(2) Where it is anticipated that the fees chargeable under this section will amount to more than $25, and the requestor has not indicated in advance a willingness to pay fees as high as are anticipated, the requestor shall be promptly notified of the amount of the anticipated fee or such portion thereof as can readily be estimated. In instances where the estimated fees will greatly exceed $25, an advance deposit may be required. Dispatch of such a notice or request shall suspend the running of the period for response by the NSC Staff until a reply is received from the requestor.

(3) Remittances shall be in the form either of a personal check or bank draft drawn on a bank in the United States, or a postal money order. Remittances shall be made payable to the Treasury of the United States and mailed to the Staff Secretary, National Security Council, Washington, DC 20506.

(4) [Reserved]

(5) A receipt for fees paid will be given only upon request. Refund of fees paid for services actually rendered will not be made.

(6) If a requestor fails to pay within thirty days for services rendered, further action on any other requests submitted by that requestor shall be suspended.

(7) The Staff Secretary, National Security Council may waive all or part of any fee provided for in this section when it is deemed to be in either the interest of the NSC Staff or of the general public.

§2103.33 Downgrading authority.

The Staff Secretary, Staff Counsel, and Director of Freedom of Information of the National Security Council Staff are authorized to downgrade NSC documents, after consultation with the appropriate NSC Staff members.
## CHAPTER XXIV—OFFICE OF SCIENCE AND TECHNOLOGY POLICY

<table>
<thead>
<tr>
<th>Part</th>
<th>Regulations to implement E.O. 12356; Office of Science and Technology Policy information security program</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2400</td>
<td>...........................................................................................................................................</td>
<td>535</td>
</tr>
</tbody>
</table>
PART 2400—REGULATIONS TO IMPLEMENT E.O. 12356; OFFICE OF SCIENCE AND TECHNOLOGY POLICY INFORMATION SECURITY PROGRAM

Subpart A—General Provisions
Sec. 2400.1 Authority.
2400.2 Purpose.
2400.3 Applicability.
2400.4 Atomic Energy Material.

Subpart B—Original Classification
2400.5 Basic policy.
2400.6 Classification levels.
2400.7 Original classification authority.
2400.8 Limitations on delegation of original classification authority.
2400.9 Classification requirements.
2400.10 Presumption of damage.
2400.11 Duration of classification.
2400.12 Identification and markings.
2400.13 Limitations on classification.

Subpart C—Derivative Classification
2400.14 Use of derivative classification.
2400.15 Classification guides.
2400.16 Derivative classification markings.

Subpart D—Declassification and Downgrading
2400.17 Policy.
2400.18 Declassification and downgrading authority.
2400.19 Declassification by the Director of the Information Security Oversight Office.
2400.20 Systematic review for declassification.
2400.21 Mandatory review for declassification.
2400.22 Freedom of Information Act and Privacy Act requests.
2400.23 Prohibition.
2400.24 Downgrading.

Subpart E—Safeguarding
2400.25 Access.
2400.26 Access by historical researchers and former Presidential appointees.
2400.27 Storage of classification information.
2400.28 Dissemination of classified information.
2400.29 Accountability and control.
2400.30 Reproduction of classified information.
2400.31 Destruction of classified information.
2400.32 Transmittal of classified information.
2400.33 Loss or possible compromise.

Subpart F—Foreign Government Information
2400.34 Classification.
2400.35 Duration of classification.
2400.36 Declassification.
2400.37 Mandatory review.
2400.38 Protection of foreign government information.

Subpart G—Security Education
2400.39 Responsibility and objectives.

Subpart H—Office of Science and Technology Policy Information Security Program Management
2400.40 Responsibility.
2400.41 Office Review Committee.
2400.42 Security Officer.
2400.43 Heads of offices.
2400.44 Custodians.
2400.45 Information Security Program Review.
2400.46 Suggestions or complaints.


Source: 48 FR 10821, Mar. 15, 1983, unless otherwise noted.

Subpart A—General Provisions

§ 2400.1 Authority.

§ 2400.2 Purpose.
The purpose of this Regulation is to ensure, consistent with the authorities of §2400.1 that information of the Office of Science and Technology Policy (OSTP) relating to national security is protected from unauthorized disclosure, but only to the extent and for such period as is necessary to safeguard the national security.
§ 2400.3 Applicability.

This Regulation governs the Office of Science and Technology Policy Information Security Program. In accordance with the provisions of Executive Order 12356 and Directive No. 1 it establishes, for uniform application throughout the Office of Science and Technology Policy, the policies and procedures for the security classification, downgrading, declassification and safeguarding of information that is owned by, produced for or by, or under the control of the Office of Science and Technology Policy.

§ 2400.4 Atomic Energy Material.

Nothing in this Regulation supersedes any requirement made by or under the Atomic Energy act of 1954, as amended. "Restricted Data" and information designated as "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued pursuant thereto by the Department of Energy.

Subpart B—Original Classification

§ 2400.5 Basic policy.

Except as provided in the Atomic Energy Act of 1954, as amended, Executive Order 12356, as implemented by Directive No. 1 and this Regulation, provides the only basis for classifying information. The policy of the Office of Science and Technology Policy is to make available to the public as much information concerning its activities as is possible, consistent with its responsibility to protect the national security. Information may not be classified unless its disclosure reasonably could be expected to cause damage to the national security.

§ 2400.6 Classification levels.

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

(1) “Top Secret” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

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

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

(b) Except as otherwise provided by statute, no other terms shall be used to identify classified information. Markings other than “Top Secret,” “Secret,” and “Confidential,” such as “For Official Use Only,” shall not be used to identify national security information. In addition, no other term or phrase shall be used in conjunction with one of the three authorized classification levels, such as “Secret Sensitive” or “Agency Confidential.” The terms “Top Secret,” “Secret,” and “Confidential” should not be used to identify nonclassified executive branch information.

(c) Unnecessary classification, and classification at a level higher than is necessary shall be scrupulously avoided.

(d) If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified “Confidential” pending a determination by an original classification authority, who shall make this determination within thirty (30) days. If there is reasonable doubt about the appropriate level of classification the originator of the information shall safeguard it at the higher level of classification pending a determination by an original classification authority, who shall make this determination within thirty (30) days. Upon the determination of a need for classification and/or the proper classification level, the information that is classified shall be marked as provided in §2400.12 of this part.

§ 2400.7 Original classification authority.

(a) Authority for original classification of information as Top Secret shall be exercised within OSTP only by the
Office of Science and Technology Policy

§ 2400.9 Classification requirements.

(a) Information may be classified only if it concerns one or more of the categories cited in Executive Order 12356, as subcategorized below, and an official having original classification authority determines that its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security.

(1) Military plans, weapons or operations;

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

(3) Foreign government information;

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

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

(6) Scientific, technological, or economic matters relating to the national security;

(7) United States Government programs for safe-guarding nuclear materials or facilities;

(8) Cryptology;

(9) A confidential source; or

(10) Other categories of information which are related to national security and that require protection against unauthorized disclosure as determined by the Director, Office of Science and Technology Policy. Each such determination shall be reported promptly to the official in OSTP who has appropriate subject matter interest and classification authority with respect to this information. That official shall decide within thirty (30) days whether to classify this information. If the information is not within OSTP’s area of classification responsibility, OSTP shall promptly transmit the information to the responsible agency. 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.

§ 2400.8 Limitations on delegation of original classification authority.

(a) The Director, OSTP is the only official authorized to delegate original classification authority.

(b) Delegations of original classification authority shall be held to an absolute minimum.

(c) Delegations of original classification authority shall be limited to the level of classification required.

(d) Original classification authority shall not be delegated to OSTP personnel who only quote, restate, extract or paraphrase, or summarize classified information or who only apply classification markings derived from source material or as directed by a classification guide.

(e) The Executive Director, OSTP, shall maintain a current listing of persons or positions receiving any delegation of original classification authority. If possible, this listing shall be unclassified.

(f) Original classification authority may not be redelegated.

(g) Exceptional Cases. When an employee, contractor, licensee, or grantee of OSTP 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 these Regulations as provided in §2400.6(d) of this part. The information shall be transmitted promptly as provided in these Regulations to
§ 2400.10

the Director of the Information Security Oversight Office.

(b) Foreign government information need not fall within any other classification category listed in paragraph (a) of this section to be classified.

(c) Certain information which would otherwise be unclassified may require classification when combined or associated with other unclassified or classified information. Classification on this basis shall be fully supported by a written explanation that, at a minimum, shall be maintained with the file or referenced on the record copy of the information.

(d) Information classified in accordance with this section shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information. Following an inadvertent or unauthorized publication or disclosure of information identical or similar to information that has been classified in accordance with Executive Order 12356 or predecessor orders, OSTP, if the agency of primary interest, shall determine the degree of damage to the national security, the need for continued classification, and in coordination with the agency in which the disclosure occurred, what action must be taken to prevent similar occurrences. If the agency of primary interest is other than OSTP, the matter shall be referred to that agency.

§ 2400.11 Duration of classification.

(a) Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified.

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

(c) Information classified under predecessor Executive Orders and marked for declassification review shall remain classified until reviewed for declassification under the provisions of Executive Order 12356.

(d) Information classified under predecessor Executive Orders that does not bear a specific date or event for declassification shall remain classified until reviewed for declassification. The authority to extend the classification of information subject to automatic declassification under predecessor Orders is limited to those officials who have classification authority over the information and are designated in writing to have original classification authority at the level of the information to remain classified. Any decision to extend this classification on other than a document-by-document basis shall be reported to the Director of the Information Security Oversight Office.

§ 2400.12 Identification and markings.

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

(1) One of the three classification levels defined in §2400.6 of this part;

(2) The identity of the original classification authority if other than OSTP; the matter shall be referred to that agency.

(3) The agency and office of origin;

(4) The date or event for declassification, or the notation “Originating Agency’s Determination Required.”

(b) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are not classified. The
Office of Science and Technology Policy

§ 2400.15

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

(c) Marking designations implementing the provisions of Executive Order 12356, including abbreviations, shall conform to the standards prescribed in Directive No. 1 issued by the Information Security Oversight Office.

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

(e) Information assigned a level of classification under predecessor Executive Orders shall be considered as classified at that level of classification despite the omission of other required markings. Omitted markings may be inserted on a document by the officials specified in § 2400.18 of this part.

§ 2400.13 Limitations on classification.

(a) In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security.

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

(c) The Director may reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security; and (2) the information may reasonably be recovered. These reclassification actions shall be reported promptly to the Director of the Information Security Oversight Office. Before reclassifying any information, the Director shall consider the factors listed in § 2001.6 of Directive No. 1, which shall be addressed in the report to the Director of the Information Security Oversight Office.

(d) Information may be classified or reclassified after OSTP has received a request for it under the Freedom of Information Act (5 U.S.C. 552a) or the Privacy Act of 1974 (5 U.S.C. 552), or the mandatory review provisions of Executive Order 12356 (section 3.4) if such classification meets the requirements of this Order and is accomplished personally and on a document-by-document basis by the Director.

Subpart C—Derivative Classification

§ 2400.14 Use of derivative classification.

(a) Derivative classification is (1) the determination that information is in substance the same as information currently classified, and (2) the application of the same classification markings. Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority. If a person who applies derivative classification markings believes that the paraphrasing, restating, or summarizing of classified information has changed the level of or removed the basis for classification, that person must consult an appropriate official of the originating agency or office of origin who has the authority to declassify, downgrade or upgrade the information.

(b) Persons who apply derivative classification markings shall:

(1) Observe and respect original classification decisions; and

(2) Carry forward to any newly created documents any assigned authorized markings. The declassification date or event that provides the longest period of classification shall be used for documents classified on the basis of multiple sources.

§ 2400.15 Classification guides.

(a) OSTP shall issue and maintain classification guides to facilitate the proper and uniform derivative classification of information. These guides shall be used to direct derivative classification.

(b) The classification guides shall be approved, in writing, by the Director or by officials having Top Secret original
classification authority. Such approval constitutes an original classification
decision.

c) Each classification guide shall specify the information subject to clas-
sification in sufficient detail to permit its ready and uniform identification
and categorization and shall set forth the classification level and duration in
each instance. Additionally, each clas-
sification guide shall prescribe declas-
sification instructions for each ele-
ment of information in terms of (1) a
period of time, (2) the occurrence of an
event, or (3) a notation that the infor-
mation shall not be automatically de-
classified without the approval of
OSTP.

d) The classification guides shall be
kept current and shall be fully re-
viewed at least every two years. The
Executive Director, OSTP shall main-
tain a list of all OSTP classification
guides in current use.

e) The Executive Director, OSTP
shall receive and maintain the record
of all approved classification
guides and changes thereto. He will as-
sist the originator in determining the
required distribution.

(f) The Director may, for good cause,
grant and revoke waivers of the re-
quirement to prepare classification
guides for specified classes of docu-
ments or information. The Director
of the Information Security Oversight Of-
Fice shall be notified of any waivers.
The Director’s decision to waive the re-
quirement to issue classification
guides for specific classes of documents
or information will be based, at a min-
imum, on an evaluation of the fol-
lowing factors:
(1) The ability to segregate and de-
scribe the elements of information;
(2) The practicality of producing or
disseminating the guide because of the
nature of the information;
(3) The anticipated usage of the guide
as a basis for derivative classification;
and
(4) The availability of alternative
sources for derivatively classifying the
information in a uniform manner.

§ 2400.16 Derivative classification
markings.

(a) Documents classified derivatively
on the basis of source documents or
classification guides shall bear all
markings prescribed in §2400.12 of this
part and Directive No. 1 as are applica-
ble. Information for these markings
shall be taken from the source docu-
ment or instructions in the appropriate
classification guide. When markings
are omitted because they may reveal a
confidential source or relationship not
otherwise evident, as described in
§2400.12 of this part, the information
may not be used as a basis for deriva-
tive classification.

(b) The authority for classification
shall be shown as directed in Directive
No. 1.

Subpart D—Declassification and
Downgrading

§ 2400.17 Policy.

Declassification of information shall
be given emphasis comparable to that
 accorded classification. Information
classified pursuant to Executive Order
12356 and prior orders shall be declas-
sified or downgraded as soon as na-
tional security considerations permit.
Decisions concerning declassification
shall be based on the loss of sensitivity
of the information with the passage of
time or on the occurrence of an event
which permits declassification. When
information is reviewed for declas-
sification pursuant to this regulation,
that information shall be declassified
unless the designated declassification
authority determines that the informa-
tion continues to meet the classifica-
tion requirements prescribed in §2400.9
of this part despite the passage of time.
The Office of Science and Technology
Policy officials shall coordinate their
review of classified information with
other agencies that have a direct inter-
est in the subject matter.

§ 2400.18 Declassification and down-
grading authority.

Information shall be declassified or
downgraded by the official who author-
ized the original classification, if that
official is still serving the same posi-
tion; the originator’s successor; a su-
ervisory official of either; or officials
delegated such authority in writing by
the Director, OSTP. The Executive Di-
rector, OSTP shall maintain a current
listing of persons or positions receiving
Office of Science and Technology Policy

§ 2400.21 Mandatory review for declassification.

(a) Except as provided in paragraph (d) of this section, all information classified under Executive Order 12356 or predecessor orders shall be subject to a review for declassification by the Office of Science and Technology Policy, if:

(1) The request is made by a United States citizen or permanent resident alien, a federal agency, or a State or local government; and

(2) The request is made in writing and describes the document or material containing the information with sufficient specificity to enable the Office of Science and Technology Policy to locate it with a reasonable amount of effort.

(b) Requests should be addressed to:
Executive Director, Office of Science and Technology Policy, Executive Office of the President, Washington, DC 20506.

(c) If the request does not reasonably describe the information sought to allow identification of documents containing such information, the requester shall be notified that unless additional information is provided or the request is made more specific, no further action will be taken.

(d) Information originated by a President, the White House Staff, by committees, commissions, or boards appointed by the President, or others specifically providing advice and counsel to a President or acting on behalf of a
§ 2400.21  President is exempted from the mandatory review provisions of § 2400.24(a) of this part. The Archivist of the United States shall have the authority to review, downgrade and declassify information under the control of the Administrator of General Services or the Archivist pursuant to sections 2107, 2107 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matters interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective presidential papers or records. Any decision by the Archivist may be appealed to the Director of the Information Security Oversight Office. Agencies with primary subject matter interest shall be notified promptly of the Director's decision on such appeals and may further appeal to the National Security Council. The information shall remain classified pending a prompt decision on the appeal.

(e) Office of Science and Technology Policy officials conducting a mandatory review for declassification shall declassify information no longer requiring protection under Executive Order 12356. They shall release this information unless withholding is otherwise authorized under applicable law.

(f) Office of Science and Technology Policy responses to mandatory review requests shall be governed by the amount of search and review time required to process the request. Normally the requester shall be informed of the Office of Science and Technology Policy determination within thirty days of receipt of the original request (or within thirty days of the receipt of the required amplifying information in accordance with paragraph (c) of this section). In the event that a determination cannot be made within thirty days, the requester shall be informed of the additional time needed to process the request. However, OSTP, shall make a final determination within one year from the date of receipt of the request except in unusual circumstances.

(g) When information cannot be declassified in its entirety, OSTP will make a reasonable effort to release, consistent with other applicable law, those declassified portions of that requested information the constitute a coherent segment.

(h) If the information may not be released in whole or in part, the requester shall be given a brief statement as to the reason for denial, and notice of the right to appeal the determination in writing within sixty days of receipt of the denial to the chairperson of the Office of Science and Technology Policy Review Committee. If appealed, the requester shall be informed in writing of the appellate determination within thirty days of receipt of the appeal.

(i) When a request is received for information originated by another agency, the Executive Director, Office of Science and Technology Policy, shall:

(1) Forward the request to such agency for review together with a copy of the document containing the information requested, where practicable, and where appropriate, with the Office of Science and Technology Policy recommendation to withhold or declassify and release any of the information;

(2) Notify the requester of the referral unless the agency to which the request is referred objects to such notice on grounds that its association with the information requires protection; and

(3) Request, when appropriate, that the agency notify the Office of Science and Technology Policy of its determination.

(j) If the request requires the rendering of services for which fees may be charged under title 5 of the Independent Offices Appropriation Act, 31 U.S.C. 483a, the Executive Director, Office of Science and Technology Policy, may calculate the anticipated amount of fees to be charged.

(1) Search for records, $5.00 per hour when the search is conducted by a clerical employee; $8.00 per hour when the search is conducted by a professional employee. No fee shall be assessed for searches of less than one hour.

(ii) Reproduction of documents. Documents will be reproduced at a rate of
§ 2400.25 Access.

(a) A person is eligible for access to classified information provided that a determination of trustworthiness has
§ 2400.26  
been made by agency heads or designated officials and provided that such access is essential to the accomplishment of lawful and authorized Government purposes. A personnel security clearance is an indication that the trustworthiness decision has been made. Procedures shall be established by the head of each office to prevent access to classified information before a personnel security clearance has been granted. The number of people cleared and granted access to classified information shall be maintained at the minimum number that is consistent with operational requirements and needs. No one has a right to have access to classified information solely by virtue of rank or position. The final responsibility for determining whether an individual's official duties require possession of or access to any element or item of classified information, and whether the individual has been granted the appropriate security clearance by proper authority, rests with the individual who has authorized possession, knowledge, or control of the information and not with the prospective recipient. These principles are equally applicable if the prospective recipient is an organizational entity, other Federal agencies, contractors, foreign governments, and others.

(b) When access to a specific classification category is no longer required for the performance of an individual's assigned duties, the security clearance will be administratively adjusted, without prejudice to the individual, to the classification category, if any, required.

(c) The Director, Office of Science and Technology Policy may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to Executive Order 12356 or predecessor orders if:

(1) Normal management and safeguarding procedures do not limit access sufficiently;

(2) The number of persons with access is limited to the minimum necessary to meet the objective of providing extra protection for the information;

(3) The special access program is established in writing; and

(4) A system of accounting for the program is established and maintained.

§ 2400.26  Access by historical researchers and former Presidential appointees.

(a) The requirement in Section 4.1(a) of Executive Order 12356 that access to classified information may be granted only as is essential to the accomplishment of authorized and lawful Government purposes may be waived as provided in paragraph (b) of this section for persons who:

(1) Are engaged in historical research projects, or

(2) Previously have occupied policymaking positions to which they were appointed by the President.

(b) Waivers under paragraph (a) of this section may be granted only if the Director, Office of Science and Technology Policy:

(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 Executive Order 12356;

(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; and

(4) Has received a written agreement from the researcher or former presidential appointee that his notes can be reviewed by OSTP for a determination that no classified material is contained therein.

§ 2400.27  Storage of classification information.

Whenever classified information is not under the personal control and observation of an authorized person, it will be guarded or stored in a locked security container approved for the storage and protection of the appropriate level of classified information as prescribed in § 2001.43 of Directive No. 1.
§ 2400.28 Dissemination of classified information.

Heads of OSTP offices shall establish procedures consistent with this Regulation for dissemination of classified material. The originating official may prescribe specific restrictions on dissemination of classified information when necessary.

(a) 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.

(b) Except as provided by 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. For purposes of this Section, the Department of Defense shall be considered one agency.

§ 2400.29 Accountability and control.

(a) Each item of Top Secret, Secret, and Confidential information is subject to control and accountability requirements.

(b) The Security Officer will serve as Top Secret Control Officer (TSCO) for the Office of Science and Technology Policy and will be responsible for the supervision of the Top Secret control program. He/she will be assisted by an Assistant Top Secret Control Officer (ATSCO) to effect the Controls prescribed herein for all Top Secret material.

(c) The TSCO shall receive, transmit, and maintain current access and accountability records for Top Secret information. The records shall show the number and distribution of all Top Secret documents, including any reproduced copies.

(d) Top Secret documents and material will be accounted for by a continuous chain of receipts.

(e) An inventory of Top Secret documents shall be made at least annually.

(f) Destruction of Top Secret documents shall be accomplished only by the TSCO or the ATSCO.

(g) Records shall be maintained to show the number and distribution of all classified documents covered by special access programs, and of all Secret and Confidential documents which are marked with special dissemination and reproduction limitations.

(h) The Security Officer will develop procedures for the accountability and control of Secret and Confidential information. These procedures shall require all Secret and Confidential material originated or received by OSTP to be controlled. Control shall be accomplished by the ATSCO.

§ 2400.30 Reproduction of classified information.

Documents or portions of documents and materials that contain Top Secret information shall not be reproduced without the consent of the originator or higher authority. Any stated prohibition against reproduction shall be strictly observed. Copying of documents containing classified information at any level shall be minimized. Specific reproduction equipment shall be designated for the reproduction of classified information and rules for reproduction of classified information shall be posted on or near the designated equipment. Notices prohibiting reproduction of classified information shall be posted on equipment used only for the reproduction of unclassified information. All copies of classified documents reproduced for any purpose including those incorporated in a working paper are subject to the same controls prescribed for the document from which the reproduction is made.

§ 2400.31 Destruction of classified information.

(a) Classified information no longer needed in current working files or for reference or record purposes shall be processed for appropriate disposition in accordance with the provisions of chapters 21 and 33 of title 44, U.S.C., which governs disposition of classified records. Classified information approved for destruction shall be destroyed in accordance with procedures and methods prescribed by the Director, OSTP, as implemented by the Security Officer. These procedures and methods must provide adequate protection to prevent access by unauthorized persons and must preclude recognition
§ 2400.32 Transmittal of classified information.

The transmittal of classified information outside of the Office of Science and Technology Policy shall be in accordance with procedures of §2001.44 of Directive No. 1. The Security Officer shall be responsible for resolving any questions relative to such transmittal.

§ 2400.33 Loss or possible compromise.

(a) Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to the Security Officer. The Security Officer shall notify the Director and the agency that originated the information as soon as possible so that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect of the compromise.

(b) The Security Officer shall initiate an inquiry to:

(1) Determine cause,
(2) Place responsibility, and
(3) Take corrective measures and appropriate administrative, disciplinary, or legal action.

(c) The Security Officer shall keep the Director advised on the details of the inquiry.

Subpart F—Foreign Government Information

§ 2400.34 Classification.

(a) Foreign government information classified by a foreign government or international organization of governments shall retain its original classification designation or be assigned a United States classification designation that will ensure a degree of protection equivalent to that required by the government or organization that furnished the information. Original classification authority is not required for this purpose.

(b) Foreign government information that was not classified by a foreign entity but was provided with the expectation, expressed or implied, that it be held in confidence must be classified because Executive Order 12356 states a presumption of damage to the national security in the event of unauthorized disclosure of such information.

§ 2400.35 Duration of classification.

Foreign government information shall not be assigned a date or event for automatic declassification unless specified or agreed to by the foreign entity.

§ 2400.36 Declassification.

Officials shall respect the intent of this Regulation to protect foreign government information and confidential foreign sources.

§ 2400.37 Mandatory review.

Except as provided in this paragraph, OSTP shall process mandatory review requests for classified records containing foreign government information in accordance with §2400.21. The agency that initially received or classified the foreign government information shall be responsible for making a declassification determination after consultation with concerned agencies. If OSTP receives a request for mandatory review and is not the agency that received or classified the foreign government information, it shall refer the request to the appropriate agency for action. Consultation with the foreign originator through appropriate channels may be necessary prior to final action on the request.

§ 2400.38 Protection of foreign government information.

 Classified foreign government information shall be protected as is prescribed by this regulation for United States classified information of a comparable level.
Subpart G—Security Education

§ 2400.39 Responsibility and objectives.

The OSTP Security Officer shall establish a security education program for OSTP personnel. The program shall be sufficient to familiarize all OSTP personnel with the provisions of Executive Order 12356 and Directive No. 1, and this regulation. It shall be designed to provide initial, refresher, and termination briefings to impress upon them their individual security responsibilities.

Subpart H—Office of Science and Technology Policy Information Security Program Management

§ 2400.40 Responsibility.

The Director, OSTP is the senior OSTP official having authority and responsibility to ensure effective and uniform compliance with and implementation of Executive Order 12356 and its implementing Directive No. 1. As such, the Director, OSTP, shall have primary responsibility for providing guidance, oversight and approval of policy and procedures governing the OSTP Information Security Program. The Director, OSTP, may approve waivers or exceptions to the provisions of this regulation to the extent such action is consistent with Executive Order 12356 and Directive No. 1.

§ 2400.41 Office Review Committee.

The Office of Science and Technology Policy Review Committee (hereinafter referred to as the Office Review Committee) is hereby established and will be responsible for the continuing review of the administration of this Regulation with respect to the classification and declassification of information or material originated or held by the Office of Science and Technology Policy. The Office Review Committee shall be composed of the Executive Director who shall serve as chairperson, the Assistant Director for National Security & Space, and the Security Officer.

§ 2400.42 Security Officer.

Under the general direction of the Director, the Special Assistant to the Executive Director will serve as the Security Officer and will supervise the administration of this Regulation. He/she will develop programs, in particular a Security Education Program, to insure effective compliance with and implementation of the Information Security Program. Specifically he/she also shall:

(a) Maintain a current listing by title and name of all persons who have been designated in writing to have original Top Secret, Secret, and Confidential Classification authority. Listings will be reviewed by the Director on an annual basis.

(b) Maintain the record copy of all approved OSTP classification guides.

(c) Maintain a current listing of OSTP officials designated in writing to have declassification and downgrading authority.

(d) Develop and maintain systematic review guidelines.

§ 2400.43 Heads of offices.

The Head of each unit is responsible for the administration of this regulation within his area. These responsibilities include:

(a) Insuring that national security information is properly classified and protected;

(b) Exercising a continuing records review to reduce classified holdings through retirement, destruction, downgrading or declassification;

(c) Insuring that reproduction of classified information is kept to the absolute minimum;

(d) Issuing appropriate internal security instructions and maintaining the prescribed control and accountability records on classified information under their jurisdiction.

§ 2400.44 Custodians.

Custodians of classified material shall be responsible for providing protection and accountability for such material at all times and particularly for locking classified material in approved security equipment whenever it is not in use or under direct supervision of authorized persons. Custodians shall follow procedures which insure that unauthorized persons
§ 2400.45 Information Security Program Review.

(a) The Director, OSTP, shall require an annual formal review of the OSTP Information Security Program to ensure compliance with the provisions of Executive Order 12356 and Directive No. 1, and this regulation.

(b) The review shall be conducted by a group of three to five persons appointed by the Director and chaired by the Executive Director. The Security Officer will provide any records and assistance required to facilitate the review.

(c) The findings and recommendations of the review will be provided to the Director for his determination.

§ 2400.46 Suggestions or complaints.

Persons desiring to submit suggestions or complaints regarding the Office of Science and Technology Policy Information Security Program should do so in writing. This correspondence should be addressed to: Executive Director, Office of Science and Technology Policy, Executive Office of the President, Washington, DC 20506.
CHAPTER XXVII—OFFICE FOR MICRONESIAN STATUS NEGOTIATIONS

<table>
<thead>
<tr>
<th>Part</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2700</td>
<td>Security information regulations</td>
</tr>
</tbody>
</table>
PART 2700—SECURITY INFORMATION REGULATIONS

Subpart A—Introduction

Sec.
2700.1 References.
2700.2 Purpose.
2700.3 Applicability.

Subpart B—Original Classification

2700.11 Basic policy.
2700.12 Criteria for and level of original classification.
2700.13 Duration of original classification.
2700.14 Challenges to classification.

Subpart C—Derivative Classification

2700.21 Definition and application.

Subpart D—Declassification and Downgrading

2700.31 Declassification authority.
2700.32 Declassification general.
2700.33 Mandatory review for declassification.
2700.34 Downgrading authority.

Subpart E—Safeguarding

2700.41 General restrictions on access.
2700.42 Responsibility for safeguarding classified information.
2700.43 Reproduction controls.
2700.44 Administrative sanctions.

Subpart F—Implementation and Review

2700.51 Information Security Oversight Committee.
2700.52 Classified Review Committee.


SOURCE: 44 FR 51574, Sept. 4, 1979. Correctly designated at 44 FR 51990, Sept. 6, 1979, unless otherwise noted.

Subpart A—Introduction

§ 2700.1 References.


§ 2700.2 Purpose.

The purpose of this Regulation is to ensure, consistent with the authorities listed in § 2700.1, that national security information originated and/or held by the Office for Micronesian Status Negotiations (OMSN), which includes the Status Liaison Office, Saipan, Northern Mariana Islands (SLNO), is protected. To ensure that such information is protected, but only to the extent and for such period as is necessary, this regulation identifies the information to be protected and specifies certain classification, declassification and safeguarding procedures to be followed.

§ 2700.3 Applicability.

This Regulation supplements E.O. 12065 within OMSN with regard to National Security Information. In consonance with the authorities listed in § 2700.1, it establishes general policies and certain procedures for the classification, declassification and safeguarding of information which is owned by, is produced for or by, or is under the control of OMSN.

Subpart B—Original Classification

§ 2700.11 Basic policy.

(a) General. It is the policy of OMSN to make available to the public as much information concerning its activities as is possible, consistent with its responsibility to protect the national security.

(b) Safeguarding national security information. Within the Federal Government there is some information which because it bears directly on the effectiveness of our national defense and the conduct of our foreign relations, must be subject to some constraints for the security of our nation.

(c) Balancing test. To balance the public’s interest in access to government information with the need to protect certain national security information from disclosure, these regulations identify the information to be protected, prescribe classification, downgrading, declassification, and safeguarding procedures to be followed, and establish education, monitoring and
sanctioning systems to insure their effectiveness. When questions arise as whether the need to protect information may be outweighed by the public interest in disclosure of the information, they shall be referred to OMSN pursuant to §2700.32(b) for a determination whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure.

§ 2700.12 Criteria for and level of original classification.

(a) General Policy. Documents or other material are to be classified only when protecting the national security requires that the information they contain be withheld from public disclosure. Information may not be classified to conceal violations of law, inefficiency, or administrative error, or to prevent embarrassment to a person, organization or agency, or to restrain competition. No material may be classified to limit dissemination, or to prevent or delay public release, unless its classification is consistent with E.O. 12065.

(b) Criteria. To be eligible for classification, information must meet two requirements:

(1) First, it must deal with one of the criteria set forth in section 1–301 of E.O. 12065;

(2) Second, the President’s Personal Representative for Micronesian Status Negotiations or his delegate who has original classification authority must determine that unauthorized disclosure of the information or material can reasonably be expected to cause at least identifiable harm to the national security.

(c) Classification designations. Only three designations of classification are authorized—“Top Secret,” “Secret,” “Confidential.” No other classification designation is authorized or shall have force.

(d) Unnecessary classification, and classification at a level higher than is necessary, shall be avoided. If there is reasonable doubt as to which designation in section 1–1 of E.O. 12065 is appropriate, or whether information should be classified at all, the less restrictive designation should be used, or the information should not be classified.

§ 2700.13 Duration of original classification.

(a) Information or material which is classified after December 1, 1978, shall be marked at the time of classification with the date or event for declassification or a date for review for declassification. This date or event shall be as early as national security permits and shall be no more than six years after original classification except as provided in paragraph (b) of this section.

(b) Only the President’s Personal Representative for Micronesian Status Negotiations may authorize a classification period exceeding six years. Originally classified information that is so designated shall be identified with the authority and reason for extension. This authority shall be used sparingly. In those cases where extension of classification is warranted, a declassification date or event, or a date for review shall be set. This date or event shall be early as national security permits and shall be no more than twenty years after original classification except that for foreign information the date or event may be up to thirty years after original classification.

§ 2700.14 Challenges to classification.

If holders of classified information believe the information is improperly or unnecessarily classified, or that original classification has been extended for too long a period, they should discuss the matter with their immediate superiors or the classifier of the information. If these discussions do not satisfy the concerns of the challenger, the matter should be brought to the attention of the chairman of the OMSN Information Security Oversight Committee, established pursuant to §2700.51. Action on such challenges shall be taken within 30 days from date of receipt and the challenger shall be notified of the results. When requested, anonymity of the challenger shall be preserved.
Office for Micronesian Status Negotiations

§ 2700.21 Definition and application.

Derivative classification is the act of assigning a level of classification to information which is determined to be the same in substance as information which is currently classified. Thus, derivative classification may be accomplished by any person cleared for access to that level of information, regardless of whether the person has original classification authority at that level.

§ 2700.22 Classification guides.

OMSN shall issue classification guides pursuant to section 2–2 of E.O. 12065. These guides, which shall be used to direct derivative classification, shall identify the information to be protected in specific and uniform terms so that the information involved can be readily identified. The classification guides shall be approved in writing by the President’s Personal Representative for Micronesian Status Negotiations. Such approval constitutes an original classification decision. The classification guides shall be kept current and shall be reviewed at least every two years.

Subpart D—Declassification and Downgrading

§ 2700.31 Declassification authority.

The Director, OMSN, is authorized to declassify OMSN originated documents after consultation with the appropriate OMSN staff members.

§ 2700.32 Declassification general.

Declassification of classified information shall be given emphasis comparable to that accorded to classification. The determination to declassify information shall not be made on the basis of the level of classification assigned, but on the loss of the sensitivity of the information with the passage of time, and with due regard for the public interest in access to official information. At the time of review, any determination not to declassify shall be based on a determination that despite the passage of time since classification, release of information reasonably could still be expected to cause at least identifiable damage to the national security.

§ 2700.33 Mandatory review for declassification.

(a) General. All information classified under the Order or prior orders, except as provided for in section 3–503 of E.O. 12065 shall be subject to review for declassification upon request of a member of the public, a government employee, or an agency.

(b) Receipt. (1) Requests for mandatory review for declassification under section 3–501 of E.O. 12065 must be in writing and should be addressed to: Office for Micronesian Status Negotiations, ATTN: Security Officer (Mandatory Review Request), Room 3356, Department of the Interior, Washington, DC 20240.

(2) The requestor shall be informed of the date of receipt of the request at OMSN. This date will be the basis for the time limits specified in paragraph (c) of this section.

(3) If the request does not reasonably describe the information sought, the requestor shall be notified that, unless additional information is provided or the request is made more specific, no further action will be taken.

(4) Subject to paragraph (b)(7) of this section, if the information requested is in the custody of and under the exclusive declassification authority of OMSN, OMSN shall determine whether the information or any reasonably segregable portion of it no longer requires protection. If so, OMSN shall promptly make such information available to the requester, unless withholding it is otherwise warranted under applicable law. If the information may not be released, in whole or in part, OMSN shall give the requester a brief statement of the reasons, a notice of the right to appeal the determination to the agency review committee, and notice that such an appeal must be filed with the review committee within 60 days.

(5) When OMSN receives a request for information in a document which is in its custody, but which was classified by
another agency, it shall refer the request to the appropriate agency for review, together with a copy of the document containing the information requested, where practicable. OMSN shall also notify the requester of the referral, unless the association of the reviewing agency with the information requires protection. The reviewing agency shall review a document in coordination with any other agency involved with the classification or having a direct interest in the subject matter. The reviewing agency shall respond directly to the requester in accordance with the pertinent procedures described above and, if requested, shall notify OMSN of its determination.

(6) Requests for declassification of classified documents originated by OMSN or another agency but in the possession and control of the Administrator of General Services, pursuant to 44 U.S.C 2107 or 2107 Note, shall be referred by the Archivist to the agency of origin for processing and for direct response to the requests. The Archivist will inform requesters of such referrals.

(7) In the case of requests for documents containing foreign government information, OMSN, if it is also the agency which initially received the foreign government information, shall determine whether the foreign government information in the document may be declassified and released in accordance with agency policies or guidelines, consulting with other agencies of subject matter interest as necessary. If OMSN is not the agency which received the foreign government information, it shall refer the request to the latter agency, which shall take action on the request. In those cases where available agency policies or guidelines do not apply, consultation with the foreign originator through appropriate channels may be advisable prior to final action on the request.

(8) If any agency makes a request on behalf of a member of the public, the request shall be considered as a request by that member of the public and handled accordingly.

(c) Review. (1) Within sixty days from its receipt, OMSN shall inform the requester of the determination of the mandatory review for declassification.

(2) If the determination is to withhold some or all of the material requested, the requester may appeal the determination. The requester shall be informed that an appeal must be made in writing within sixty days of receipt of the denial and should be addressed to the chairperson of the OMSN Classification Review Committee established pursuant to §2700.52.

(3) No agency in possession of a classified document may, in response to a request for the document made under the Freedom of Information Act (5 U.S.C. 552) or under section 3-5 of E.O. 12065, refuse to confirm the existence or non-existence of the document, unless the fact of its existence or non-existence would itself be classifiable.

(4) The requester shall be informed of the appellate determination within thirty days of receipt of the appeal.

(5) In considering requests for mandatory review, OMSN may decline to review again any request for material which has been recently reviewed and denied, except insofar as the request constitutes an appeal under paragraph (f) of this section.

(d) Processing of Requests. The processing of requests by OMSN shall be as follows:

(1) The Security Officer or his designee shall record the request, and arrange for search and review of the documents. The documents will be reviewed for declassification in accordance with these regulations or any applicable guidelines. If the documents remain classified and are not to be released, in whole or in part, the reviewing office will also prepare a letter informing the requester as described in paragraph (b)(4) of this section. The letter to the requester shall be signed by the President’s Personal Representative for Micronesian Status Negotiations, his Deputy or the Status Liaison Officer. The Security Officer or his designee shall record disposition of the case and forward the letter of denial to the requester.

(2) If any request requires obtaining the views of other agencies, the receiving office shall arrange coordination of review with such other agencies.

(3) When all documents involved in the request are declassified and released, the receiving office will send a
release statement, to the requester, and shall inform the requester of any fees due before releasing documents.

(4) In the case of documents of agency origin requested by a Presidential Library on behalf of a member of the public, if there is a partial denial, the letter will advise the requester as described in paragraph (b)(4) of this section, but the requester will be referred to the Archivist for copies of the released document, with portions excised. The receiving office will transmit such documents, with portions marked to be excised, to Archives which will transmit them with portions excised to the Presidential Library for its records and for use in the case of further similar requests.

(5) The Security Officer or his designee shall also coordinate requests from other agencies seeking the views of OMSN as to declassification of documents originated by such other agencies but involving information of primary subject matter interest to OMSN. The Security Officer or his designee will transmit the documents to the reviewing individual for a determination as to declassification and will coordinate the reply of OMSN to the requesting agency.

(e) Appeals. (1) The President's Personal Representative for Micronesian Status Negotiations shall receive appeals for denial of documents by OMSN. Such appeals shall be addressed to President's Personal Representative for Micronesian Status Negotiations, Suite 3356, Interior Department Building, Washington, DC 20240. The appeal must be received in OMSN within 60 days of the date of the original denial letter or the final release of documents, whichever is later.

(2) Appeals shall be decided within 30 days of their receipt.

(f) Fees. (1) Fees for the location and reproduction of information which is the subject of a mandatory review request shall be assessed according to the following schedule:

(i) Reproduction of documents: Documents will be reproduced at a rate of $.25 per page for all copying of four pages or more. No fee shall be assessed for reproducing documents which are three pages or less, or for the first three pages of longer documents.

(ii) Where it is anticipated that the fees chargeable under this section will amount to more than $25.00, and the requester has not indicated in advance a willingness to pay fees as high as are anticipated, the requester shall be promptly notified of the amount of the anticipated fee or such portion thereof as can readily be estimated. In instances where the estimated fees will greatly exceed $25.00, an advance deposit may be required. Dispatch of such a notice or request shall suspend the running of the period for response by OMSN until a reply is received from the requester.

(2) Where it is anticipated that the fees chargeable under this section will amount to more than $25.00, and the requester has not indicated in advance a willingness to pay fees as high as are anticipated, the requester shall be promptly notified of the amount of the anticipated fee or such portion thereof as can readily be estimated. In instances where the estimated fees will greatly exceed $25.00, an advance deposit may be required. Dispatch of such a notice or request shall suspend the running of the period for response by OMSN until a reply is received from the requester.

(3) Remittance shall be in the form either of a personal check or bank draft on a bank in the United States, or a postal money order. Remittance shall be made payable to Treasurer of the United States and mailed to the address noted in paragraph (b)(1) of this section.

(4) A receipt for fees paid will be provided only upon request. Refund of fees for services actually rendered will not be made.

(5) OMSN may waive all or part of any fee provided for in this section when it is deemed to be in either the interest of OMSN or of the general public.

$2700.34 Downgrading authority.

The Security Officer, OMSN is authorized to downgrade OMSN originated documents after consultation with the staff member who is charged with functional responsibility for the subject matter under question.

Subpart E—Safeguarding

§2700.41 General restrictions on access.

(a) Determination of need-to-know. Classified information shall be made available to a person only when the possessor of the classified information establishes in each instance, except as provided in section 4-3 of E.O. 12065,
that access is essential to the accomplishment of official Government duties or contractual obligations.

(b) Determination of Trustworthiness. A person is eligible for access to classified information only after a showing of trustworthiness as determined by the President’s Personal Representative for Micronesian Status Negotiations based upon appropriate investigations in accordance with applicable standards and criteria.

§ 2700.42 Responsibility for safeguarding classified information.

(a) General Policy. The specific responsibility for the maintenance of the security of classified information rests with each person having knowledge or physical custody thereof, no matter how obtained. The ultimate responsibility for safeguarding classified information rests on each supervisor to the same degree that supervisor is charged with functional responsibility.

(b) Security and Top Secret Control Officers. The Director, OMSN, and the Status Liaison Officer, Saipan, are assigned specific security responsibilities as Security Officer and Top Secret Control Officer.

(c) Handling. All documents bearing the terms “Top Secret,” “Secret” and “Confidential” shall be delivered to the Top Secret Control Officer or his designee immediately upon receipt. All potential recipients of such documents shall be advised of the names of such designees and updated information as necessary. In the event that the Top Secret Control Officer or his designee are not available to receive such documents, they shall be turned over to the office supervisor and secured, unopened, in a designated combination safe located in OMSN or SLNO, as appropriate until the Top Secret Control Officer is available. All materials not immediately deliverable to the Top Secret Control Officer shall be delivered at the earliest opportunity. Under no circumstances shall classified material that cannot be delivered to the Top Secret Control Officer be stored other than in the designated safe.

(d) Storage. All classified documents shall be stored in the designated combination safe or safes located in OMSN or SLNO as appropriate. The combination shall be changed as required by ISOO Directive No. 1, section IV F (5)(a). The combinations shall be known only to the Security Officer and his designees with the appropriate security clearance.

(e) Security Education Program. The Security Officer shall establish a program of briefings to familiarize personnel with the provisions of E.O. 12065 and implementing directives. Such briefings shall be held once per year, or more frequently. Before any new or newly assigned employee enters on duty, he shall be given instruction in sufficient detail in security procedures and practices to inform him of his responsibilities arising from his access to classified data.

(f) Access by Historical Researchers and Former Presidential Appointees. In keeping with provisions 4–301 and 4–302 of E.O. 12065, the President’s Personal Representative for Micronesian Status Negotiations shall designate appropriate officials to determine, prior to granting access to classified information, the propriety of such action in the interest of national security and assurance of the recipient’s trustworthiness and need-to-know.

§ 2700.43 Reproduction controls.

OMSN and SLNO shall maintain records to show the number and distribution of all OMSN originated classified documents. Reproduction of classified material shall take place only in accordance with section 4–4 of E.O. 12065 and any limitations imposed by the originator. Should copies be made, they are subject to the same controls as the original document. Records showing the number of distribution of copies shall be maintained by the Office Supervisor and the log stored with the original documents. These measures shall not restrict reproduction for the purposes of mandatory review.

§ 2700.44 Administrative sanctions.

Officers and employees of the United States Government assigned to OMSN shall be subject to appropriate administrative sanctions if they knowingly and willingly commit a violation under section 5–5 of E.O. 12065. These sanctions may include reprimand, suspension without pay, removal, termination
of classification authority, or other sanction in accordance with applicable law or the applicable regulations of the agency from which they are assigned to OMSN.

Subpart F—Implementation and Review
§ 2700.51 Information Security Oversight Committee.

The OMSN Information Security Oversight Committee shall be chaired by the Security Officer, OMSN. The Committee shall be responsible for acting on all suggestions and complaints concerning the administration of the OMSN information security program. The chairperson shall also be responsible for conducting an active oversight program to ensure effective implementation of E.O. 12065.

§ 2700.52 Classified Review Committee.

The OMSN Classification Review Committee shall be chaired by the President’s Personal Representative for Micronesian Status Negotiations. The Committee shall decide appeals from denials of declassification requests submitted pursuant to section 3-5 of E.O. 12065. The Committee shall consist of the President’s Personal Representative, Department of Defense/Legal Advisor and Political/Economic Advisor.
<table>
<thead>
<tr>
<th>Part</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2800</td>
<td>561</td>
</tr>
<tr>
<td>Security procedures</td>
<td>..........................</td>
</tr>
</tbody>
</table>

CHAPTER XXVIII—OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES
PART 2800—SECURITY PROCEDURES

Sec.
2800.1 Purpose.
2800.2 Guiding directives.
2800.3 Policy.
2800.4 General information.
2800.5 Policies.
2800.6 Delegation of classification and declassification authority.
2800.7 Designation of chairperson for Ad Hoc Committees.

ATTACHMENTS TO PART 2800
ATTACHMENT 1—EMPLOYMENT AGREEMENT & INDOCTRINATION STATEMENT
ATTACHMENT 2—SECURITY TERMINATION STATEMENT
ATTACHMENT 3—SAMPLE


SOURCE: 44 FR 66591, Nov. 20, 1979, unless otherwise noted.

§ 2800.1 Purpose.
To establish procedures and provide guidance for the security of classified information and material within the Office of the Vice President.

§ 2800.2 Guiding directives.

§ 2800.3 Policy.
The classification, declassification, safeguarding and handling of classified information within the Office of the Vice President will comply with the letter and spirit of those directives listed in §2800.2. All personnel of the Office of the Vice President are responsible individually for complying with the provisions of these regulations in all respects. The provisions of these regulations applicable to all personnel assigned or detailed to the Office of the Vice President.

§ 2800.4 General information.
(a) Staff Security Officer/Top Secret Control Officer. A Vice Presidential Staff Security Officer and Assistant Staff Security Officer will be assigned to perform the duties as outlined in these regulations. They will normally be on the staff of the Assistant to the Vice President for National Security Affairs. The Staff Security Officer and Assistant Staff Security Officer will serve as Top Secret Control Officer and Assistant Top Secret Control Officer and custodians of classified material for the Office of the Vice President respectively, and will be responsible for the overall supervision of the Top Secret Control program. They will maintain positive control over the movement of all Top Secret material under their jurisdiction.

(b) Custodian, Office of the Assistant to the Vice President for Congressional Relations. The Assistant to the Vice President for Congressional Relations, Office of the President of the Senate, will be designated as Custodian of classified material for that office. He will be responsible for compliance with the instructions contained herein. In this capacity, he will be charged with safeguarding classified material necessary to the operation of the office.

(c) National Security Classifications. Classifications of National Security Information are defined in Executive Order 12065, sections 1–102 through 1–104.

(d) Prohibited Markings. (1) The caveats “FOR OFFICIAL USE ONLY” and “ADMINISTRATIVELY RESTRICTED” are used within the Office of the Vice President to designate certain unclassified information which requires control. These caveats will under no circumstances be applied to information which qualifies as classified information. Further, neither they nor other terms will be used in conjunction with the prescribed security classifications of CONFIDENTIAL, SECRET and TOP SECRET.

(2) Unclassified information bearing either of the foregoing administrative designations cannot be protected from release under the national security exemption of the Freedom of Information Act (although other exemptions may be available).

(e) Security Clearances. No person shall be given access to classified information or material unless a favorable background investigation has been
completed determining that the individual is trustworthy and that access is necessary for the performance of official duties.

(1) Security Clearance Procedures. (i) The Counsel to the Vice President will:
   (A) Be responsible for the processing of full field investigations for personnel assigned to the Vice President’s staff. Department of Defense detailees are processed by the Defense Investigative Service.
   (B) Inform the Staff Security Office of individuals whose full field investigations have been satisfactorily completed and approved and of any subsequent changes.
   (C) Notify the Staff Security Office as soon as he/she is aware that a staff member is planning to terminate his/her employment.

(ii) The Staff Security Office will provide newly cleared persons with a security orientation briefing covering policy and procedures for handling classified information and material. After the briefing individuals will sign a Statement of Understanding of Security Procedures (Attachment 1). This statement will be kept on file by the Staff Security Office.

(iii) There is no such thing as an “Interim Security Clearance” for persons employed by or detailed to the Office of the Vice President. Under no circumstances will uncleared persons be given access to classified material. Access to classified material will be denied until the individual has had a satisfactorily completed background investigation, has received the security orientation briefing and signed the Statement of Understanding of Security Procedures.

(iv) The Staff Security Office, as part of an individual’s departure debriefing, will remind them of their continuing responsibilities to protect classified information to which they have had access during the performance of their official duties. After being debriefed, the individual will sign a Security Termination Statement acknowledging his responsibilities (Attachment 2).

(2) Satisfactory completion of a background investigation does not in itself grant an individual access to classified information. Individual clearances for access to classified information or material will be controlled by the Staff Security Office and certified in writing on an individual basis.

(f) Access to Classified Material. Each member of the staff who has custody or possession of classified information is responsible for providing the required degree of protection from unauthorized disclosure at all times.

(1) Classified information and material will only be disclosed to an individual after it has been determined that the individual possesses the required clearance and has a valid “need to know.” Persons releasing the information shall be responsible in every case for determining the recipient’s eligibility for access.

(2) Access to Sensitive Compartmented Intelligence Information will be controlled by the Assistant to the Vice President for National Security Affairs.

(g) Custody and safekeeping of Classified Material. (1) Classified material addressed to the Office of the Vice President will normally be delivered to and receipted for by the Staff Security Office where it will be entered into the classified material control system.

(i) Staff members receiving classified material from any source by any means will personally deliver such material to the Staff Security Office for appropriate entry into the classified control system.

(ii) Conversely, members of the staff desiring to transmit classified material will deliver the material to the Staff Security Office for handling in accordance with paragraph (h)(5) of this section.

(2) Storage of Classified Material. (i) Classified material will be stored only in accordance with the provisions of ISOO Directive No. 1, paragraph IV–F–1 through 4.

(ii) Filing of unclassified material in security containers is prohibited except where the unclassified material is an integral part of a file which contains classified material. If extenuating circumstances necessitate the use of a security container for storing only unclassified material, the container will be marked with a sign stating “This container is not used to store
Office of the Vice President of the U.S.

§ 2800.4

classified material” or “Do not store classified material in this container.”

(3) Record of safe locations. The Staff Security Office will assign numbers to all security containers used to store classified material in the Office of the Vice President. A record of safe numbers, locations and date of last combination change will be maintained in the Staff Security Office.

(4) Changing of lock combinations. Combinations of security containers will be changed by the Staff Security Office or the Secret Service. This service may be requested by contacting the Staff Security Office. Combinations will be changed in accordance with the provisions of ISOO Directive No. 1, paragraph IV–F–5.

(5) Records of combinations. Records of combinations shall be maintained by the Staff Security Office. Whenever a combination is changed, the new combination and other required information will be recorded on GSA Optional Form 63. The sealed envelope will then be delivered to the Staff Security Office for retention in the vault safe.

(6) Custodians. Each container used for storage of classified material within the Office of the Vice President will have assigned a primary and alternate custodian. Responsibility for security of these containers shall rest with those persons, and their names shall be affixed on the outside of the top drawer of each container positioned so as to be readily discernible. Optional Form 63 shall be used for this purpose.

(h) Handling of Classified Material—(1) Use of cover sheets. A separate cover sheet indicating the classification of the material will be fastened to the top page of cover of each CONFIDENTIAL, SECRET or TOP SECRET document.

(2) Unattended documents. Classified material will be under the direct supervision of a person with an appropriate security clearance and a verified need-to-know at all times when in use. Special care will be taken to insure that classified material is not left unsecured or unattended in an office.

(3) Working papers. Working papers are documents, including drafts, photographs, etc., created to assist in the formulation and preparation of finished papers. Working papers containing classified information will be marked with the appropriate classification and provided the same degree of protection as that given to other documents of an equal category of classification.

(4) Communications security. Classified information shall not be discussed over any voice communications device except as authorized over approved secure communications circuits. This restriction also applies to electrical transmission of classified material via any unsecure circuitry involving teletypes, DEX equipment or other systems of a like nature. Appropriate secure facilities for the discussion or transmittal of classified material may be arranged by contacting the Staff Security Office.

(5) Transmittal of Classified Material—

(i) Outside the Office of the Vice President and the White House Complex. The Staff Security Office is responsible for transmitting or transferring all classified material outside the Office of the Vice President and the White House Complex in accordance with the provisions of ISOO Directive No. 1, paragraphs I, G and H.

(ii) Within the Office of the Vice President and the White House Complex. Transfer or movement of classified material will be accomplished only by properly cleared persons handcarrying the material to the recipient. The material shall be carried in an envelope marked with the appropriate classification. Use of see through messenger envelopes is not authorized. Recipients will sign a receipt (GSA Optional Form 112) for all material classified SECRET and TOP SECRET. Whenever TOP SECRET material is transferred, the Staff Security Office will be notified in order to maintain accurate accountability of the material. Classified material will never be delivered to an uncleared person, left in an unoccupied office, or sent through unclassified mail delivery/distribution systems.

(iii) Staff members requiring the use of classified material at conferences or meetings held outside the Washington, DC Metropolitan area and who intend to use commercial transportation shall provide the material to the Staff Security Office far enough in advance to assure that the material will be available
§ 2800.4 32 CFR Ch. XXVIII (7–1–01 Edition)

on or before the date needed. This requirement does not apply when utilizing government/military transportation. In this case, material may be handcarried. The Staff Security Office will brief each staff member prior to departure concerning security requirements or arrangements needed to safeguard the material while away from his office. For meetings or conferences within the Washington, DC Metropolitan area, members may handcarry classified material. Use of classified material during a conference or meeting requires increased awareness and precautionary handling to avoid security violations and/or compromises. Staff members using classified material during a meeting or conference are responsible for ensuring that the material is properly protected at all times, and that personnel present possess appropriate clearances for the material being presented.

(iv) Visits to foreign countries. Special precautions must be taken when visiting foreign countries to ensure classified material is protected at all times. For all visits to foreign countries a member of the staff will be appointed as custodian for all classified material required for the success of the mission. This individual will be the holder of a diplomatic passport which exempts him from customs inspections. Individual so designated will coordinate with United States embassy personnel in the country to be visited for securing of classified material within the embassy compound or other appropriate secure area during the course of the visit.

(6) Preparation and marking of Classified Material. All classified material originating within the office of the Vice President will be prepared and marked by properly authorized and cleared personnel in accordance with ISOO Directive No. 1, paragraphs I, G, and H. A sample letter is attached for your guidance (Attachment 3). Derivative information will be prepared and classified in accordance with ISOO Directive No. 1, paragraphs II A through C. Questions concerning procedures should be directed to the Staff Security Office.

(7) Reproduction of Classified Material.

(i) Reproduction of classified material will be accomplished only by properly cleared persons.

(ii) Reproduction of TOP SECRET material will be accomplished only by a member of the Staff Security Office or a designated representative of that office.

(iii) Accountability of reproduced classified material will be maintained by informing the Staff Security Office of the reproduction of SECRET and TOP SECRET material, the number of copies reproduced and their disposition.

(iv) Reproduction machines can retain the imagery of material passed through them. Therefore, to avoid inadvertent disclosure of classified information through subsequent use of machines, staff members will always run machines through four cycles (four blank pages) after the last page of the classified material has been reproduced. These pages will be destroyed in the same manner as classified material.

(8) Destruction of Classified Material.

(i) SECRET and TOP SECRET material will be given to the Staff Security Office for destruction to insure destruction is properly recorded and destroyed material is removed from the classified control system.

(ii) CONFIDENTIAL material may be destroyed in the holder’s office by tearing lengthwise and placing in a “Burn Bag” specifically designated for classified material.

(iii) Classified waste material will be separated from other office waste material and placed in “Burn Bags.” Classified waste material includes working papers, notes, drafts of classified correspondence, carbon paper, typewriter ribbons and any other material containing information requiring destruction. “Burn Bags” will be collected daily by a member of the White House Executive Protective Service who will then dispose of the bags in a secure facility.

(iv) Typewriter ribbons. Classified material can be reproduced from imprints on used typewriter ribbons. Therefore, ribbons which are used in the preparation of classified material must be safeguarded accordingly, i.e., they will
Office of the Vice President of the U.S. § 2800.6

be stored in a safe at the close of business, destroyed as classified waste when no longer serviceable, etc.

(9) Inventories. The Staff Security Office will conduct inventories of all TOP SECRET material charged to the Office of the Vice President at least annually to determine the adequacy of control procedures and insure accountability.

(i) Loss or compromise. Any person who has knowledge of loss of possible compromise of classified information shall promptly report the circumstances to the Staff Security Office for appropriate action in accordance with ISOO Directive No. 1, paragraph IV, H.

(j) Penalties. Any individual breach of security may warrant penalties up to and including the separation of the individual from his employment or criminal prosecution.

(k) Special access. Special access authority is required for release of Sensitive Compartmented Intelligence Information. The names of personnel cleared for access to this category of information are on file in the Staff Security Office.

§ 2800.5 Policies.

(a) Basic policy. Except as provided in the Atomic Energy Act of 1943, as amended, Executive Order 12065, as implemented by ISOO Directive No. 1, provides the only basis for classifying information. It is the policy of this office to make available to the public as much information concerning its activities as possible consistent with the need to protect the national security. Accordingly, security classification shall be applied only to protect the national security.

(b) Duration of classification. Classification shall not be continued longer than necessary for the protection of national security. Each decision to classify requires a simultaneous determination of the duration such classification must remain in effect. For further guidance, refer to sections 1-401 and 1-402, E.O. 12065.

(c) Declassification. Declassification of information shall be given emphasis comparable to that accorded to classification. Decisions concerning declassification shall be based on the loss of the information’s sensitivity with the passage of time or upon the occurrence of a declassification event. For further guidance, refer to sections 3-102, 3-103 and 3-104 of E.O. 12065.

(d) Systematic review for declassification. Systematic review for declassification will be in accordance with sections 3-204, 3-401 and 3-503 of E.O. 12065.

(e) Mandatory review requests. Requests from a member of the public, a government employee, or an agency, to declassify and release information will be acted upon within 60 days provided the request reasonably identifies the information. After review, the information or any reasonably segregable portion thereof that no longer requires protection, shall be declassified and released, except as provided in section 3-503, E.O. 12065, unless withholding is otherwise warranted under applicable law.

(f) Classification guides. The Chief Counsel, National Security Council, has determined that, in view of the limited amount of material originally classified by this office, the preparation and publication of classification guides is not required.

(g) Access to Classified Information by historical researchers and former Presidential appointees. Access may be granted under the provisions of section 4-3 of E.O. 12065; however, access is permissive and not mandatory.

§ 2800.6 Delegation of classification and declassification authority.

Pursuant to the provisions of sections 1-201 and 3-103 of E.O. 12065 of June 28, 1978, the following officials within the Office of the Vice President, are designated to originally classify and declassify information as “SECRET” and/or “CONFIDENTIAL”:

(a) Chief of Staff to the Vice President.

(b) Counsel to the Vice President.

(c) Executive Assistant to the Vice President.

(d) Assistant to the Vice President for National Security Affairs.

(e) Assistant to the Vice President for Issues Development and Domestic Policy.

(f) Additionally, the following individuals are designated to declassify “SECRET” and/or “CONFIDENTIAL”
§ 2800.7 Designation of chairperson for Ad Hoc Committees.

The Counsel to the Vice President is designated as the responsible official to chair Ad Hoc Committees as necessary to act on all suggestions and complaints with respect to the administration of the information security program.
As consideration for employment with the Office of the Vice President and as a condition for continued employment I hereby declare that I intend to be governed by and I will comply with the following provisions:

1. By virtue of the performance of my official duties while employed by or assigned to the Office of the Vice President, I expect to be the recipient of classified information, materials, plans or intelligence data which concern the national defense and foreign relations of the United States and which are the property of the United States Government. I have been furnished and I understand the provisions of (a) the Espionage Act, Title 18, USC, Section 793 and 794, concerning the disclosure of information relating to the national defense of the United States and the penalties provided for violations thereof; (b) Title 18, USC, Section 1001, concerning the making of false statements; and (c) Executive Order 12065 entitled "National Security Information."

2. I understand that one of the obligations of my employment by or assignment to the Office of the Vice President is strict compliance with the provisions of Federal laws, directives and regulations with respect to the safeguarding of classified information of the United States Government from unauthorized disclosure.

3. I agree that in the course of my employment by or assignment to the Vice President's staff and subsequent thereto, I will not divulge, publish or reveal by any means any classified information, intelligence data or knowledge which I may acquire by virtue of such employment, except as authorized by competent authority pursuant to the provisions of Federal statutes, regulations and directives. Should an attempt be made by any unauthorized person to obtain classified information from me I will report such incident to the Staff Security Officer for the Office of the Vice President, the nearest office of the Federal Bureau of Investigation or to the nearest U.S. Embassy, Consulate or U.S. Military Command.
4. I understand that upon the termination of my employment by or assignment to the Vice President's staff, none of the classified information or material to which I have access or which I have originated in the course of that employment or assignment may be removed or retained by me, except as authorized by competent authority.

5. I understand that a change in my assignment or employment will not relieve me of my obligations under this statement, and that the provisions of this statement will remain binding upon me after termination of my service with the Office of the Vice President and my services with the United States Government.

______________________________
Signature

Witnessed and accepted in behalf of the Vice President of the United States on

__________, 19__, by __________________________
SECURITY TERMINATION STATEMENT

On the occasion of the termination of my employment by or assignment to the staff of the Office of the Vice President, I hereby state that:

1) I am not retaining possession of or taking with me any document or other material containing classified information affecting the national defense or foreign relations of the United States.

2) I will not hereafter in any manner reveal or divulge any such classified information of which I have gained knowledge during my employment by or assignment to the Office of the Vice President, except as authorized by competent authority pursuant to the provisions of Federal statutes, regulations and directives. Should an attempt be made by any unauthorized person to obtain such classified information from me, I will report the incident to the Staff Security Officer of the Office of the Vice President, the nearest office of the Federal Bureau of Investigation, or the nearest U.S. Embassy, Consulate, or U.S. Military Command.

3) I have read and understand the provisions of the Espionage Act, Title 18, USC, Sections 793 and 794, concerning unlawful disclosure of information affecting the national defense, and the provisions of Title 18, USC, Section 1001, regarding the making of false statements. With this understanding, I state that the information I have given herein is, to the best of my knowledge and belief, correct and complete and is being furnished to the U.S. Government for purposes of protection of classified information which affects the national defense, or foreign relations, of the United States.

__________________________  __________________________
date                     signature

__________________________  __________________________
WITNESS                   name (typed or printed)
January 25, 1979

MEMORANDUM FOR The Vice President
FROM: A. Staff Member
SUBJECT: Classified Markings (U)

XXX XXXXXX xx X XXXXXXXXXX XXXXXXXX XXXXX XX
XX XXXXXX XXXXXXXX XXX XXXXXXXXXX XXXXXXXX XXXXXX
XX XXXXXXXX. XX XXX XXX XXX XXX XXXXXX XX XX
XX XXXXXX XXXXXXXXXX XXXXXXXX XX XXXXXX XX. (C)

XXX XXXX XXXX XXXX XX XXX XXX XXX XXX XXXXXXXX
XXX XXX XXX XXX XXX XXX XXXXXXXXXX XXXXXXXX. XXXX XXX-
XXX XXX XXX XXX XXX XXXXXXXXXX XXXXXXXX. (S)

XXX XXXXXX XXXXX XX XXXXXX XXX XXXXXX
XXX XXXXXX XX XXX XXXXXX. (U)

X XX XXXXXXXX XXX XXXXXXXXX XXXXXXXXXX XX XXX XXX
XXX XXXXXX XXX XXX XXX XXX XXX XXX XXXXXX XXXXXX
XXX XXX XXX XXX XXX XXX XXXXXXXXXX XXX XXX XXX XXX
XX XXX XXX XXXXXXXXXX XXXXXX XXXXXX. XXXXXX XXX XXX
XXX XXXXXX XXXXXX. (TS)

Classified by Director, XXX
Declasify on January 24, 1984
Review for Declassification on January 24, 1984
Downgrade to __________ on __________ Enter appropriate terminology