

Nuclear Regulatory Commission

§ 95.35

granted access to classified information. The Facility Security Officer shall forward the executed SF-312 to the CSA for retention. If the employee refuses to execute the SF-312, the licensee or other facility shall deny the employee access to classified information and submit a report to the CSA. The SF-312 must be signed and dated by the employee and witnessed. The employee's and witness' signatures must bear the same date.

(e) Initial Security Briefings. Before being granted access to classified information, an employee shall receive an initial security briefing that includes the following topics:

- (1) A Threat Awareness Briefing.
- (2) A Defensive Security Briefing.
- (3) An overview of the security classification system.
- (4) Employee reporting obligations and requirements.
- (5) Security procedures and duties applicable to the employee's job.

(f) *Refresher Briefings*. The licensee or other facility shall conduct refresher briefings for all cleared employees every 3 years. As a minimum, the refresher briefing must reinforce the information provided during the initial briefing and inform employees of appropriate changes in security regulations. This requirement may be satisfied by use of audio/video materials and/or by issuing written materials.

(g) Debriefings. Licensee and other facilities shall debrief cleared employees at the time of termination of employment (discharge, resignation, or retirement); when an employee's access authorization is terminated, suspended, or revoked; and upon termination of the Facility Clearance.

(h) Records reflecting an individual's initial and refresher security orientations and security termination must be maintained for three years after termination of the individual's access authorization.

[62 FR 17694, Apr. 11, 1997, as amended at 64 FR 15652, Apr. 1, 1999]

§ 95.34 Control of visitors.

(a) *Uncleared visitors*. Licensees, certificate holders, or others subject to this part shall take measures to preclude access to classified information by uncleared visitors.

(b) *Foreign visitors*. Licensees, certificate holders, or others subject to this part shall take measures as may be necessary to preclude access to classified information by foreign visitors. The licensee, certificate holder, or others shall retain records of visits for 5 years beyond the date of the visit.

[64 FR 15652, Apr. 1, 1999]

CONTROL OF INFORMATION

§ 95.35 Access to matter classified as National Security Information and Restricted Data.

(a) Except as the Commission may authorize, no person subject to the regulations in this part may receive or may permit any individual 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 individual.

(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.