be limited to programs in which the

number of persons who will have access ordinarily will be reasonably small and commensurate with the objective of providing enhanced~~extra~~ protection for the information involved.

RATIONALE: The proposed language clarifies that security requirements for special access programs may be enhancements of other requirements, rather than just additional measures.

TREASURY Comment: Revise paragraph 4.4(b)(2) as follows:

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

RATIONALE: To be consistent with Presidential Decision Directive 29.

DOD Comment: Revise paragraph 4.4(b)(4) as follows:

(4) The agency head or principal deputy ~~and the Executive Secretary of the National Security Council or designee~~ shall review annually each special access program to determine whether it continues to meet the requirements of this Order.

RATIONALE: The proposed language is needed to be consistent with responsibilities of approval authorities as described in paragraph 4.4(a).

NSC Comment: Revise paragraph 4.4(b)(4) as follows:

(4) The agency head or principal deputy and the Assistant to the President for National Security Affairs~~Executive Secretary of the National Security Council~~ or designee shall review annually each special access program to determine whether it continues to meet the requirements of this Order.

RATIONALE: Ensure consistency with the Government's position in Armstrong v. Executive Office of the President that the NSC is not an agency.

DOD Comment: Add subparagraph (5) to 4.4(b) as follows:

(5) If requested, the Assistant to the President for National Security Affairs shall be briefed annually on each special access program.

RATIONALE: The proposed language eliminates duplication of effort since the agency head or principle deputy already ensures that all special access programs meet the requirements of the Executive Order.

Section 4.5 Access by Historical Researchers and Former Presidential Appointees.

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

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

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

(1) *Determines in writing that access is consistent with the interest of national security;*

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

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

DOD Comment: Revise Section 4.5 as follows:

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

~~(1) Are engaged in historical research projects; or~~

~~(2) previously have occupied policy-making positions to which they were appointed by the President.~~

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

(1) Determines in writing that access is consistent with the interest of national security; and

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

~~(3) limits the access granted to former presidential appointees to items that the person originated, reviewed, signed, or received while serving as a presidential appointee.~~

(c) Agency historians, consultants, and historians under contract will have access to classified information in accordance with Paragraph 4.2(a) of this Order.

RATIONALE: The proposed change will permit former presidential appointees access to classified information that is equivalent to that of historians.

Section 5.1 Definitions.

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

(b) *"Violation" means:*

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

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

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

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

COMMERCE Comment: Clarify paragraph 5.1(c). (No language provided.)

RATIONALE: Uncertain as to what constitutes an "infraction" without providing examples.

TREASURY Comment: Clarify paragraph 5.1(c).

RATIONALE: A clear definition of infraction is necessary in order to more effectively distinguish it from a "violation." This will avoid inconsistent agency interpretations.

Section 5.2 Policy Direction.

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

(b) The Director of the Information Security Oversight Office shall be responsible for implementing and monitoring the program established under this Order.

CIA Comment: General comment on Section 5.2: The Security Policy Board should be the policy making entity, not ISOO, which would fulfill recommendations of the Joint Security Commission and PDD 29. ISOO would continue to play the oversight role for the Order.

RATIONALE: N/A.

TREASURY Comment: General Comment on Section 5.2: The draft Order conflicts with PDD 29 which establishes the Security Policy Board as the entity responsible for security policy. It recommends that ISOO continue "to lend its expertise in the roles of oversight, monitoring and administration." Also suggests adding a new paragraph to this section acknowledging the responsibilities of the Security Policy Board.

RATIONALE: Self explanatory.

DOD Comment: General Comment on Section 5.2: DOD indicates that during a January 3, 1995, meeting "with many of the key individuals present, it was agreed that the Security Policy Board, which is co-chaired by the Deputy Secretary of Defense, would be included in the draft order. The Board will be responsible for developing policy." DOD further stated that ISOO would remain the oversight entity, but would not make policy.

RATIONALE: Self explanatory.

CIA Comment: Revise paragraph 5.2(b) as follows:

(b) ~~The Director of the Information Security Oversight Office~~ Security Policy Board shall be responsible for formulating and implementing ~~and monitoring~~ security policy for the program established under this Order.

RATIONALE: The new language acknowledges the role of the Security Policy Board.

CIA Comment: Revise paragraph 5.2(b) as follows:

~~(b)~~(c) The Director of the Information Security Oversight Office shall be responsible for ~~implementing and monitoring~~ and oversight of the program established under this Order.

RATIONALE: Recognizes ISOO's role in classification management and oversight under the Order.

Section 5.3 Information Security Oversight Office.

(a) *There is established an Information Security Oversight Office.*
(1) *Remainder Reserved.*

(b) *The Director shall:*

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

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

(3) review agency implementing regulations and agency guides for systematic declassification review. The Director shall require any regulation or guide to be changed if inconsistent with this Order or its implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation or guide shall remain in effect pending a prompt decision on the appeal;

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

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

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

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

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

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

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

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

TREASURY Comment: General comment on Section 5.3: Change paragraph 5.3(b)(1) and (2) and 5.3(c) to address the responsibilities of the Security Policy Board under PDD 29.

RATIONALE: N/A.

DEA Comment: General comment on Section 5.3: Could not properly assess section 5.3 because 5.3(a)(1) is reserved.

RATIONALE: N/A.

DOD Comment: General comment on Section 5.3: Suggests including the Security Policy Board in this section acknowledging its responsibility to develop policy, as agreed during a "January 23, 1995, meeting of the Intelligence Community Executive Committee."

RATIONALE: N/A.

NSC Comment: Revise paragraph 5.3(b)(1) as follows:

(1) Develop, in consultation with the agencies, and promulgate, subject to the ~~approval of the National Security Council~~ concurrence of the Assistant to the President for National Security Affairs, directives for the implementation of this Order, which shall be binding on the agencies;

RATIONALE: Ensure consistency with the Government's position in Armstrong v. Executive Office of the President that the NSC is not an agency.

NSC Comment: Revise paragraph 5.3(b)(3) as follows:

(3) review agency implementing regulations and agency guides for systematic declassification review. The Director shall require any regulation or guide to be changed if inconsistent with this Order or its implementing directives. Any such decision by the Director may be appealed to the ~~National Security Council~~ President through the Assistant to the President for National Security Affairs. The agency regulation or guide shall remain in effect pending a prompt decision on the appeal;

RATIONALE: Ensure consistency with the Government's position in Armstrong v. Executive Office of the President that the NSC is not an agency.

NRC Comment: Revise paragraph 5.3(b)(4) as follows:

(4) have the authority to conduct on-site reviews of each agency's program established under this Order, and to require of each agency, those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the

affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the National Security Council within 60 days of the Director's request for access. Access shall be denied pending a prompt decision by the National Security Council; The Director of ISOO shall report any violations of this Order or its implementing directives to the affected agency head or to the senior agency official so that corrective action, if appropriate, may be taken. Any such report pertaining to the implementation of this Executive Order by a contractor, licensee, certificate holder, or grantee shall be directed to the agency that is exercising operational oversight over the contractor, licensee, certificate holder, or grantee.

RATIONALE: The additional language makes this section consistent with E.O. 12829, National Industrial Security Program.

NSC Comment: Revise paragraph 5.3(b)(4) as follows:

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

Security Affairs within 60 days of the Director's request for access. Access shall be denied pending a prompt decision ~~by the National Security Council~~;

RATIONALE: Ensure consistency with the Government's position in Armstrong v. Executive Office of the President that the NSC is not an agency.

TREASURY Comment: Revise paragraph 5.3(b)(7) as follows:

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

RATIONALE: Acknowledges role of Security Policy Board.

NSC Comment: Revise paragraph 5.3(b)(8) as follows:

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

RATIONALE: Ensure consistency with the Government's position in Armstrong v. Executive Office of the President that the NSC is not an agency.

TREASURY Comment: Revise paragraph 5.3(b)(9) as follows:

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

RATIONALE: None given.

CIA Comment: Revise paragraph 5.3(c) as follows:

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

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

RATIONALE: Acknowledges the Security Policy Board's responsibility in
formulating security policy, while recognizing ISOO's major role in
classification management and oversight under the Order.

Section 5.4 Interagency Security Classification Appeals Panel.

(a) Establishment and Administration.

*(1) There is established an Interagency Security Classification Appeals
Panel ("Panel"). The Secretaries of State and Defense, the Attorney General,
the Director of Central Intelligence, the Archivist of the United States, and the*

Executive Secretary of the National Security Council shall each appoint a senior level representative to serve as a member of the Panel. The President shall designate the Chairman of the Panel.

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

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

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

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

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

(b) Functions. The Panel shall:

(1) Decide on appeals by persons who have filed classification challenges under Section 1.9 of this Order;

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

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

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

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

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

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

(d) Agency heads will cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. An agency head may appeal a decision of the Panel to the President through the National Security Council.

DOD Comment: General comment on Sections 5.4 and 5.5:

Delete requirement for an Interagency Security Classification Appeals Panel and Information Security Policy Advisory Council.

RATIONALE: These entities represent additional resource impact. Every consideration should be given to elimination of structures having similar responsibilities.

NRC Comment: General comment on Section 5.4: The ISCAP should include representation beyond the diplomatic, defense and intelligence communities.

RATIONALE: Provides a broader government security perspective to Panel activities.

NSC Comment: Revise paragraph 5.4(a)(1) as follows:

(1) There is established an Interagency Security Classification Appeals Panel ("Panel"). The Secretaries of State and Defense, the Attorney General,

the Director of Central Intelligence, the Archivist of the United States, and the ~~Executive Secretary~~ Assistant to the President for National Security Affairs ~~Council~~ shall each appoint a senior level representative to serve as a member of the Panel. The President shall designate the Chairman of the Panel.

RATIONALE: Ensure consistency with the Government's position in Armstrong v. Executive Office of the President that the NSC is not an agency.

DOE Comment: Revise paragraph 5.4(a)(1) as follows:

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

RATIONALE: The Department of Energy is not designated as a member of this panel. DOE's broad experience in classification matters, including not only policy and procedures under the Executive Order, but also for Restricted Data and Formerly Restricted Data under the Atomic Energy Act, warrants its participation.

CIA Comment: Revise paragraph 5.4(c)(1) as follows:

(1) The Panel will consider appeals only on actions in which the appellant has exhausted his or her administrative remedies within the responsible agency, the appellant agrees to be bound by the decision of the Panel, the appellant agrees to waive any rights to obtain the information (either directly or by proxy) through the Freedom of Information Act and the Privacy Act, and there is no current action pending on the issue within the federal courts and the information has not been the subject of review by the federal courts or the Panel within the past two years;

RATIONALE: Ensures that individuals who exercise this appeal right do not use it to subvert established FOIA and Privacy Act administrative processes within CIA and other intelligence agencies. The requester should not be able to return to the agency for another round of review after the Panel has denied a request.

TREASURY Comment: Clarify paragraph 5.4(c)(1), the role of the Interagency Security Classification Appeals Panel.

RATIONALE: As written, the Panel will consider appeals of mandatory declassification cases in which there is no current action pending on the issue

in the federal courts. Is appeal to the Panel in lieu of appeal to a Federal Court, or can an unsuccessful appellate appeal the Panel's denial to a federal court? It is not clear that an Executive Order can deny an appellant recourse to the courts.

NSC Comment: Revise paragraph 5.4(c)(3) as follows:

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

RATIONALE: Ensure consistency with the Government's position in Armstrong v. Executive Office of the President that the NSC is not an agency.

NSC Comment: Revise paragraph 5.4(d) as follows:

(d) Agency heads will cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. An agency head may appeal a decision of the Panel to the President through the Assistant to the President for National Security Affairs~~Council~~.

RATIONALE: Ensure consistency with the Government's position in Armstrong v. Executive Office of the President that the NSC is not an agency.

Section 5.5 Information Security Policy Advisory Council.

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

(b) Functions. The Council shall:

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

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

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

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

(d) Administration.

(1) Each Council member may be compensated at a rate of pay not to exceed the daily equivalent of the annual rate of basic pay in effect for grade GS-18 of the general schedule under section 5376 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Council.

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

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

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

AID Comment: General comment on Section 5.5: The Council should not be able to establish its own length of service.

RATIONALE: There needs to be external oversight and approval.

TREASURY Comment: General comment on Section 5.4 and 5.5: Merge the functions of the Security Policy Advisory Board and the Information Security Policy Advisory Council.

RATIONALE: There is no clear distinction between either group. The change would avoid duplication of functions. Overall policy should be as prescribed by the Security Policy Board.

Section 5.6 General Responsibilities.

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

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

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

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

(A) Overseeing the agency's program established under this Order, provided, an agency head may designate a separate official to oversee special access programs authorized under this Order. This official shall provide a full accounting of the agency's special access programs at least annually;

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

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

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

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

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

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

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

(b) The Inspector General of each agency shall conduct periodic evaluations of the implementation and administration of the program established under this Order. To the extent permitted by statute, those portions of each Inspector General's reports that deal with this program shall be provided to the agency head and the Director of the Information Security Oversight Office.

STATE Comment: Revise paragraph 5.6(a)(2) as follows:

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

RATIONALE: The Department of State is committed to greater openness. However, the Department has limited resources, and no assurances exist that sufficient funds will be made available to the Department.

NRC Comment: Revise paragraph 5.6(a)(3)(G) as follows:

(G) assuring that the performance ~~of contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of:~~ (i) ~~Original classification authorities;~~ (ii) ~~security managers or security specialists;~~ and (iii) ~~all other personnel whose duties significantly involve the creation or handling of classified information;~~ and (1) those with original classification authority, (2) security managers or specialists, and (3) personnel with significant involvement in the creating or handling of classified information reflect consideration of such duties and responsibilities. This may be in the form of a specific critical element, sub-element, or other appropriate reference; and

RATIONALE: Because of the initiatives discussed in the Vice President's report, "Creating A Government That Works Better & Costs Less," it seems appropriate to write language broadly enough to fit any performance appraisal system that may replace the present one.

AID Comment: Delete paragraph 5.6(a)(3)(G).

RATIONALE: The number of personnel affected could be extremely large in some agencies, and it would be difficult to enforce the inclusion of the element where required. AID has been successful in sustaining disciplinary actions, without benefit of a mandatory security element. Misconduct regarding security is already covered in draft paragraph 5.7(c).

COMMERCE Comment: Revise paragraph 5.6(a)(3)(G) to make the agency head, not the senior official, responsible.

RATIONALE: To dictate via executive order the substance and requirements of performance plans limits managerial prerogatives, runs against efforts to empower employees, and establishes a dangerous precedent. The focus and emphasis on classification and declassification of information is more suitably left to the discretion of individual units and agencies. A program

review such as that formerly employed by the Information Security Oversight Office seems likely to be a more effective means for focusing attention on the issue.

FEMA Comment: General comment on paragraph 5.6(a)(3)(H):

FEMA is concerned regarding the requirement for "accounting for the costs associated with the implementation of this order." Specific guidance which allows this Agency to meet this objective, within existing resources, is required before we could agree to this clause.

RATIONALE: N/A.

ISOO Comment: Add a new paragraph 5.6(a)(3)(I) as follows:

(I) assigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint or suggestion arising out of this Order that pertains to classified information that originated in a component of the agency which no longer exists and for which there is no clearly designated successor in function.

RATIONALE: Many public requests, etc., that pertain to older information within an agency go unanswered for many months because the originating

office no longer exists and no other office wants to take responsibility. This provision should rectify in a simple way what has sometimes caused significant embarrassment for the executive branch.

NRC (IG) Comment: General Comment on paragraph 5.6(b):

5 U.S.C. Appendix 3, 4(a)(1) of the Inspector General Act authorizes IGs to review agency's compliance with programs and make recommendations on their economy and efficiency, and to prevent fraud, waste, and abuse. Thus, even without paragraph 5.6(b), IGs are empowered to review agency's compliance with respect to classification programs.

RATIONALE: N/A.

USDA (IG) Comment: General comment on paragraph 5.6(b): USDA IG objects to this requirement.

RATIONALE: USDA IG is concerned about lack of resources to conduct this function.

EPA (IG) Comment: General comment on paragraph 5.6(b):

EPA objects to paragraph 5.6(b).

RATIONALE: We believe the audits conducted by Offices of the Inspector General should result from an annual planning process, which involves risk assessments of agency programs and activities. In this way, limited resources can be devoted to areas with the greatest risk of fraud, waste, and abuse.

COMMERCE Comment: Revise paragraph 5.6(b) as follows:

(b) ~~The Inspector General of e~~ Each agency shall conduct periodic evaluations of the implementation and administration of the program established under this Order. To the extent permitted by statute, those portions of each Inspector General's reports that deal with this program shall be provided to the agency head and the Director of the Information Security Oversight Office.

RATIONALE: This requirement assumes that a significant knowledge base regarding matters related to information classification and declassification already exists within the various agency Inspector General offices, which may not be true. Further, it is felt that the agency head should make such determinations.

NASA (IG) Comment: Revise paragraph 5.6(b) as follows:

(b) The Inspector General of each agency shall consider ~~conduct~~ periodic evaluations of the implementation and administration of the program established under this Order during the IG planning process. To the extent permitted by statute, those portions of each Inspector General's reports that deal with this program shall be provided to the agency head and the Director of the Information Security Oversight Office.

RATIONALE: This language removes the mandate to conduct such reviews, and gives the IGs the flexibility to conduct the reviews on this program only as needed.

HHS (IG) Comment: Revise paragraph 5.6(b) such that the reporting requirement not apply to this Department or, at a minimum, that we be afforded the flexibility to determine whether to conduct the reviews.

RATIONALE: HHS is minimally involved in classified matters, and has only a very small amount of classified information. Therefore, competing demands within the HHS would take a higher priority.

Section 5.7 Sanctions.

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

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

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

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

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

(4) contravene any other provision of this Order or its implementing directives.

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

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

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

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

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

TREASURY Comment: Revise paragraph 5.7(a) as follows:

(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.

RATIONALE: This will ensure consistency in that policy comes from the Security Policy Board.

NRC Comment: Revise paragraph 5.7(b) as follows:

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

RATIONALE: Section 5.7 provides no sanctions for historical researchers and former Presidential Appointees as well as certificate holders under the Energy Policy Act of 1992 who are authorized access to classified information under Section 4.5, and who may violate this Order.

STATE Comment: Revise paragraph 5.7(b) as follows:

(b) Anyone in possession of classified information shall be subject to appropriate sanctions. 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:

RATIONALE: This change will make clear that even individuals such as historical researchers and former officials with access to classified information are among those who must follow the provisions of this Executive Order.

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, including the exemptions to the Freedom of Information Act, the Privacy Act, and the National Security Act of 1947.

(d) Executive Order No. 12356 of April 6, 1982, is revoked as of the effective date of this Order.

CIA Comment: Revise paragraph 6.1(a) as follows:

(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, as amended. "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.

RATIONALE: The National Security Act has been amended since 1947.

TREASURY Comment: General Comment: In paragraph 6.1(b), insert reference to the Security Policy Board as also having authority to request interpretation of the Order with respect to any questions.

RATIONALE: Self explanatory.

Section 6.2 Effective Date.

This Order shall become effective 180 days from the date of its issuance.

NO COMMENTS RECEIVED ON SECTION 6.2.

SECURITY POLICY BOARD

Arlington, Virginia 22202

SFB 066-95
29 March 1995

MEMORANDUM FOR: Security Policy Board Members and Observers

FROM: Peter D. Saderholm
Executive Secretary

SUBJECT: Equity Problems with Proposed Language in the
Executive Order on Classified National
Security Information

1. Action Requested: That a call be placed to the White House Chief of Staff in an attempt to reverse the proposed effort by the Office of Management and Budget (OMB) to exclude the Security Policy Board from having a policy role in classification management.

2. Background: As you may recall, during the 10 February 1995 meeting of the Security Policy Board (Board), we primarily discussed and resolved a number of due process provisions associated with the draft Executive Order (E.O.) on Access to Classified Information. This E.O. is now at the White House and will undergo a short period of public comment. At that same meeting, we discussed the draft E.O. on Classified National Security Information. The Board expressed concern over the exclusive policy roles and responsibilities outlined therein for the Information Security Oversight Office (ISOO). Your position was that this Board established by Presidential Directive should have the responsibility for security policy development including classification management recognizing that ISOO must retain some independent monitoring and oversight role in the process. The National Security Council (NSC) representative at the meeting, Mr. George Tenet, briefed of his intent to narrow the ISOO scope of operation and to meet with me to work out language that would ensure a proper role for the Board in security policy formulation. You then directed that I report the results of the agreement to you.

3. Regrettably, the meeting proposed by the NSC has not occurred despite regular attempts on our part to schedule a meeting. Nevertheless, we have just received proposed E.O. language from the NSC that is represented as having been approved by the OMB, the White House, and the NSC. This

SUBJECT: Equity Problems with Proposed Language in the
Executive Order on Classified National Security
Information

language, which is enclosed, excludes the Board from having any role in the development of classification management policy or security education and training programs. Instead, OMB has assumed the role and delegates the responsibility to ISOO. The Board is relegated to issuing a directive on safeguarding classified information.

4. It is my belief that this proposed language has wide-ranging implications for the Board, none of which are favorable.

5. Recommendation: That you call the White House Chief of Staff to request that the Board be given a responsibility for the development of classification management policy for this nation. In this regard, it should be noted that OMB already sits on the Board. This policy role in no way is designed to diminish the responsibilities of ISOO for oversight and monitoring as clearly outlined in the draft E.O.



Peter D. Saderholm

Attachment

Section 5.2 Program Direction.

and Collectors
of
SPB

(a) The Director of the Office of Management and Budget, in consultation with the Assistant to the President for National Security Affairs, shall issue such directives as are necessary to implement this Order. These directives shall be binding upon the agencies. Directives issued by the Director of the Office of Management and Budget shall establish standards for:

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

(b) The Director of the Office of Management and Budget shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.

(c) The Security Policy Board, established by a Presidential Decision Directive, shall issue a directive on safeguarding classified information. This directive shall pertain to the handling, storage, distribution, transmittal and destruction of and accounting for classified information.

Section 5.3 Information Security Oversight Office

(v) There is established within the Office of Management and Budget an Information Security Oversight Office. The Director of the Office of Management and Budget shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(ii) Under the direction of the Director of the Office of Management and Budget and in consultation with the Assistant to the President for National Security Affairs, the Director of the Information Security Oversight Office shall:

(1) develop directives for the implementation of this order;

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

(3) review and approve agency implementing regulations and agency guides for systematic declassification review prior to their issuance by the agency;

(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 its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the Director of the Office of Management and Budget within 60 days of the request for access. Access shall be denied pending a prompt decision by the Director of the Office of Management and Budget, who shall consult on this decision with the Assistant to the President for National Security Affairs;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend presidential approval through the Director of the Office of Management and Budget;

(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 on the implementation of this order; and

(9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

Talking Points For Security Policy Board Members

1. Action Requested: That a call to the White House Chief of Staff be made to reverse the proposed language in the Executive Order on Classified National Security Information which excludes the Security Policy Board (SPB) from having a policy role in classification management.

2. Background:

- Prior to Presidential Decision Directive-29 (PDD-29) which created the SPB, the Information Security Oversight Office (ISOO) had responsibility for classification management, security training, safeguarding and declassification policy formulation.
- President Clinton's decision to issue PDD-29 established the SPB as the principal mechanism for reviewing and proposing to the National Security Council (NSC) legislative initiatives and executive orders pertaining to U.S. Security policy, procedures and practices.
- The PDD identified 26 U.S. Departments and Agencies, to include the ISOO, for membership in the SPB structure thereby ensuring a collaborative security policy decision making process. The utility of this process has produced the desired results as evidenced in the forthcoming E.O. on Access to Classified Information.
- During the 10 February 1995 SPB meeting, the NSC representative, George Tenet, briefed his intention to narrow the ISOO scope of operation and to meet with the SPB Staff Director, Peter Saderholm, to craft language that would ensure a proper role for the Board in security policy formulation and implementation. Regrettably, the meeting proposed by the NSC has not occurred despite repeated attempts by SPB Staff Director Saderholm to schedule it.
- Notwithstanding the SPB staff's repeated attempts to schedule a meeting, the SPB staff has documented its' concerns with the Order to the NSC in a 27 January 1995 letter and a 23 March 1995 facsimile.

3. Points to Raise and Points Likely To Be Raised by Mr. Panetta:

- **Point to Raise:** Excluding the SPB from classification management policy obfuscates the role and future credibility of the SPB as established by PDD-29.

-- **Likely Disagreement:** I don't see how excluding the SPB from classification management policy will obfuscate the role and future credibility of the SPB.

-- **Recommended Response:** The SPB, as established by PDD-29, is the principal mechanism for coordinating, formulating and evaluating security policy. Classification management is, along with personnel security, a cornerstone of our security system. Excluding the SPB from the decision making process for classification management will reduce the SPB ability to affect positive change pertinent to security costs, risk management and threat appropriate measures

- **Point to Raise:** It is significant to recognize that classification management is the root of all security issues. Without classified information we have little need for security. It is both the beginning and the end. To exclude the SPB, or, for that matter, the NSC from involvement in the classification and declassification of Nation Security information does not appear to be good business.

-- **Likely Disagreement:** I don't discount the significance of the role of classification management in the sphere of overall security policy. My concern is that for too long security policy, especially classification management policy, has operated in a vacuum with little or no regard to current political, economical and military realities.

-- **Recommended Response:** I can appreciate your concerns and can assure you that the SPB apparatus is fully mindful of those concerns. In fact, PDD-29, which establishes the SPB, includes among its principles that our security policies must be both cost effective and flexible to facilitate change and realistically match our countermeasures to the threats we face. It also establishes an Presidential Advisory Board charged with reviewing proposed policy for compliance with these principles. In addition, the membership of the SPB has sufficient breadth and political sensitivity to address these issues.

- **Point to Raise:** The exclusion of the SPB from a classification management role sets the stage for the elimination of one-half of the SPB committees and structure. Namely, the committees for Classification Management, Training & Professional Development and Information Systems Security would, at best, be relegated to an advisory role.

-- **Likely Disagreement:** So what is wrong with the SPB having an advisory role? As you point out, the PDD calls for an Advisory Board?

-- **Recommended Response:** The PDD does have provision for an Advisory Board but this is meant to provide for a non-government perspective of our security policies, practices and procedures. I agree, there is nothing wrong with the SPB having an advisory role but that role is meant to supplement not supplant the policy making function of the SPB.

- **Point to Raise:** The Order authorizes the Office of Management and Budget to issue security policy directives binding upon all government agencies thereby relegating the role of the NSC to a consultant status despite the fact we are discussing classified National Security Information.

-- **Likely Disagreement:** This is precisely what this administration wants to do in terms of furthering openness in government.

-- **Recommended Response:** If you really want the true aims of the administration to be implemented, doesn't it make more sense to have a Board of senior political appointees, like the SPB, responsible for this activity? The Board, with its divergent viewpoints present at the table, will be far more likely to implement actual administration policy than a single bureaucratic organization. Therefore, it makes far more sense to have ISOO report to the SPB.

- **Point to Raise:** The failure of the Order to allow input of the preponderance of U.S. Departments and Agencies in the development of classification management policy substantially lessens the likelihood of flexible policies which realistically match the threats we face and provide the security we need at a price we can afford.

- Likely Disagreement: Why can't OMB and ISOO develop such policy?

--Recommended Response: I am not saying they can't. I am saying the probability of timely success is substantially greater when you include an all-inclusive group that has a substantial interest in the outcome and that operates with a decision driven process and has the programmatic responsibility to operate securely at lower cost.

- **Point to Raise:** Establishing an SPB was a recommendation of the Joint Security Commission and is the President's solution for security policy formulation, evaluation and implementation. It evolved from a comprehensive review of security policies and practices in the U.S. government. The proposed E.O., crafted before the creation of the SPB, does not fully capitalize on the inherent value of an all-inclusive policy making body. I am unsure if OMB has an appreciation for what the President is trying to achieve with the SPB

- Disagreement: I can just as easily envision OMB seeking input from all affected departments and agencies prior to issuing policy directives. Besides, the wording of the proposed E.O. calls for OMB to consult with the NSC.

- Recommended Response: I can understand your vision but would remind you that OMB along with ISOO are members of the SPB structure and therefore, in that capacity, already have a substantial role in security policy making. Our vision is an all inclusive body that can produce an E.O. on Access to Classified Information (or on any subject) in a short time frame and with broad support.

- **Point to Raise:** The role of ISOO in overseeing and monitoring the U.S. government's classification management policy is not an issue. Nor are the provisions for declassification in the proposed E.O. We support this new philosophy and the ISOO management of the process.

4. Action Requested: That you call the White House Chief of Staff and urge the Chief of Staff to modify the E.O. language to reflect the classification policy-making role of the SPB.

SECURITY POLICY BOARD

Arlington, Virginia 22202

SPB 005-95
9 January 1995

MEMORANDUM FOR: Assistant Secretary of Defense
(Intelligence and Security)
Executive Director for Intelligence
Community Affairs

FROM: Peter D. Saderholm
Director, Security Policy Board Staff

SUBJECT: Final Coordination of the Draft Executive
Order on Classified National Security
Information

1. Subject draft Executive Order (E.O.), dated 17 March 1994, has been sent to the Office of Management and Budget (OMB) for final coordination. Indications are that it will be distributed for the final 60 day coordination period this week.

2. Our review to date reveals that the draft E.O. does not enjoy wide support within the Federal community. Essentially, it is an E.O. on declassification and it's cost and resource implications in this regard are substantial. Meanwhile, almost no emphasis is placed on ensuring the actual process of initial classification is being conducted in an efficient and effective manner. In summary, it emphasizes reacting to all the information that is classified rather than devoting resources toward the reduction of the amount of information that is classified in the first place. This puts the government in a lose, lose situation as the classification of documents, information, equipment, and processes is not performed by security personnel. Yet, the act of classification is the prime multiplier of security costs at a time when security funding is being substantially reduced.

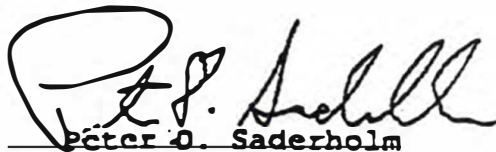
3. A means exists to allow the draft E.O. to be instituted on schedule while, at the same time, allowing for continuing review, update, and modification to achieve greater cost efficiency and a better balance to classification management within the Federal government. The solution is to establish the Security Policy Board (SPB) as the policy issuance authority for classification management

SUBJECT: Final Coordination of the Draft E.O. on Classified
National Security Information

vice the Information Security Oversight Office (ISOO). With the SPB responsible for classification management policy, our nation's policy in this regard can evolve as warranted by established needs and priorities. ISOO can then devote its minimal resources toward facilitating and overseeing the classification and declassification efforts of our government. Moreover, operating under the SPB policy structure will afford ISOO the opportunity to benefit from and help direct the considerable resources the SPB organizations have in the areas of training and professional development, as well as other disciplines needed to improve the Government's security programs. This team approach would finally enable the security community to be proactive in the areas of classification and declassification.

4. The draft E.O. has been pending in excess of two years and the administration is eager to enact it. Also, the OMB coordination period of 60 days is minimal. What is needed is a focused effort on behalf of the government to surgically amend the E.O. so that the process of classification management can be responsive to the new order that exists in this country without completely scuttling the administration's draft. Accordingly, it is proposed that the co-chairs of the SPB direct the members of the Security Policy Forum to develop a consolidated response to OMB on the draft E.O. It is believed a consolidated input would likely have more impact than a series of individual department and agency memoranda. A proposed decision memorandum to this effect for the co-chairs is at the Attachment.

5. I would be happy to discuss this issue with you or your staff at their convenience.



Peter O. Saderholm

Attachment