Nuclear Regulatory Commission

§ 95.36 Access by representatives of the International Atomic Energy Agency or by participants in other international agreements.

(a) Except as the Commission may authorize, no licensee, certificate holder, or other person subject to the regulations in this part may receive or may permit any other licensee, certificate holder, or other person to have access to matter revealing Secret or Confidential National Security Information or Restricted Data unless the individual has:

(1)(i) A “Q” access authorization which permits access to matter classified as Secret and Confidential Restricted Data or Secret and Confidential National Security Information which includes intelligence information, CRYPTO (i.e., cryptographic information) or other classified communications security (COMSEC) information, or

(ii) An “L” access authorization which permits access to matter classified as Confidential Restricted Data and Secret and Confidential National Security Information other than that noted in paragraph (a)(1)(i) of this section except that access to certain Confidential COMSEC information is permitted as authorized by a National Communications Security Committee waiver dated February 14, 1984.

(2) An established “need-to-know” for the matter (See Definitions, §95.5).

(3) NRC-approved storage facilities if classified documents or material are to be transmitted to the licensee, certificate holder, or other person.

(b) Matter classified as National Security Information or Restricted Data shall not be released by a licensee or other person subject to part 95 to any personnel other than properly access authorized Commission licensee employees, or other individuals authorized access by the Commission.

(c) Access to matter which is National Security Information at NRC-licensed facilities or NRC-certified facilities by authorized representatives of IAEA is permitted in accordance with §95.36.

§ 95.37 Classification and preparation of documents.

(a) Classification. Classified information generated or possessed by a licensee, certificate holder, or other person must be appropriately marked. Classified material which is not conducive to markings (e.g., equipment) may be exempt from this requirement. Classified material which is not conducive to markings (e.g., equipment) may be exempt from this requirement. These exemptions are subject to the approval of the CSA on a case-by-case basis. If a person or facility generates or possesses information that is believed to be classified based on guidance provided by the NRC or by derivation from classified documents, but which no authorized classifier has determined to be classified, the information must be protected and marked with the appropriate classification markings pending review and signature of an NRC authorized classifier. This information shall be protected as classified information pending final determination.

(b) Classification consistent with content. Each document containing classified information shall be classified Secret or Confidential according to its content. NRC licensees, certificate holders, or other persons subject to the requirements of 10 CFR part 95 may not make original classification decisions.

(c) Markings required on face of documents. (1) For derivative classification of classified National Security Information:

(i) Derivative classifications of classified National Security Information must contain the identity of the source document or the classification guide, including the agency and office of origin, on the “Derived From” line and its classification date. If more than one source is cited, the “Derived From” line should indicate “Multiple Sources.” The derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document.

(ii) Each release of classified information shall be marked with the specific categories of documents that the authorized representative has had access and the date of this access. A licensee, certificate holder, or other person subject to this part shall also retain Division of Security Operations disclosure authorizations for 5 years beyond the date of any visit or inspection when access to classified information was permitted.

(2) Other categories of documents may be marked as classified in accordance with the authority granted by the Division of Security Operations.

(3) Derivative classifications of classified National Security Information must be protected and marked with the appropriate classification markings pending review and signature of an NRC authorized classifier. This information shall be protected as classified information pending final determination.

(4) Each release of classified information shall be marked with the specific categories of documents that the authorized representative has had access and the date of this access. A licensee, certificate holder, or other person subject to this part shall also retain Division of Security Operations disclosure authorizations for 5 years beyond the date of any visit or inspection when access to classified information was permitted.

(5) Each release of classified information shall be marked with the specific categories of documents that the authorized representative has had access and the date of this access.