AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

(2) Confidential matter may be transported by one of the methods set forth in paragraph (c)(1) of this section, by U.S. express or certified mail. Express or certified mail may be used in transmission of Confidential documents to Puerto Rico or any United States territory or possession.

(d) *Telecommunication of classified information*. Classified information may not be telecommunicated unless the telecommunication system has been approved by the CSA. Licensees, certificate holders or other persons who may require a secure telecommunication system shall submit a telecommunication plan as part of their request for facility clearance, as outlined in § 95.15, or as an amendment to their existing Standard Practice Procedures Plan for the protection of classified information.

(e) *Security of classified information in transit*. Classified matter that, because of its nature, cannot be transported in accordance with § 95.39(c), may only be transported in accordance with procedures approved by the CSA. Procedures for transporting classified matter are based on a satisfactory transportation plan submitted as part of the licensee's, certificate holder, or other person's request for facility clearance or submitted as an amendment to its existing Standard Practice Procedures Plan.

[62 FR 17696, Apr. 11, 1997, as amended at 64 FR 15652, Apr. 1, 1999; 72 FR 49564, Aug. 28, 2007]

§ 95.41 External receipt and dispatch records.

Each licensee, certificate holder or other person possessing classified information shall maintain a record that reflects:

(a) The date of the material;

(b) The date of receipt or dispatch;

(c) The classification;

(d) An unclassified description of the material; and

(e) The identity of the sender from which the material was received or recipient to which the material was dispatched. receipt and dispatch records must be retained for 2 years.

[62 FR 17697, Apr. 11, 1997]

§ 95.43 Authority to reproduce.

(a) Each licensee, certificate holder, or other person possessing classified information shall establish a reproduction control system to ensure that reproduction of classified material is held to the minimum consistent with operational requirements. Classified reproduction must be accomplished by authorized employees knowledgeable of the procedures for classified reproduction. The use of technology that prevents, discourages, or detects the unauthorized reproduction of classified documents is encouraged.

(b) Unless restricted by the CSA, Secret and Confidential documents may be reproduced. Reproduced copies of classified documents are subject to the same protection as the original documents.

(c) All reproductions of classified material must be conspicuously marked with the same classification markings as the material being reproduced. Copies of classified material must be reviewed after the reproduction process to ensure that these markings are visible.

[62 FR 17697, Apr. 11, 1997, as amended at 72 FR 49564, Aug. 28, 2007]

§ 95.45 Changes in classification.

(a) Documents containing classified National Security Information must be downgraded or declassified as authorized by the NRC classification guides or as determined by the NRC. Requests for downgrading or declassifying any NRC classified information should be forwarded to the NRC's Division of Nuclear Security, Nuclear Security and Incident Response, using an appropriate method listed in § 95.9. Requests for downgrading or declassifying of Restricted Data will be forwarded to the NRC Division of Nuclear Security for coordination with the Department of Energy.

(b) If a change of classification or declassification is approved, the previous classification marking must be canceled and the following statement, properly completed, must be placed on the first page of the document:

Classification canceled (or changed to)

_____

(Insert appropriate classification)

By authority of

(Person authorizing change in classification)

By

(Signature of person making change and date thereof)

(c) New markings reflecting the current classification status of the document will be applied in accordance with the requirements of §95.37.

(d) Any licensee, certificate holder, or other person making a change in classification or receiving notice of such a change shall forward notice of the change in classification to holders of all copies as shown on their records.

[62 FR 17697, Apr. 11, 1997, as amended at 64 FR 15653, Apr. 1, 1999; 68 FR 41222, July 11, 2003; 68 FR 58823, Oct. 10, 2003; 72 FR 49564, Aug. 28, 2007]

§95.47 Destruction of matter containing classified information.

Documents containing classified information may be destroyed by burning, pulping, or another method that ensures complete destruction of the information that they contain. The method of destruction must preclude recognition or reconstruction of the classified information. Any doubts on methods should be referred to the CSA.

[64 FR 15653, Apr. 1, 1999]

§95.49 Security of automatic data processing (ADP) systems.

Classified data or information may not be processed or produced on an ADP system unless the system and procedures to protect the classified data or information have been approved by the CSA. Approval of the ADP system and procedures is based on a satisfactory ADP security proposal submitted as part of the licensee's, certificate holder's, or other person's request for facility clearance outlined in §95.15 or submitted as an amendment to its existing Standard Practice Procedures Plan for the protection of classified information.

[72 FR 49564, Aug. 28, 2007]

§95.51 Retrieval of classified matter following suspension or revocation of access authorization.

In any case where the access authorization of an individual is suspended or revoked in accordance with the procedures set forth in part 25 of this chapter, or other relevant CSA procedures, the licensee, certificate holder, or other person shall, upon due notice from the Commission of such suspension or revocation, retrieve all classified information possessed by the individual and take the action necessary to preclude that individual having further access to the information.

[72 FR 49564, Aug. 28, 2007]

§95.53 Termination of facility clearance.

(a) If the need to use, process, store, reproduce, transmit, transport, or handle classified matter no longer exists, the facility clearance will be terminated. The licensee, certificate holder, or other person for the facility may deliver all documents and matter containing classified information to the Commission, or to a person authorized to receive them, or must destroy all classified documents and matter. In either case, the licensee, certificate holder, or other person for the facility shall submit a certification of nonpossession of classified information to the NRC Division of Nuclear Security within 30 days of the termination of the facility clearance.

(b) In any instance where a facility clearance has been terminated based on a determination of the CSA that further possession of classified matter by the facility would not be in the interest of the national security, the licensee, certificate holder, or other person for the facility shall, upon notice from the CSA, dispose of classified documents in a manner specified by the CSA.

[72 FR 49564, Aug. 28, 2007]

§95.55 Continued applicability of the regulations in this part.

The suspension, revocation or other termination of access authorization or the termination of facility clearance