(10) *Monitoring*. Maintain effective monitoring, communications and warning systems, including,

(i) Measures designed to ensure that security systems and equipment are in good working order and inspected, tested, calibrated, and otherwise maintained;

(ii) Measures designed to regularly test security systems, note deficiencies, correct for detected deficiencies, and record results so that they are available for inspection by the Department; and

(iii) Measures to allow the facility to promptly identify and respond to security system and equipment failures or malfunctions;

(11) *Training*. Ensure proper security training, exercises, and drills of facility personnel;

(12) *Personnel surety*. Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets, including,

(i) Measures designed to verify and validate identity;

(ii) Measures designed to check criminal history;

(iii) Measures designed to verify and validate legal authorization to work; and

(iv) Measures designed to identify people with terrorist ties;

(13) *Elevated threats*. Escalate the level of protective measures for periods of elevated threat;

(14) *Specific threats, vulnerabilities, or risks*. Address specific threats, vulnerabilities or risks identified by the Assistant Secretary for the particular facility at issue;

(15) *Reporting of significant security incidents*. Report significant security incidents to the Department and to local law enforcement officials;

(16) *Significant security incidents and suspicious activities*. Identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site;

(17) *Officials and organization*. Establish official(s) and an organization responsible for security and for compliance with these standards;

(18) *Records*. Maintain appropriate records; and

(19) Address any additional performance standards the Assistant Secretary may specify.

(b) [Reserved]

§ 27.235 Alternative security program.

(a) Covered facilities may submit an Alternate Security Program (ASP) pursuant to the requirements of this section. The Assistant Secretary may approve an Alternate Security Program, in whole, in part, or subject to revisions or supplements, upon a determination that the Alternate Security Program meets the requirements of this part and provides for an equivalent level of security to that established by this part.

(1) A Tier 4 facility may submit an ASP in lieu of a Security Vulnerability Assessment, Site Security Plan, or both.

(2) Tier 1, Tier 2, or Tier 3 facilities may submit an ASP in lieu of a Site Security Plan. Tier 1, Tier 2, and Tier 3 facilities may not submit an ASP in lieu of a Security Vulnerability Assessment.

(b) The Department will provide notice to a covered facility about the approval or disapproval, in whole or in part, of an ASP, using the procedure specified in § 27.240 if the ASP is intended to take the place of a Security Vulnerability Assessment or using the procedure specified in § 27.245 if the ASP is intended to take the place of a Site Security Plan.

§ 27.240 Review and approval of security vulnerability assessments.

(a) *Review and approval*. The Department will review and approve in writing all Security Vulnerability Assessments that satisfy the requirements of § 27.215, including Alternative Security Programs submitted pursuant to § 27.235.

(b) If a Security Vulnerability Assessment does not satisfy the requirements of § 27.215, the Department will provide the facility with a written notification that includes a clear explanation of deficiencies in the Security Vulnerability Assessment. The facility shall then enter further consultations with the Department and resubmit a