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 sufficient Security Vulnerability Assessment by the time specified in the written notification provided by the Department under this section. If the resubmitted Security Vulnerability Assessment does not satisfy the requirements of § 27.215, the Department will provide the facility with written notification (including a clear explanation of deficiencies in the SVA) of the Department's disapproval of the SVA.

§ 27.245 Review and approval of site security plans.

(a) *Review and Approval*. (1) The Department will review and approve or disapprove all Site Security Plans that satisfy the requirements of § 27.225, including Alternative Security Programs submitted pursuant to § 27.235.

(i) The Department will review Site Security Plans through a two-step process. Upon receipt of Site Security Plan from the covered facility, the Department will review the documentation and make a preliminary determination as to whether it satisfies the requirements of § 27.225. If the Department finds that the requirements are satisfied, the Department will issue a Letter of Authorization to the covered facility.

(ii) Following issuance of the Letter of Authorization, the Department will inspect the covered facility in accordance with § 27.250 for purposes of determining compliance with the requirements of this Part.

(iii) If the Department approves the Site Security Plan in accordance with § 27.250, the Department will issue a Letter of Approval to the facility, and the facility shall implement the approved Site Security Plan.

(2) The Department will not disapprove a Site Security Plan submitted under this part based on the presence or absence of a particular security measure. The Department may disapprove a Site Security Plan that fails to satisfy the risk-based performance standards established in § 27.230.

(b) When the Department disapproves a preliminary Site Security Plan issued prior to inspection or a Site Security Plan following inspection, the Department will provide the facility with a written notification that includes a clear explanation of deficiencies in the Site Security Plan. The facility shall then enter further consultations with the Department and resubmit a sufficient Site Security Plan by the time specified in the written notification provided by the Department under this section. If the resubmitted Site Security Plan does not satisfy the requirements of § 27.225, the Department will provide the facility with written notification (including a clear explanation of deficiencies in the SSP) of the Department's disapproval of the SSP.

§ 27.250 Inspections and audits.

(a) *Authority*. In order to assess compliance with the requirements of this Part, authorized Department officials may enter, inspect, and audit the property, equipment, operations, and records of covered facilities.

(b) Following preliminary approval of a Site Security Plan in accordance with § 27.245, the Department will inspect the covered facility for purposes of determining compliance with the requirements of this Part.

(1) If after the inspection, the Department determines that the requirements of § 27.225 have been met, the Department will issue a Letter of Approval to the covered facility.

(2) If after the inspection, the Department determines that the requirements of § 27.225 have not been met, the Department will proceed as directed by § 27.245(b) in ''Review and Approval of Site Security Plans.''

(c) *Time and Manner*. Authorized Department officials will conduct audits and inspections at reasonable times and in a reasonable manner. The Department will provide covered facility owners and/or operators with 24-hour advance notice before inspections, except

(1) If the Under Secretary or Assistant Secretary determines that an inspection without such notice is warranted by exigent circumstances and approves such inspection; or

(2) If any delay in conducting an inspection might be seriously detrimental to security, and the Director of the Chemical Security Division determines that an inspection without notice is warranted, and approves an inspector to conduct such inspection.

(d) *Inspectors*. Inspections and audits are conducted by personnel duly authorized and designated for that purpose as ''inspectors'' by the Secretary or the Secretary's designee.

(1) An inspector will, on request, present his or her credentials for examination, but the credentials may not be reproduced by the facility.

(2) An inspector may administer oaths and receive affirmations, with the consent of any witness, in any matter.

(3) An inspector may gather information by reasonable means including, but not limited to, interviews, statements, photocopying, photography, and video- and audio-recording. All documents, objects and electronically stored information collected by each inspector during the performance of that inspector's duties shall be maintained for a reasonable period of time in the files of the Department of Homeland Security maintained for that facility or matter.

(4) An inspector may request forthwith access to all records required to be kept pursuant to § 27.255. An inspector shall be provided with the immediate use of any photocopier or other equipment necessary to copy any such record. If copies can not be provided immediately upon request, the inspector shall be permitted immediately to take the original records for duplication and prompt return.

(e) *Confidentiality*. In addition to the protections provided under CVI in § 27.400, information received in an audit or inspection under this section, including the identity of the persons involved in the inspection or who provide information during the inspection, shall remain confidential under the investigatory file exception, or other appropriate exception, to the public disclosure requirements of 5 U.S.C. 552.

(f) *Guidance*. The Assistant Secretary shall issue guidance identifying appropriate processes for such inspections, and specifying the type and nature of