and to facilitate its control, foreign government information should be stored separately from other classified information. To avoid additional costs, separate storage may be accomplished by methods such as separate drawers of a container. The safeguarding standards described below may be modified if required or permitted by treaties or agreements, or for other obligations, with the prior written consent of the National Security Authority of the originating government.

1. Top Secret. Records shall be maintained of the receipt, internal distribution, destruction, access, reproduction, and transmittal of foreign government Top Secret information. Reproduction requires the consent of the originating government. Destruction will be witnessed.

2. Secret. Records shall be maintained of the receipt, external dispatch and destruction of foreign government Secret information. Other records may be necessary if required by the originator. Secret foreign government information may be reproduced to meet mission requirements unless prohibited by the originator. Reproduction shall be recorded unless this requirement is waived by the originator.

3. Confidential. Records need not be maintained for foreign government Confidential information unless required by the originator.

4. Restricted and other foreign government information provided in confidence. In order to assure the protection of other foreign government information provided in confidence (e.g., foreign government “Restricted,” “Designated,” or unclassified provided in confidence), such information must be classified under E.O. 12958. The receiving agency, or a receiving U.S. contractor, licensee, grantee, or certificate holder acting in accordance with instructions received from the U.S. Government, shall provide a degree of protection to the foreign government information at least equivalent to that required by the government or international organization that provided the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to US CONFIDENTIAL information. If the foreign protection requirement is lower than the protection required for US CONFIDENTIAL information, the following requirements shall be met:

a. Documents may retain their original foreign markings if the responsible agency determines that these markings are adequate to meet the purposes served by U.S. classification markings. Otherwise, documents shall be marked, “This document contains (insert name of country) (insert classification level) information to be treated as US (insert classification level).” The notation, “Modified Handling Authorized,” may be added to either the foreign or U.S. markings authorized for foreign government information. If remarking foreign originated documents or matter is impractical, an approved cover sheet is an authorized option.

b. Documents shall be provided only to those who have an established need-to-know, and where access is required by official duties.

c. Individuals being given access shall be notified of applicable handling instructions. This may be accomplished by a briefing, written instructions, or by applying specific handling requirements to an approved cover sheet.

d. Documents shall be stored in such a manner so as to prevent unauthorized access.

e. Documents shall be transmitted in a method approved for classified information, unless this method is waived by the originating government.

5. Third-country transfers. The release or disclosure of foreign government information to any third-country entity must have the prior consent of the originating government if required by a treaty, agreement, bilateral exchange, or other obligation.
CHAPTER XXI—NATIONAL SECURITY COUNCIL

\begin{center}
\begin{tabular}{lll}
\textit{Part} & Rules and regulations to implement the Privacy Act of 1974
\hspace{1cm} & Page \\
2102 & \hspace{1cm} & 525 \\
2103 & Regulations to implement E.O. 12065—including procedures for public access to documents that may be declassified & 528 \\
\end{tabular}
\end{center}
PART 2102—RULES AND REGULATIONS TO IMPLEMENT THE PRIVACY ACT OF 1974

Sec. 2102.1 Introduction.
2102.2 Purpose and scope.
2102.3 Definitions.
2102.4 Procedures for determining if an individual is the subject of a record.
2102.13 Requirements for access to a record.
2102.15 Requirements for requests to amend records.
2102.21 Procedures for appeal of determination to deny access to or amendment of requested records.
2102.31 Disclosure of a record to persons other than the individual to whom it pertains.
2102.41 Fees.
2102.51 Penalties.
2102.61 Exemptions.

AUTHORITY: 5 U.S.C. 552a (f) and (k).
SOURCE: 40 FR 47746, Oct. 9, 1975, unless otherwise noted.

§ 2102.1 Introduction.
(a) Insofar as the Privacy Act of 1974 (5 U.S.C. 552a) applies to the National Security Council (hereafter NSC), it provides the American public with expanded opportunities to gain access to records maintained by the NSC Staff which may pertain to them as individuals. These regulations are the exclusive means by which individuals may request personally identifiable records and information from the National Security Council.

(b) The NSC Staff, in addition to performing the functions prescribed in the National Security Act of 1947, as amended (50 U.S.C. 401), also serves as the supporting staff to the President in the conduct of foreign affairs. In doing so the NSC Staff is acting not as an agency but as an extension of the White House Office. In that the White House Office is not considered an agency for the purposes of this Act, the materials which are used by NSC Staff personnel in their role as supporting staff to the President are not subject to the provisions of the Privacy Act of 1974. A description of these White House Office files is, nevertheless, appended to the NSC notices of systems of files and will be published annually in the Federal Register.

(c) In general, Records in NSC files pertain to individual members of the public only if these individuals have been (1) employed by the NSC, (2) have corresponded on a foreign policy matter with a member of the NSC or its staff, or (3) have, as a U.S. Government official, participated in an NSC meeting or in the preparation of foreign policy-related documents for the NSC.

§ 2102.2 Purpose and scope.
(a) The following regulations set forth procedures whereby individuals may seek and gain access to records concerning themselves and will guide the NSC Staff response to requests under the Privacy Act. In addition, they outline the requirements applicable to the personnel maintaining NSC systems of records.

(b) These regulations, published pursuant to the Privacy Act of 1974, Pub. L. 93–579, Section 552a (f) and (k), 5 U.S.C. (hereinafter the Act), advise of procedures whereby an individual can:
1. Request notification of whether the NSC Staff maintains or has disclosed a record pertaining to him or her in any non-exempt system of records;
2. Request a copy of such record or an accounting of that disclosure;
3. Request an amendment to a record; and,
4. Appeal any initial adverse determination of any request under the Act.

(c) These regulations also specify those systems of records which the NSC has determined to be exempt from certain provisions of the Act and thus not subject to procedures established by this regulation.

§ 2102.3 Definitions.
As used in these regulations:
(a) Individual. A citizen of the United States or an alien lawfully admitted for permanent residence.
(b) Maintain. Includes maintain, collect, use or disseminate. Under the Act it is also used to connote control over, and, therefore, responsibility for, systems of records in support of the NSC statutory function (50 U.S.C. 401, et seq.).
(c) Systems of Records. A grouping of any records maintained by the NSC from which information is retrieved by
§ 2102.4 Procedures for determining if an individual is the subject of a record.

(a) Individuals desiring to determine if they are the subject of a record or system of records maintained by the NSC Staff should address their inquiries, marking them plainly as a PRIVACY ACT REQUEST, to:

Staff Secretary, National Security Council, Room 374, Old Executive Office Building, Washington, DC 20506.

All requests must be made in writing and should contain:

(1) A specific reference to the system of records maintained by the NSC as listed in the NSC Notices of Systems and Records (copies available upon request); or

(2) A description of the record or systems of records in sufficient detail to allow the NSC to determine whether the record does, in fact, exist in an NSC system of records.

(b) All requests must contain the printed or typewritten name of the individual to whom the record pertains, the signature of the individual making the request, and the address to which the reply should be sent. In instances when the identification is insufficient to insure disclosure to the individual to whom the information pertains in view of the sensitivity of the information, NSC reserves the right to solicit from the requestor additional identifying information.

(c) Responses to all requests under the Act will be made by the Staff Secretary, or by another designated member of the NSC Staff authorized to act in the name of the Staff Secretary in responding to a request under this Act. Every effort will be made to inform the requestor if he or she is the subject of a specific record or system of records within ten working days (excluding Saturdays, Sundays and legal Federal Holidays) of receipt of the request. Such a response will also contain the procedures to be followed in order to gain access to any record which may exist and a copy of the most recent NSC notice, as published in the FEDERAL REGISTER, on the system of records in which the record is contained.

(d) Whenever it is not possible to respond in the time period specified above, the NSC Staff Secretary or a designated alternate will, within ten working days (excluding Saturdays, Sundays, and legal Federal Holidays), inform the requestor of the reasons for the delay (e.g., insufficient requestor information, difficulties in record location, etc.), steps that need to be taken in order to expedite the request, and the date by which a response is anticipated.

§ 2102.13 Requirements for access to a record.

(a) Individuals requesting access to a record or system of records in which there is information concerning them must address a request in writing to the Staff Secretary of the NSC (see § 2102.1). Due to restricted access to NSC offices in the Old Executive Office Building where the files are located, requests cannot be made in person.

(b) All written requests should contain a concise description of the records to which access is requested. In addition, the requestor should include any other information which he or she feels would assist in the timely identification of the record. Verification of the requestor’s identity will be determined under the same procedures used in requests for learning of the existence of a record.

(c) To the extent possible, any request for access will be answered by the Staff Secretary or a designated alternate within ten working days (excluding Saturdays, Sundays, and legal Federal holidays) of the receipt of the
request. In the event that a response cannot be made within this time, the requestor will be notified by mail of the reasons for the delay and the date upon which a reply can be expected.

(d) The NSC response will forward a copy of the requested materials unless further identification or clarification of the request is required. In the event access is denied, the requestor shall be informed of the reasons therefore and the name and address of the individual to whom an appeal should be directed.

§ 2102.15 Requirements for requests to amend records.

(a) Individuals wishing to amend a record contained in the NSC systems of records pertaining to them must submit a request in writing to the Staff Secretary of the NSC in accordance with the procedures set forth herein.

(b) All requests for amendment or correction of a record must state concisely the reason for requesting the amendment. Such requests should include a brief statement which describes the information the requestor believes to be inaccurate, incomplete, or unnecessary and the amendment or correction desired.

(c) To the extent possible, every request for amendment of a record will be answered within ten working days (excluding Saturdays, Sundays, and legal Federal holidays) of the receipt of the request. In the event that a response cannot be made within this time, the requestor will be notified by mail of the reasons for the delay and the date upon which a reply can be expected. A final response to a request for amendment will include the NSC Staff determination on whether to grant or deny the request. If the request is denied, the response will include:

(1) The reasons for the decision;
(2) The name and address of the individual to whom an appeal should be directed;
(3) A description of the process for review of the appeal within the NSC; and
(4) A description of any other procedures which may be required of the individual in order to process the appeal.

§ 2102.21 Procedures for appeal of determination to deny access to or amendment of requested records.

(a) Individuals wishing to appeal an NSC Staff denial of a request for access or to amend a record concerning them must address a letter of appeal to the Staff Secretary of the NSC. The letter must be received within thirty days from the date of the Staff Secretary’s notice of denial and, at a minimum, should identify the following:

(1) The records involved;
(2) The dates of the initial request and subsequent NSC determination; and
(3) A brief statement of the reasons supporting the request for reversal of the adverse determination.

(b) Within thirty working days (excluding Saturdays, Sundays and legal Federal holidays) of the date of receipt of the letter of appeal, the Assistant to the President for National Security Affairs (hereinafter the “Assistant”), or the Deputy Assistant to the President for National Security Affairs (hereinafter the “Deputy Assistant”), acting in his name, shall issue a determination on the appeal. In the event that a final determination cannot be made within this time period, the requestor will be informed of the delay, the reasons therefor and the date on which a final response is expected.

(c) If the original request was for access and the initial determination is reversed, a copy of the records sought will be sent to the individual. If the initial determination is upheld, the requestor will be so advised and informed of the right to judicial review pursuant to 5 U.S.C. 552a(g).

(d) If the initial denial of a request to amend a record is reversed, the records will be corrected and a copy of the amended record will be sent to the individual. If the initial determination is upheld by the Assistant to the President, the requestor will be so advised and informed of his or her right to seek judicial review of the final agency determination, pursuant to section 552a(g) of title 5, U.S.C. In addition, the requestor will be advised of his right to have a concise statement of the reasons for disagreeing with the final determination appended to the disputed records. This statement
§ 2102.31 Disclosure of a record to persons other than the individual to whom it pertains.

(a) Except as provided by the Privacy Act, 5 U.S.C. 552a(b), the NSC will not disclose a record concerning an individual to another person or agency without the prior written consent of the individual to whom the record pertains.

§ 2102.41 Fees.

(a) Individuals will not be charged for:

(1) The first copy of any record provided in response to a request for access or amendment;

(2) The search for, or review of, records in NSC files;

(3) Any copies reproduced as a necessary part of making a record or portion thereof available to the individual.

(b) After the first copy has been provided, records will be reproduced at the rate of twenty-five cents per page for all copying of four pages or more.

(c) The Staff Secretary may provide copies of a record at no charge if it is determined to be in the interest of the Government.

(d) The Staff Secretary may require that all fees be paid in full prior to the issuance of the requested copies.

(e) Remittances shall be in the form 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 “United States Treasury” and mailed to the Staff Secretary, National Security Council, Washington, DC 20506.

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

§ 2102.51 Penalties.

Title 18, U.S.C. section 1001, Crimes and Criminal Procedures, makes it a criminal offense, subject to a maximum fine of $10,000 or imprisonment for not more than five years or both, to knowingly and willfully make or cause to be made any false or fraudulent statements or representations in any matter within the jurisdiction of any agency of the United States. Section (i)(3) of the Privacy Act (5 U.S.C. 552a) makes it a misdemeanor, subject to a maximum fine of $5,000, to knowingly and willfully request or obtain any record concerning an individual under false pretenses. Sections (i)(1) and (2) of 5 U.S.C. 552a provide penalties for violations by agency employees, of the Privacy Act or regulations established thereunder.

§ 2102.61 Exemptions.

Pursuant to subsection (k) of the Privacy Act (5 U.S.C. 552a), the Staff Secretary has determined that certain NSC systems of records may be exempt in part from sections 553(c)(3), (d), (e)(1), (e)(4), (G), (H), (I), and (f) of title 5, and from the provisions of these regulations. These systems of records may contain information which is classified pursuant to Executive Order 11652. To the extent that this occurs, records in the following systems would be exempt under the provision of 5 U.S.C. 552a(k)(1):

NSC 1.1—Central Research Index,
NSC 1.2—NSC Correspondence Files, and
NSC 1.3—NSC Meetings Registry.

PART 2103—REGULATIONS TO IMPLEMENT E.O. 12065—INCLUDING PROCEDURES FOR PUBLIC ACCESS TO DOCUMENTS THAT MAY BE DECLASSIFIED

Subpart A—Introduction

Sec.
2103.1 References.
2103.2 Purpose.
2103.3 Applicability.

Subpart B—Original Classification

2103.11 Basic policy.
2103.12 Level of original classification.
2103.13 Duration of original classification.
2103.14 Challenges to classification.

Subpart C—Derivative Classification

2103.21 Definition and application.
Subpart D—Declassification and Downgrading

§ 2103.31 Declassification authority.
§ 2103.32 Mandatory review for declassification.
§ 2103.33 Downgrading authority.

Subpart E—Safeguarding

§ 2103.41 Reproduction controls.

Subpart F—Implementation and Review

§ 2103.51 Information Security Oversight Committee.
§ 2103.52 Classification Review Committee.


SOURCE: 44 FR 2384, Jan. 11, 1979, unless otherwise noted.

Subpart A—Introduction

§ 2103.1 References.

§ 2103.2 Purpose.
The purpose of this regulation is to ensure, consistent with the authorities listed in §2103.1, that national security information processed by the National Security Council Staff is protected from unauthorized disclosure, but only to the extent, and for such period, as is necessary to safeguard the national security.

§ 2103.3 Applicability.
This regulation governs the National Security Council Staff Information Security Program. In consonance with the authorities listed in §2103.1, it establishes the policy and procedures for the security classification, downgrading, declassification, and safeguarding of information that is owned by, is produced for or by, or is under the control of the National Security Council Staff.

Subpart B—Original Classification

§ 2103.11 Basic policy.
It is the policy of the National Security Council Staff to make available to the public as much information concerning its activities as is possible, consistent with its responsibility to protect the national security.

§ 2103.12 Level of original classification.
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 Executive Order 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.

§ 2103.13 Duration of original classification.
Original classification may be extended beyond six years only by officials with Top Secret classification authority. This extension authority shall be used only when these officials determine that the basis for original classification will continue throughout the entire period that the classification will be in effect and only for the following reasons:
(a) The information is “foreign government information” as defined by the authorities in §2301.1;
(b) The information reveals intelligence sources and methods;
(c) The information pertains to communication security;
(d) The information reveals vulnerability or capability data, the unauthorized disclosure of which can reasonably be expected to render ineffective a system, installation, or project important to the national security;
(e) The information concerns plans important to the national security, the unauthorized disclosure of which reasonably can be expected to nullify the effectiveness of the plan;
(f) The information concerns specific foreign relations matters, the continued protection of which is essential to the national security;
§ 2103.14 Challenges to classification.
If holders of classified information believe that 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 chairperson of the NSC Information Security Oversight Committee (see §2103.51 of this part).

Subpart C—Derivative Classification
§ 2103.21 Definition and application.
Derivative classification is the act of assigning a level of classification to information that is determined to be the same in substance as information that 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.

Subpart D—Declassification and Downgrading
§ 2103.31 Declassification authority.
The Staff Secretary, Staff Counsel, and Director of Freedom of Information of the National Security Council Staff are authorized to declassify NSC documents after consultation with the appropriate NSC Staff members.

§ 2103.32 Mandatory review for declassification.
(a) Receipt. (1) Requests for mandatory review for declassification under section 3-501 of Executive Order 12065 must be in writing and should be addressed to:
National Security Council, ATTN: Staff Secretary (Mandatory Review Request), Old Executive Office Building, Washington, DC 20506.
(2) The requestor shall be informed of the date of receipt of the request. This date will be the basis for the time limits specified in paragraph (b) 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.
(b) Review. (1) The requestor shall be informed of the National Security Council Staff determination within sixty days of receipt of the initial request.
(2) If the determination is to withhold some or all of the material requested, the requestor may appeal the determination. The requestor shall be informed that such an appeal must be made in writing within sixty days of receipt of the denial and should be addressed to the chairperson of the National Security Council Classification Review Committee.
(3) The requestor shall be informed of the appellate determination within thirty days of receipt of the appeal.
(c) Fees. (1) Fees for the location and reproduction of information that is the subject of a mandatory review request shall be assessed according to the following schedule:
(i) 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 $.25 per page for all copying of four pages or more. No fee shall be assessed for reproducing documents that are three pages or less, or for the first three pages of longer documents.
§ 2103.52 Classification Review Committee.

The NSC Classification Review Committee shall be chaired by the Staff Secretary of the National Security Council. The Committee shall decide appeals from denials of declassification requests submitted pursuant to section 3-5 of Executive Order 12065. The Committee shall consist of the chairperson, the NSC Director of Freedom of Information, and the NSC Staff member with primary subject matter responsibility for the material under review.

§ 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.

§ 2103.41 Reproduction controls.

The Staff Secretary shall maintain records to show the number and distribution of all Top Secret documents, of all documents covered by special access programs distributed outside the originating agency, and of all Secret and Confidential documents that are marked with special dissemination or reproduction limitations.

Subpart F—Implementation and Review

§ 2103.51 Information Security Oversight Committee.

The NCS Information Security Oversight Committee shall be chaired by the Staff Counsel of the National Security Council Staff. The Committee shall be responsible for acting on all suggestions and complaints concerning the administration of the National Security Council information security program. The chairperson, who shall represent the NSC Staff on the Interagency Information Security Committee shall also be responsible for conducting an active oversight program to ensure effective implementation of Executive Order 12065.

§ 2103.52 Classification Review Committee.

The NSC Classification Review Committee shall be chaired by the Staff Secretary of the National Security Council. The Committee shall decide appeals from denials of declassification requests submitted pursuant to section 3-5 of Executive Order 12065. The Committee shall consist of the chairperson, the NSC Director of Freedom of Information, and the NSC Staff member with primary subject matter responsibility for the material under review.