PART 400—EMPLOYEE FINANCIAL DISCLOSURE AND ETHICAL CONDUCT STANDARDS REGULATIONS

AUTHORITY: 5 U.S.C. 7301.

SOURCE: 60 FR 17628, Apr. 7, 1995, unless otherwise noted.

§ 400.101 Cross-reference to employee financial disclosure and ethical conduct standards regulations.

Employees of the Export-Import Bank of the United States (Bank) should refer to:

(a) The executive branch-wide financial disclosure regulations at 5 CFR part 2634;

(b) The executive branch-wide Standards of Ethical Conduct at 5 CFR part 2635; and

(c) The Bank regulations at 5 CFR part 6201 which supplement the executive branch-wide standards.

PART 403—CLASSIFICATION, DECLASSIFICATION, AND SAFEGUARDING OF NATIONAL SECURITY INFORMATION

Sec.

AUTHORITY: E.O. 12356, National Security Information, April 2, 1982 (3 CFR, 1982 Comp. p. 166) (hereafter referred to as the *Order*), Information Security Oversight Directive No. 1, June 25, 1982 (32 CFR part 2001) (hereafter referred to as the *Directive*), and National Security Decision Directive 84, ''Safeguarding National Security Information,'' signed by the President on March 11, 1983 (hereafter referred to as *NSDD 84*).

SOURCE: 50 FR 27215, July 2, 1985, unless otherwise noted.

§ 403.1 General policies and definitions.

(a) This regulation of the Export-Import Bank (the Bank) implements executive orders which govern the classification, declassification, and safeguarding of national security information and material of the United States. This regulation is based on Executive Order 12356, National Security Information, April 2, 1982 (3 CFR, 1982 Comp. p. 166) (hereafter referred to as the *Order*), Information Security Oversight Directive No. 1, June 25, 1982 (32 CFR part 2001) (hereafter referred to as the *Directive*), and National Security Decision Directive 84, ''Safeguarding National Security Information,'' signed by the President on March 11, 1983 (hereafter referred to as *NSDD 84*). Violation of the provisions of part 403 may result in the imposition of administrative penalties, and civil and criminal penalties under applicable law. Executive Order 12356 prescribes a uniform system for classifying, declassifying, and safeguarding national security information. It recognizes that it is essential that the public be informed concerning the activities of the Government, but that the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure. Information may not be classified under the Order unless its disclosure reasonably could be expected to cause damage to the national security.

(b) For the purposes of the Order, the Directive and these guidelines, the following terms shall have the meanings specified below:

(1) *Information* means any information or material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government.

(2) *National security information* means information that has been determined pursuant to this Order or any predecessor order to require protection against unauthorized disclosure and that is so designated.

(3) *Foreign government information* means:

(i) Information provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the

information, the source of the information, or both, are to be held in confidence; or

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

(4) *National security* means the national defense or foreign relations of the United States.

(5) *Confidential source* means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship, or both, be held in confidence.

(6) *Original classification* means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

§ 403.2 Responsibilities.

In the carrying out of security procedures, responsibility falls on all personnel generally and on certain personnel in a more particular manner.

(a) *Individual.* Each employee of the Bank having access to classified material has an individual responsibility to protect such information. Classified information should be secured in approved equipment or facilities whenever it is not under the direct control of the employee.

(b) *Office and Division Heads.* These officials have the additional responsibility of a continuing review for ascertaining that security procedures are properly observed by the personnel comprising their respective offices.

(c) *Security Officer.* (1) The Security Officer has the responsibility for developing, inspecting, and advising on procedures and controls for safeguarding classified material originating in, received by, in transit through, or in custody of the Bank; the training and orientation of employees; the carrying out of inspections; and the destruction of obsolete and non-record material.

(2) The Security Officer shall be responsible for disseminating written material and conducting oral briefings to inform Bank personnel of the Order, Directive, and regulations. An explanation of the practical application of these procedures and the underlying policy objectives thereof shall be emphasized.

(d) *Security Committee.* (1) This Committee consists of the General Counsel, as Chairperson, the Security Officer, and other Bank employees, as designated by the President and Chairman (hereinafter referred to as the *Chairman)* and is responsible for the implementation and enforcement of the Order and the Directive. This Committee will act on all matters with respect to the Bank's administration of these regulations.

(2) All suggestions and complaints regarding the Bank's Information Security Program, including those regarding over-classification, failure to declassify, or delay in declassifying, not otherwise provided for herein, shall be referred to the Security Committee for review.

(3) The Security Committee shall have responsibility for recommending to the Chairman appropriate administrative action to correct abuse or violation of these regulations or of any provision of the Order or Directive thereunder, including but not limited to notification by warning letter, formal suspension without pay, and removal. Upon receipt of such a recommendation, the Chairman shall make a decision and advise the Security Committee of this action.

§ 403.3 Classification principles and authority.

(a) *Classification Principles.* (1) Except as provided in the Atomic Energy Act of 1954, as amended, the Order provides the only basis for classifying national security information. Information held by the Bank will be made available to the public to the extent possible consistent with the need to protect the national defense or foreign relations, as required by the interests of the United

States and its citizens. Accordingly, security classification shall be applied only to protect the national security.

(2) Before a classification determination is made, each item of information that may require protection shall be identified exactly. This requires identification of that specific information, disclosure of which could affect the national security. When there is reasonable doubt about the need to classify, the information should be safeguarded as if it were confidential until a final determination is made by an authorized classifier as to its classification. The final determination must be made within thirty (30) days.

(b) *Classification Designations.* Information which requires protection against unauthorized disclosure in the interest of national security (*classified information*) shall be classified at one of the following three levels:

(1) TOP SECRET shall be applied only 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 only 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.

Except as provided by statute, no other terms, such as *SENSITIVE*, *OFFICIAL BUSINESS ONLY*, *AGENCY*, *BUSINESS*, *ADMINISTRATIVELY*, etc., shall be used within the Bank in conjunction with any of the three classification levels defined above.

(c) *Original Classification Authority and Criteria.* (1) The Bank's authority to assign original classification to any document is limited as follows and is nondelegable:

Classification	Classifier
CONFIDENTIAL.	President and Chairman. First Vice President and Vice Chairman. General Counsel. Senior Vice Presidents. Security Officer.

(2) A determination to classify information shall be made by an original classification authority when the information concerns one or more of categories (i) through (x) of this paragraph, and when the unauthorized disclosure of the information, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security. Information shall be considered for classification if it concerns:

(i) Military plans, weapons, or operations;

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

(iii) Foreign government information;

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

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

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

(vii) United States Government programs for safeguarding nuclear materials or facilities;

(viii) Cryptology;

(ix) A confidential source; or

(x) Other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President of the United States, by the Chairman or by other officials who have been delegated original classification authority by the President. Recommendations concerning the need to designate additional categories of information that may be considered for classification shall be forwarded through the Security Officer to the Chairman for determination. Such a determination shall be reported to the Director of the Information Security Oversight Office.

(3) Information that is determined to concern one or more of the above categories shall be classified when an original classification authority also 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. Accordingly, certain information which would otherwise be unclassified may require classification when associated with other unclassified or classified information. Classification on this basis shall be supported by a written explanation that, at a minimum, shall be maintained with the file or reference on the recent copy of the information.

(4) Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or disclosure of intelligence sources or methods is presumed to cause damage to the national security.

(5) Information classified in accordance with the above classification categories 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.

(d) *Duration of Original Classification.* (1) 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. If the date or event for declassification cannot be determined at the time of classification, the standard notation ''Originating Agency's Determination Required'', or its abbreviation ''OADR'', should be entered on the ''Declassify on'' line.

(2) Automatic declassification determinations under predecessor orders shall remain valid unless the classification is extended by an authorized declassification authority. These extensions may be by individual documents or categories of information, provided, however, that any extension of classification on other than an individual document basis shall be reported to the Director of the Information Security Oversight Office. The declassification authority shall be responsible for notifying holders of the information of such extensions.

(3) Information classified under predecessor orders and marked for declassification review shall remain classified until reviewed for declassification under the provisions of the Order.

(e) *Marking and Identification.* (1) Classified information must be marked, or otherwise identified, to inform and warn the holder of the information of its sensitivity. The classifier is responsible for ensuring that proper classification markings are applied. At the time of 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:

(i) One of the three classification levels defined in § 403.3(b); ''(TS)'' for Top Secret, ''(S)'' for Secret, ''(C)'' for Confidential, and ''(U)'' for Unclassified; with each page marked at top and bottom according to the highest level of classified information on each page.

(ii) The identity of the original classification authority if other than the person whose name appears as the approving or signing official;

(iii) The agency and office of origin; and

(iv) The date or event for declassification, or the notation ''Originating Agency's Determination Required.''

(2) 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 Chairman 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.

(3) Marking designations implementing the provisions of the Order, including abbreviations, shall conform to the standards prescribed in implementing directives issued by the Information Security Oversight Office. All authorized classifiers shall be issued a uniform stamp that has a ''Classified by'' line and a ''Declassify on'' line.

(4) Documents that contain foreign government information shall include either the marking, ''FOREIGN GOVERNMENT INFORMATION'', or a marking that otherwise indicates that the information is foreign government

information. If that fact must be concealed, the document will be marked as if it were of U.S. origin. 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.

(5) Documents that contain information relating to intelligence sources or methods shall include the following marking unless proscribed by the Director of the Central Intelligence; WARNING NOTICE—INTELLIGENCE SOURCES OR METHODS INVOLVED.

(6) Information assigned a level of classification under predecessor 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 General Counsel or the Security Officer.

(f) *Limitations on Classification.* (1) 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.

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

(3) The Chairman or other authorized original classifiers may reclassify information previously declassified and disclosed if it is determined in writing that—

(i) The information requires protection in the interest of national security, and

(ii) The information may reasonably be recovered.

In making such determination, the Chairman or any other authorized original classifier shall consider the following factors: The lapse of time following disclosure; the nature and extent of disclosure; the ability to bring the fact of reclassification to the attention of persons to whom the information was disclosed; the ability to prevent further disclosure; and the ability to retrieve the information voluntarily from persons not authorized access to its reclassified state. These reclassification actions shall be reported promptly to the Director of the Information Security Oversight Office.

(4) Information may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of the Order and these regulations, if such classification meets the requirements of the Order and is accomplished personally and on a document-by-document basis by the Chairman, the Vice Chairman, or the Security Officer.

§ 403.4 Derivative classification.

(a) *Use of derivative classification.* (1) Unlike original classification which is an initial determination, derivative classification is an incorporation, paraphrasing, restatement, or generation in new form of information that is already classified. Derivative classification is the responsibility of those 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. Original classification authority is not required for derivative classification.

(2) Persons who apply such derivative classification markings shall:

(i) Respect original classification decisions;

(ii) Verify the information's current level of classification so far as practicable before applying the markings; and

(iii) Carry forward to any newly created documents the assigned dates or events for declassification or review. The latest date for declassification should be entered in the case of multiple source documents.

(b) *New Material.* (1) New material that derives its classification from information classified on or after the effective date of the Order, April 2, 1982, shall be marked with the declassification date or event, or the date for review, as assigned to the source information.

(2) New material that derives its classification under prior orders shall be treated as follows:

(i) If the source material bears a classification date or event 20 years or less from the date or origin, that date or event shall be carried forward on the new material.

(ii) If the source material bears no declassification date or event or is marked for declassification beyond 20 years, the new material shall be marked with a date for review for declassification at 20 years from the date of original classification of the source material.

(iii) If the source material is foreign government information bearing no date or event for declassification or is marked for declassification beyond 30 years, the new material shall be marked for review for declassification at 30 years from the date of original classification of the source materials.

(iv) A copy of the source document or documents should be maintained with the file copy of the new document or documents which have been derivatively classified.

§ 403.5 Declassification and downgrading.

(a) *Authority and policy for declassification and downgrading.* Information that continues to meet the classification requirements prescribed in § 403.3(c) despite the passage of time will continue to be safeguarded. However, information which is properly classified at the time it is developed may not necessarily require protection indefinitely. National security information over which the Bank exercises final classification jurisdiction shall be declassified or downgraded as soon as national security considerations permit. Information shall be declassified or downgraded by:

(1) The official who authorized the original classification, if that official is still serving in the same position, by a successor, or by a supervisory official of either; or

(2) Officials specifically delegated this authority in writing by the Chairman or by the Security Officer. A list of those who may be so delegated shall be maintained by the Security Officer.

(3) If the Director of the Information Security Oversight Office determines that information is unlawfully classified, the Director may require the Export-Import Bank to declassify it. Any such decision by the Director may be appealed to the National Security Council. The information shall remain classified until the appeal is decided.

(b) *Declassification Procedure.* Information marked with a specific declassification date or event shall be declassified on that date or upon occurrence of that event. The overall classification markings shall be lined through a statement placed on the cover or first page to indicate the declassification authority, by name and title, and the date of declassification. If practicable, the classification markings on each page shall be cancelled; otherwise, the statement on the cover or first page shall indicate that the declassification applies to the entire document.

(c) *Notification to Holders.* When classified information has been properly marked with specific dates or events for declassification it is not necessary to issue notices of declassification to any holders. However, when declassification action is taken earlier than originally scheduled, or the duration of classification is extended, the authority making such changes shall promptly notify all holders to whom the information was originally transmitted. This notification shall include the marking action to be taken, the authority for the change (name and title), and the effective date of the change. Upon receipt of notification, recipients shall make the proper changes and shall notify holders to whom they have transmitted the classified information.

(d) *Downgrading.* Information designated a particular level of classification may be assigned a lower classification level by the original classifier or by an official authorized to declassify the same information. Prompt notice of such downgrading shall be provided to known holders of the information. Classified information marked for automatic downgrading under previous Executive Orders shall be reviewed to determine that it no longer continues to meet classification requirements despite the passage of time.

(e) *Transferred Information.* Classified information transferred from one agency to another in conjunction with a transfer of functions, and not merely for storage purposes, shall be considered under the control of the receiving agency for purposes of downgrading and declassification, subject to consultation with any other agency that has an interest in the subject matter of the information. Prior to forwarding classified information to an approved storage facility of the Bank, to a Federal records center, or to the National Archives for permanent preservation, the information shall be reviewed for downgrading or declassification.

§ 403.6 Systematic review for declassification.

Classified information determined by the Archivist of the United States to be of sufficient value to warrant permanent retention will be subject to systematic declassification review by the Archivist in accordance with guidelines provided by the Bank, as originator of the information. These guidelines shall be developed by the Security Officer who is designated by the Bank to assist the Archivist in the review process. The guidelines shall be reviewed every five years or as requested by the Archivist of the United States.

§ 403.7 Mandatory review for declassification.

(a) Classified information under the jurisdiction of the Bank shall be reviewed for declassification upon receipt of a request by a United States citizen or permanent resident alien, a Federal agency, or a State or local government. A request for mandatory review of classified information shall be submitted in writing and describe the information with sufficient particularity to locate it with a reasonable amount of effort. Requests may be addressed to the:

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

(b) The Bank's response to mandatory review requests will be governed by the amount of search and review time required to process the request. The Bank will acknowledge receipt of all requests, and will inform the requester if additional time is needed to process the request. Except in unusual circumstances, the Bank will make a final determination within one year from the date of receipt of the request.

(c) When information cannot be declassified in its entirety, the Bank will make a reasonable effort to release, consistent with other applicable laws, those declassified portions that constitute a coherent segment.

(d) The bank shall determine whether information under the classification jurisdiction of the Bank or any reasonably segregable portion of it no longer requires protection. If so, the General Counsel shall promptly make such information available to the requester, and shall inform the requester of any fees due before releasing the document. If the information may not be released, in whole or in part, the General Counsel shall give the requester a brief statement of the reasons, and a notice, mailed with return receipt requested, of the right to appeal the determination within 60 days of the denial letter's receipt.

(e) The agency that initially received or classified records containing foreign government information shall be responsible for making a declassification determination on review requests for classified records which contain such foreign government information. Such requests shall be referred to the appropriate agency for action.

(f) When the Bank receives a mandatory declassification review request for records in its possession that were originated by another agency, it shall forward the request to that agency. The Bank may request notification of the declassification determination.

(g) Information originated by a President, the White House staff, by committees, commissions, or boards appointed by the President, or other specifically providing advice and counsel to a President or acting on behalf of a President is exempted from the provisions of mandatory review for declassification, except as consistent with applicable laws that pertain to presidential papers or records.

(h) The bank shall process requests for declassification that are submitted under the provisions of the Freedom of Information Act, as amended, or the

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

additional information as it is developed.

(9) Whenever the Bank determines during the course of an investigation that it is necessary to compel or induce the cooperation of an employee, the Bank shall first consult with the Department of Justice. The Department of Justice will coordinate with the Bank to determine the procedures the Bank may use to compel an employee's participation without foreclosing possible criminal proceedings.

(10) The Bank shall maintain records of all disclosures that have been reported or investigated.

(11) All employees shall cooperate fully with officials of the Bank or other agencies who are conducting investigations of unauthorized disclosures of classified information.

(12) Employees determined by the Bank to have knowingly participated in an unauthorized disclosure of classified information or who have refused to cooperate with an investigation of such a disclosure shall be denied further access to classified information and shall be subject to other appropriate administrative sanctions. Prior to taking action against an employee in connection with the unauthorized disclosure or classified information, the Bank shall consult with the Department of Justice, National Security Division.

[50 FR 27215, July 2, 1985, as amended at 72 FR 66043, Nov. 27, 2007]

PART 404—INFORMATION DISCLOSURE

Subpart A—Procedures for Disclosure of Records Under the Freedom of Information Act

Sec.

Subpart B—Protection of Privacy and Access to Records Under the Privacy Act of 1974

Subpart C—Demands for Testimony of Current and Former Ex-Im Bank Personnel and for Production of Ex-Im Bank Records

Subparts D–E [Reserved]

AUTHORITY: 12 U.S.C. 635(a)(1); 5 U.S.C. 552, 5 U.S.C. 552(a), 5 U.S.C. 553.

Section 404.7 also issued under E.O. 12600, 52 FR 23781, 3 CFR, 1987 Comp., p. 235.

Section 404.21 also issued under 5 U.S.C. 552a note.

Subpart C also issued under 5 U.S.C. 301, 12 U.S.C. 635.