

PART 400—EMPLOYEE FINANCIAL DISCLOSURE AND ETHICAL CONDUCT STANDARDS REGULATIONS

AUTHORITY: 5 U.S.C. 7301.

§ 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.

[60 FR 17628, Apr. 7, 1995]

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

Sec.

403.1 General policies and definitions.

403.2 Responsibilities.

403.3 Classification principles and authority.

403.4 Derivative classification.

403.5 Declassification and downgrading.

403.6 Systematic review for declassification.

403.7 Mandatory review for declassification.

403.8 Appeals.

403.9 Fees.

403.10 Safeguarding.

403.11 Enforcement and investigation procedures.

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 exec-

utive 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

§ 403.2

12 CFR Ch. IV (1-1-11 Edition)

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