

Memorandum



Subject

Comments on Draft Executive Order Entitled
"Classified National Security Information"

Date

February 10, 1995

To

Mac Reed
Office of Management and
Budget

From

 Rosemary Hart
Senior Counsel
Office of Legal Counsel

I have marked with the comments of the Department of Justice a copy of the draft Executive Order entitled "Classified National Security Information." We have limited our review to legal and technical problems only.

We wish to highlight several comments:

1. Definition of "agency". The government has taken the position in Armstrong v. Executive Office of the President, No. 89-142, D.D.C., that because the NSC's sole function is to advise and assist the President in the implementation of his national security responsibilities, the NSC is not an "agency" within the meaning of the FOIA definition. If it is the intent of this order to make the NSC subject to its requirements, and in order to be consistent with our litigating position, we suggest that section 1.1(i) be revised to incorporate the definition of agency contained in 5 U.S.C. § 105. We believe that the more inclusive definition is preferable because it covers all establishments within the Executive Office of the President whereas the definition in § 552(f) does not cover all such establishments.

In addition, one of the tests for whether an entity is solely an "advise and assist" entity is whether it exercises any authority independent of the President. The Department has argued that the various Executive Orders that assign certain responsibilities to the NSC do not give it independent authority. For some existing orders this is a bit of an uphill battle. In this draft, there are many provisions that use the formula "to the President through the NSC," a formulation that is consistent with our position that NSC has no independent authority. (See e.g. §3.4(d)(3), 4.2(h), 5.3(b)(8); 5.4(d).) However, there are also many provisions that seem to assign NSC a more "independent" role even though ultimately it will exercise that authority on behalf of the President. (See e.g., §3.2(c); 5.2(a); 5.3(b) -- this is particularly a problem given the language for NSC approval and the binding nature of the directives intended; 5.3(b)(3) and (4).) We would suggest that all provisions use the formulation of "the President through the

National Security Council."

2. Judicial review. We believe that the provisions that explicitly state they do not amplify or modify the substantive criteria for classification and create substantive or procedural rights that are judicially enforceable are intended to be in the disjunctive and, therefore, "or" should replace "and" in sections 1.2(b) and 3.2(b).

In addition, there are provisions that provide for administrative appeals or procedures that leave open the possibility that judicial review may be available because the proviso is not specifically included with that section. To preclude the unintended possibility of judicial review, we recommend keeping the provisos in the sections in which they are currently found and then adding a general proviso at the end, something to the effect of "In addition to the specific provisos contained in sections X and X, nothing in this order amplifies or modifies the substantive criteria, etc."

3. Exemptions. In section 3.6(A)(3), concerning exempting material that has been reviewed within the past 2 years: We suggest that the exemption be expanded to include material that was reviewed more than two years ago for litigation that is still pending.

4. Inspector General authority. The addition of the word "agency's" in line two of section 5.6 (b) clarifies that an agency's Inspector General will be conducting evaluations only within his or her own agency.

5. Appeals Panel. Suggested revisions to section 5.4 pertaining to the Interagency Security Classification Appeals Panel seek to clarify which responsibilities are properly categorized as rules and procedures to be established in the by-laws (which, according to section 5.4(c), are to establish rules and procedures dealing with the acceptance, consideration and issuance of decisions on appeals) and which are other, more general functions of the Panel that are to be established by the President.

In addition to the above comments, we have noted several parts of the draft Order that we find vague or unclear and offered clarifying language. Please feel free to call me at 514-2027 if you wish to discuss any of our questions or proposed changes.

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 ^{of} 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 ^{the} laws of the United States of America, it is hereby ordered as follows:

center
Part 1

Original Classification

Section 1.1 Definitions. *For purposes of this order:*

~~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.

l.c.

(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).

105

(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.

l.c.
l.c.

(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.

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 ^{is} classifying 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 ^{classification authority} 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~~ or
- (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.

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.

No bold
(see
current
EO)

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

underline, No italics 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.

no bold (2) ["]Top Secret["] original classification authority may be delegated only by the President[^] ^{by ^}or an agency head or official designated pursuant to paragraph (a)(2), above.

l.c.

(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. l.c.

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

(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 l.c. l.c.

whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

Section 1.5 Classification Categories.

Information may not be considered for classification unless it concerns:

(a) ~~M~~ilitary plans, weapons, or operations;

l.c.

(b) ~~F~~oreign government information;

l.c.

(c) ~~I~~ntelligence activities (including special activities), intelligence sources or methods, or cryptology;

l.c.

(d) ~~F~~oreign relations or foreign activities of the United States, [including confidential sources];

l.c.

(e) ~~S~~cientific, technological, or economic matters relating to the national security;

It is unclear what additional category is described by "including confidential sources". What is the intent here? Is "confidential sources" a sub-category of the other 2 categories of foreign relations or foreign activities?

Not that in the definition section, all 3 words are capitalized.

(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.

lc.

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

this term is used here for the first time, but isn't defined until § 3.1(b). (pg. 20). maybe we should ~~not~~ define in section 1's definition or add cross-reference to 3.1(b) definition ("as defined in...")

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. l.c.

(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; l.c.

(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. l.c.

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; l.c.
l.c.
l.c.

(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);

l.c.
l.c. l.

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

l.c.

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

l.c.

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

l.c. l.

(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.

l.c.

l.c.

l.c.

1
of the license
granted herein.

Vague
need
refinement
e.g. as suggested

Isn't marking the same as marking?
"marking designations" - what's the difference?

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

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

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

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

Section 1.8 *Classification Prohibitions and Limitations.*

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

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

protection in the interest of national security.

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

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

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. § 552) or the Privacy Act of 1974 (5 U.S.C. § 552a), or the mandatory review provisions of Section 3.6 of this Order 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

l.c. k
l.c.

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.

l.c. l.c.

(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.

*l.c.
l.c.*

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

l.c.

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:

- 4 (1) individuals are not subject to retribution for bringing such actions; ✓
4 (2) an opportunity is provided for review by an impartial official or panel; ✓
4 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. ✓ ✓

l.c.
l.c.

Part 2

Derivative Classification

Section 2.1 Definitions. For purposes of this order:

~~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

delete.
unnecessary

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 ^{g that} ~~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.

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) ~~Ob~~serve and respect original classification decisions; and

l.c.

(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: ^{add space} (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.

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~~.

l.c.

(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. *l.c.*

Part 3

Declassification and Downgrading

Section 3.1 Definitions. *For purposes of this order:*

~~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. *l.c.*

(c) "Declassification authority" means:

(1) The official who authorized the original classification, if that official is still serving in the same position; *l.c.*

(2) the originator's ^{classification authority'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. *l.c. l.c.*

(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 ^("Archivist") 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.

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. l.c.

(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 l.c.

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:

l.c.

- (1) Amplify or modify the substantive criteria or procedures for classification; ~~and~~ *or*
- (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 President

l.c.

through the National Security Council. The information shall remain classified pending a prompt decision on the appeal.

(see to written comment)

(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.

l.c.

l.c.

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.

l.c.

(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.

l.c.

(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.

l.c.

l.c.

(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

of the United States ("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 ^{subsection} 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.~~ ^{l.c. d.c.}

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. ^{l.c.}

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

- (1) ~~R~~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 ~~O~~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; l.c.
- (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 ^{classified information?} 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:

l.c.

- (1) ~~A~~ description of the information; should be
- (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
- l.c.

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 ^{delete; colloquial} of action for compliance with the requirements of this Section, including the establishment of interim target dates. Each such plan ^{delete} 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.

Section 3.5 Systematic Declassification Review.

(a) Each agency that has originated classified information under this Order l.c. 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 l.c. Order. Agencies shall prioritize the systematic review of records based upon: l.c.

(1) Recommendations of the Information Security Policy Advisory l.c. Council, established in Section 5.5 of this Order, on specific subject areas for l.c. l.c. 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 l.c. 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

del.
not in the
dictionary

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. l.c.

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

Section 3.6 *Mandatory Declassification Review.*

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

(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.

or the information is the subject of pending litigation

(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. l.c.

(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. l.c.

(e) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of cryptologic information, and the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods. The Archivist shall develop special procedures for the review of information accessioned into the National Archives of the United States.

Section 3.7 *Processing Requests 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:

l.c.
l.c.

(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.

l.c.

(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.

l.c.

l.c.

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.

Part 4

Safeguarding

Section 4.1 *Definitions.* For purposes of this order:

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

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

Section 4.2 *General Restrictions on Access.*

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

- (1) ~~A~~ determination of trustworthiness has been made by an agency head or the agency head's designee; *l.c.*
- (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, *that* ~~which~~ collect, create, communicate, compute, disseminate, process, or store classified information have controls that:

- l.c.*
- (1) ~~P~~revent 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 ~~O~~rders, an agency shall *l.c.* 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.

no bold

(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.

e.c.

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.

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 l. c.
- (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. l.c. l.c.

(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~~. l.c.

(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~~. l.c. l.c. l.c.

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

l.c.

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:

l.c.

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

l.c.

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

l.c.

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

l.c.

(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

l.c.

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

Part 5

Implementation and Review

Section 5.1 *Definitions.*

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

(b) "Violation" means:

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

(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 l.c.

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

(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.

l.c.

Section 5.2 Policy Direction.

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

l.c.

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

l.c.

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 *President, through the* National Security Council, directives for the implementation of this Order, which shall be binding on the agencies;

l.c.

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

l.c.

l.c.

(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;

l.c.

(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;

l.c.

(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;

l.c.

(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;

l.c.

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

l.c.

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

l.c.

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

l.c.

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

Section 5.4 Interagency Security Classification Appeals Panel.

(a) *Establishment and Administration.*

(1) There is established an Interagency Security Classification Appeals Panel ("Panel"). The 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. *from among the Panel members*

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

*check with White House Clerk:
Is this consistent with other Administration EO's and directives?
45*

(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.

✓ l.c.

l.c.

l.c. l.c.

l.c. l.c.

(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;

l.c.

✓

✓

(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.

place in (d) below; it's not a function of the by-laws.

(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.

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

shouldn't this be listed as a separate function in paragraph (b)?
It has nothing to do with "accepting, considering & issuing decisions, on appeals," which (c) identifies as the function of the by-laws.

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. [?]

shall establish

to set
forth its rules
and procedures,
including the

Not consistent
w/ § 5.4

(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;

l.c.

l.c.

(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.

Section 5.6 *General Responsibilities.*

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

(1) ~~D~~emonstrate personal commitment and commit senior management to the successful implementation of the program established under this ~~O~~der;

l.c.

l.c.

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

l.c.

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

(A) ~~Ø~~overseeing the agency's program established under this ~~Ø~~Order, provided, an agency head may designate a separate official to oversee special access programs authorized under this ~~Ø~~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.

agency's

l.c.

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.

l.c.

(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.

unnecessary
to set
out in
full if
you're just
restating
definitions
of
"violation"
and
"infraction."

Why not
delete and
just say
"commit
a violation
or infraction
as defined
in § 5.1"
?

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

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

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

Part 6

General Provisions

Section 6.1 *General Provisions.*

(a) Nothing in this ~~Order~~ shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act. l.c.

(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. l.c.

(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.

l.c.

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

l.c.

Section 6.2 *Effective Date.*

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