AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO



Privacy Act of 1974, in accordance with the provisions of those acts. (*See*, 12 CFR part 404 and 12 CFR part 405, respectively.) In any case, however, exemptions under the Freedom of Information Act or other exemptions under applicable law may be invoked by the Bank to deny material on grounds other than classification.

(i) The Bank shall refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classifiable under the Order.

### § 403.8 Appeals.

(a) The Vice Chairman is designated to receive appeals on requests for declassification which have been denied by the Bank. Such appeals shall be addressed to:

First Vice President & Vice Chairman, Export-Import Bank of the United States, 811 Vermont Avenue NW., Washington, DC 20571

The appeal must be received within 60 days after receipt by appellant of the denial letter. Appeals shall be decided within 30 days of their receipt by the Vice Chairman.

(1) If the decision is to declassify the materials in their entirety, the Vice Chairman shall promptly make such information available to the requester, and inform the requester of any fees due before releasing the documents.

(2) If the decision is to deny declassification of a portion of the material, the Vice Chairman shall promptly make the part which was declassified available to the requester, and shall advise the requester, in writing, of the reasons for the partial denial of declassification.

(3) If the decision is to deny declassification of all the material, the Vice Chairman shall promptly advise the requester, in writing, of the reasons for such denial.

### § 403.9 Fees.

The following specific fees shall be applicable with respect to services rendered to members of the public under these regulations, by the Bank, except that the search fee will normally be waived when the search involves less than one-half hour of clerical time.

| | |
|---|---|
| (a) Search for records, per hour or fraction thereof: | |
| (i) Professional | $11.00 |
| (ii) Clerical | 6.00 |
| (b) Computer service charges per second for actual use of computer central processing unit | .25 |
| (c) Copies made by photostat or otherwise (per page); maximum of 5 copies will be provided | .10 |
| (d) Certification of each record as a true copy | 1.00 |
| (e) Certification of each record as a true copy under official seal | 1.50 |
| (f) Duplication of architectural photographs and drawings | 2.00 |

Fees must be paid in full prior to issuance of requested copies. Remittances shall be in the form either of a personal check or bank draft drawn on a bank in the United States, or postal money order. Remittances shall be made payable to the order of the Export-Import Bank of the United States, and mailed to:

General Counsel, Export-Import Bank of the United States, 811 Vermont Avenue NW., Washington, DC 20571

### § 403.10 Safeguarding.

(a) *General Access Requirements*. Except as provided in § 403.10(c), access to classified information shall be granted in accordance with the following:

(1) *Determination of Trustworthiness*. No person shall be given access to classified information or material unless a favorable determination has been made as to his trustworthiness. The determination of eligibility, referred to as a security clearance, shall be based on such investigations as the Bank may require in accordance with the standards and criteria of applicable law and Executive orders.

(2) *Determination of Need to Know*. In addition to a security clearance, a person must have a need for access to the particular classified information or material sought in connection with the performance of official duties or contractual obligations. The determination of that need shall be made by officials having responsibility for the classified information or material.

(b) *Classified Information Nondisclosure Agreement*. All persons with authorized access to classified information shall be required to sign a nondisclosure agreement, Standard Form 189, as a

condition of access. This form shall be retained in the security file of the individual for 50 years.

(c) *Access by Historical Researchers and Former Presidential Appointees.* The Bank shall obtain written agreements from requesters to safeguard the information to which they are given access as permitted by the Order and written consent to the Bank's review of their notes and manuscripts for the purpose of determining that no classified information is contained therein. A determination of trustworthiness is a precondition to a requester's access. If the access requested by historical researchers and former Presidential Appointees requires the rendering of services for which fair and equitable fees may be charged pursuant to title 5 of the Independent Offices Appropriations Act, 65 Stat. 290, 31 U.S.C. 483a (1976), the requester shall be so notified and the fees may be imposed.

(d) *Media Contacts.* All contacts by members of the media which concern classified information shall be directed to the attention of the Security Officer, Room 1031, Export-Import Bank of the United States, 811 Vermont Avenue NW., Washington, DC 20571.

(e) *Dissemination.* Except as otherwise provided by directives issued by the President through the National Security Council, classified information originating in another agency and in the possession of the Bank may not be disseminated outside the Bank without the consent of the originating agency.

(f) *Accountability Procedures.* Dissemination of various levels of classified information or material shall be within the control and responsibility of designated control officers. Particularly stringent controls shall be placed on information and material classified as TOP SECRET.

(1) *TOP SECRET.* Designated as TOP SECRET control officers are the Chairman, Vice Chairman and the Security Officer who alone have authority to receive TOP SECRET information for the Bank. Other personnel authorized in writing by the Chairman or Security Officer also may receive TOP SECRET information for the Bank. It shall be the responsibility of these individuals with respect to all TOP SECRET information:

(i) To receive the material for the Bank;

(ii) To maintain registers which will reflect the routing of the material and the return thereof in a reasonable length of time for security storage;

(iii) To dispatch and make record of material disseminated to authorize persons outside the Bank;

(iv) To make a physical inventory of all material at least annually; and

(v) To maintain current access records.

(2) *SECRET.* Designated as SECRET control officers are the Security Officer and the Analysis, Records & Communications Manager, who have the responsibility with respect to all information classified in this category:

(i) To receive the material for the Bank;

(ii) To maintain registers which will reflect the routing of the material and the return thereof in a reasonable length of time for security storage;

(iii) To dispatch and make record of material disseminated to authorized persons outside the Bank;

(iv) To maintain current access records.

(3) *CONFIDENTIAL.* Designated as CONFIDENTIAL control officers are the Security Officer and the Analysis, Records & Communications Manager who have responsibility with respect to all information classified in this category:

(i) To review material for the Bank;

(ii) To route the material to proper Bank offices;

(iii) To dispatch and make record of material disseminated to authorized persons outside the Bank;

(iv) To maintain current access records.

(g) *Storage.* Classified information shall be stored only in facilities or under conditions adequate to prevent unauthorized persons from gaining access to it and in accordance with the Directive as well as General Services Administration standards and specifications. Reference may be made to 32 CFR 2001.41, 2001.43 for preliminary guidance regarding these standards and specifications.

(h) *Coversheets.* Department of State (DSC) classified incoming cables are to

be logged in and routed to the appropriate offices in double envelopes. When these cables are being used in various offices, classified coversheets must be used to protect the documents. This practice eliminates the possibility of inadvertently mixing classified with non-classified material, and promotes security awareness. Coversheets are obtainable from the Office of the Security Director.

(i) *Transmittal.* (1) To be transmitted outside the Bank, all classified documents must be sent through the Security Office and have attached EIB Form 71–2, approved by one of the following: the President and Chairman, First Vice President and Vice Chairman, a Senior Vice President, General Counsel, Vice President or Security Officer.

(2) *Preparation and Receipting.* Classified information shall be enclosed in opaque inner and outer covers before transmitting. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee. Transmittal documents shall indicate on their face the highest level of any information transmitted, and must clearly state whether or not the transmittal document itself is classified after removal of enclosures and attachments. The outer cover shall be sealed and addressed with no identification of the classification of its contents. A receipt shall be attached to or enclosed in the inner cover, except that CONFIDENTIAL information shall require a receipt only if the sender deems it necessary. The receipt shall identify the sender, addressee, and the document but shall contain no classified information. It shall be immediately signed by the recipient and returned to the sender. Any of these wrapping and receipting requirements may be waived by agency heads under conditions that will provide adequate protection and prevent access by unauthorized persons.

(3) *Transmittal of CONFIDENTIAL information.* CONFIDENTIAL information shall be transmitted within and between the fifty States, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories or possessions by one of the means established for higher classifications, or by United States Postal Service, certified first class, or express mail service, when prescribed by an agency head. Outside these areas, CONFIDENTIAL information shall be transmitted only as is authorized for higher classification levels.

(4) Transmittal of TOP SECRET and SECRET information shall be in accordance with the Directive. Reference may be made to 32 CFR 2001.44 for preliminary guidance.

(j) *Destruction.* Classified information no longer needed in working files or for record or reference purposes shall be processed for appropriate disposition in accordance with Chapters 21 and 33 of title 44 U.S.C., when govern disposition of Federal Records. All classified information approved for destruction must be torn and placed in containers designated as burnbags which are available through the Office Services Section of the Bank. Destruction of such information will be carried out by the Security Officer or a designee by use of a disintegrator or by burning. The method of destruction selected must preclude recognition or reconstruction of the classified information or material. Records of destruction will be maintained by the Security Office for TOP SECRET information and material with serialized markings or material for which there is a special need to record its destruction.

(k) *Reproduction controls.* (1) Reproduction of classified documents is prohibited, except by personnel authorized in writing by the Chairman or Security Officer.

(2) TOP SECRET documents may not be reproduced without the consent of the originating agency unless otherwise marked by the originating office.

(3) Reproduction of SECRET and CONFIDENTIAL documents may be restricted by the originating agency.

(4) Reproduced copies of classified documents are subject to the same accountability and controls as the original documents.

(5) Records shall be maintained by the Security Officer to show the number and distribution or reproduced copies of all TOP SECRET documents, of all documents covered by special access programs distributed outside the

originating agency, and all SECRET and all CONFIDENTIAL documents which are marked with special dissemination and reproduction limitations.

### § 403.11 Enforcement and investigation procedures.

(a) *Loss or Possible Compromise.* Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to the Security Officer of the Bank. In turn, the originating agency shall be notified about the loss or compromise in order that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect, and prevent further such loss or compromise. An immediate inquiry shall be initiated by the Bank for the purposes: (1) Of determining cause and responsibility and (2) taking corrective measures and appropriate administrative, disciplinary, or legal action.

(b) *Reporting and Investigating Unauthorized Disclosures.* (1) Employees who have reason to believe that an unauthorized disclosure of classified information has occurred shall report the disclosure to their supervisor, who shall inform the Security Officer.

(2) The Bank shall promptly notify the Information Security Oversight Office at the General Services Administration, Washington, DC 20405, of all unauthorized disclosures of classified information.

(3) If the Bank believes that it is the source of an unauthorized disclosure of classified information that it originated, it shall evaluate the disclosure under paragraph (b)(7) of this section. If the disclosure is serious, the Bank shall report the disclosure and the results of the evaluation to the Department of Justice together with notification that it is conducting an internal investigation.

(4) If the Bank believes that it is the source of an unauthorized disclosure of classified information that it handled but did not originate, it shall report the disclosure to the Department of Justice and to the originating agency(ies) or department(s) for evaluation under paragraph (b)(7) of this section. If the Bank cannot determine the identity of the originating agency(ies) or department(s), it shall report the disclosure to the Department of Justice together with any information or reasonable inferences as to the identity of the originating agency(ies) or department(s).

(5) If the Bank receives a request for an evaluation of information it originated, it shall, if the evaluation shows the disclosure was serious, inform the agency(ies) or department(s) from which the disclosure occurred of this conclusion and request that the agency(ies) or department(s) conduct an internal investigation.

(6) If the Bank determines that an unauthorized disclosure of classified information has occurred but that it neither originated, handled nor disclosed the information, it shall report the disclosure to the likely originating agency(ies) or department(s).

(7) In determining whether a disclosure is sufficiently serious to warrant reporting to the Department of Justice, the Bank, if it is the originating agency, shall ascertain the nature of the disclosed information, determine the extent to which it disseminated the information and evaluate the disclosure to determine whether it seriously damages its mission and responsibilities. In evaluating the damage caused by the disclosure, the Bank shall consider such matters as whether the disclosure jeopardizes an ongoing project, operation or source of information and to what extent the policy goals underlying the project or operation must be altered.

(8) In any instance where the Bank is determined to be the source of an unauthorized disclosure and an evaluation by the Bank or the originating agency(ies) or department(s) determines the disclosure to be of a serious nature, an internal investigation will be initiated and an investigation report, containing such information as may be required by the Department of Justice, will be submitted to the Department of Justice within 15 days after notification from the originating agency or Department of Justice, but in any case no later than 30 days. If the investigation report is not completed within 15 days, the Bank shall submit as much of the required information as is available at that time and furnish