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.