PART 3 [RESERVED]

PART 3a—NATIONAL SECURITY INFORMATION

GENERAL

Sec.
3a.1 Purpose.
3a.2 Authority.

CLASSIFICATION

3a.11 Classification of official information.
3a.12 Authority to classify official information.
3a.13 Classification responsibility and procedure.

DECLASSIFICATION AND DOWNGRADING

3a.21 Authority to downgrade and declassify.
3a.22 Declassification and downgrading.
3a.23 Review of classified material for declassification purposes.

CLASSIFICATION MARKINGS AND SPECIAL NOTATIONS

3a.31 Classification markings and special notations.

ACCESS TO CLASSIFIED MATERIALS

3a.41 Access requirements.

SECURITY OFFICERS

3a.51 Designation of security officers.

STORAGE AND CUSTODY OF CLASSIFIED INFORMATION

3a.61 Storage and custody of classified information.

ACCOUNTABILITY FOR CLASSIFIED MATERIAL

3a.71 Accountability for classified material.

TRANSMITTAL OF CLASSIFIED MATERIAL

3a.81 Transmittal of classified material.

DATA INDEX SYSTEM

3a.91 Data index system.

AUTHORITY: E.O. 11652 (37 FR 5209, March 10, 1972), National Security Council Directive of May 17, 1972 (37 FR 10053, May 19, 1972), sec. 309 of the Federal Power Act (49 Stat. 858, 859; 16 U.S.C. 825h) and sec. 16 of the Natural Gas Act (52 Stat. 830; 15 U.S.C. 717*o*).

SOURCE: Order 470, 38 FR 5161, Feb. 26, 1973, unless otherwise noted.

GENERAL

§ 3a.1 Purpose.

This part 3a describes the Federal Power Commission program to govern the classification, downgrading, declassification, and safeguarding of national security information. The provisions and requirements cited herein are applicable to the entire agency except that material pertaining to personnel security shall be safeguarded by the Personnel Security Officer and shall not be considered classified material for the purpose of this part.

§ 3a.2 Authority.

Official information or material referred to as classified in this part is expressly exempted from public disclosure by 5 U.S.C. 552(b)(1). Wrongful disclosure thereof is recognized in the Federal Criminal Code as providing a basis for prosecution. E.O. 11652, March 8, 1972 (37 FR 5209, March 10, 1972), identifies the information to be protected, prescribes classification, downgrading, declassification, and safeguarding procedures to be followed and establishes a monitoring system to insure its effectiveness. National Security Council Directive Governing the Classification, Downgrading, Declassification and Safeguarding of National Security Information, May 17, 1972 (37 FR 10053, May 19, 1972), implements E.O. 11652.

CLASSIFICATION

§ 3a.11 Classification of official information.

(a) *Security Classification Categories.* Information or material which requires protection against unauthorized disclosure in the interest of the national defense or foreign relations of the United States (hereinafter collectively termed *national security*) is classified Top Secret, Secret or Confidential, depending upon the degree of its significance to national security. No other categories are to be used to identify official information or material requiring protection in the interest of national security, except as otherwise expressly provided by statute. These classification categories are defined as follows:

(1) *Top Secret*. Top Secret refers to national security information or material which requires the highest degree of protection. The test for assigning Top Secret classification is whether its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Examples of *exceptionally grave damage* include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security. This classification is to be used with the utmost restraint.

(2) *Secret*. Secret refers to national security information or material which requires a substantial degree of protection. The test for assigning Secret classification shall be whether its unauthorized disclosure could reasonably be expected to cause serious damage to the national security. Examples of *serious damage* include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security. The classification Secret shall be sparingly used.

(3) *Confidential*. Confidential refers to national security information or material which requires protection, but not to the degree described in paragraphs (a) (1) and (2) of this section. The test for assigning Confidential classification shall be whether its unauthorized disclosure could reasonably be expected to cause damage to the national security.

(b) Classified information will be assigned the lowest classification consistent with its proper protection. Documents will be classified according to their own content and not necessarily according to their relationship to other documents.

(c) The overall classification of a file or group of physically connected documents will be at least as high as that of the most highly classified document therein. When put together as a unit or complete file, the classification of the highest classified document contained therein will be marked on a cover sheet, file folder (front and back), or other similar covering, and on any transmittal letters, comments, or endorsements.

(d) *Administrative Control Designations*. These designations are not security classification designations, but are used to indicate a requirement to protect material from unauthorized disclosure. Material identified under the provisions of this subparagraph will be handled and protected in the same manner as material classified Confidential except that it will not be subject to the central control system described in §3a.71. Administrative Control designations are:

(1) *For Official Use Only*. This designation is used to identify information which does not require protection in the interest of national security, but requires protection in accordance with statutory requirements or in the public interest and which is exempt from public disclosure under 5 U.S.C. 552(b) and §388.105(n) of this chapter.

(2) *Limited Official Use*. This administrative control designation is used by the Department of State to identify nondefense information requiring protection from unauthorized access. Material identified with this notation must be limited to persons having a definite need to know in order to fulfill their official responsibilities.

(e) A letter or other correspondence which transmits classified material will be classified at a level at least as high as that of the highest classified attachment or enclosure. This is necessary to indicate immediately to persons who receive or handle a group of documents the highest classification involved. If the transmittal document does not contain classified information, or if the information in it is classified lower than in an enclosure, the originator will include a notation to that effect. (See §3a.31(e).)

[Order 470, 38 FR 5161, Feb. 26, 1973, as amended by Order 225, 47 FR 19055, May 3, 1982]