§ 95.29 Establishment of Restricted or Closed areas.

(a) If, because of its nature, sensitivity or importance, classified matter cannot otherwise be effectively controlled in accordance with the provisions of §§95.25 and 95.27, a Restricted or Closed area must be established to protect this matter.

(b) The following measures apply to Restricted Areas:

(1) Restricted areas must be separated from adjacent areas by a physical barrier designed to prevent unauthorized access (physical, audio, and visual) into these areas.

(2) Controls must be established to prevent unauthorized access to and removal of classified matter.

(3) Access to classified matter must be limited to persons who possess appropriate access authorization or other written CSA disclosure authorization and who require access in the performance of their official duties or regulatory obligations.

(4) Persons without appropriate access authorization for the area visited must be escorted by an appropriate CSA access authorized person at all times while within Restricted or Closed Areas.

(5) Each individual authorized to enter a Restricted or Closed Area must be issued a distinctive form of identification (e.g., badge) when the number of employees assigned to the area exceeds thirty per shift.

(6) During nonworking hours, admittance must be controlled by protective personnel. Protective personnel shall conduct patrols during nonworking hours at least every 8 hours and more frequently if necessary to maintain a commensurate level of protection. Entrances must be continuously monitored by protective personnel or by an approved alarm system.

(c) Due to the size and nature of the classified material, or operational necessity, it may be necessary to construct Closed Areas for storage because GSA-approved containers or vaults are unsuitable or impractical. Closed Areas must be approved by the CSA. The following measures apply to Closed Areas:

(1) Access to Closed Areas must be controlled to preclude unauthorized access. This may be accomplished ...
§ 95.31 Protective personnel.

Whenever protective personnel are used to protect classified information they shall:

(a) Possess an “L” access authorization (or CSA equivalent) if the licensee, certificate holder, or other person possesses information classified Confidential National Security Information, Confidential Restricted Data or Secret National Security Information.

(b) Possess a “Q” access authorization (or CSA equivalent) if the licensee, certificate holder, or other person possesses Secret Restricted Data related to nuclear weapons design, manufacturing and vulnerability information; and certain particularly sensitive Naval Nuclear Propulsion Program Information (e.g., fuel manufacturing technology) and the protective personnel require access as part of their regular duties.

[72 FR 49562, Aug. 28, 2007]

§ 95.33 Security education.

All cleared employees must be provided with security training and briefings commensurate with their involvement with classified information. The facility may obtain defensive security, threat awareness, and other education and training information and material from their CSA or other sources.

(a) Facility Security Officer training. Licensees and others are responsible for ensuring that the Facility Security Officer, and others performing security duties, complete security training deemed appropriate by the CSA. Training requirements must be based on the facility’s involvement with classified information and may include a Facility Security Officer orientation course and, for Facility Security Officers at facilities with safeguarding capability, a Facility Security Officer Program Management Course. Training, if required, should be completed within 1 year of appointment to the position of Facility Security Officer.

(b) Government-provided briefings. The CSA is responsible for providing initial security briefings to the Facility Security Officer, and for ensuring that other briefings required for special categories of information are provided.

(c) Temporary help suppliers. A temporary help supplier, or other contractor who employs cleared individuals solely for dispatch elsewhere, is responsible for ensuring that required briefings are provided to their cleared personnel. The temporary help supplier or the using licensee’s, certificate holder’s, or other person’s facility may conduct these briefings.

(d) Classified Information Nondisclosure Agreement (SF-312). The SF-312 is an agreement between the United States and an individual who is cleared for access to classified information. An employee issued an initial access authorization must, in accordance with the requirements of §25.23 of this chapter, execute an SF-312 before being granted access to classified information. The Facility Security Officer shall forward