(ii) Tier 3 and Tier 4 covered facilities must routinely complete and submit a Top-Screen no less than three years, and no more than three years and 60 calendar days, from the date of the Department's approval of the facility's most recent Site Security Plan.

(2) *Security Vulnerability Assessment.* Unless otherwise notified and following a Top-Screen resubmission pursuant to paragraph (b)(1) of this section, a covered facility must complete and submit a new Security Vulnerability Assessment within 90 calendar days of written notification from the Department or within the time frame specified in any subsequent FEDERAL REGISTER notice.

(3) *Site Security Plan.* Unless otherwise notified and following a Security Vulnerability Assessment resubmission pursuant to paragraph (b)(2) of this section, a covered facility must complete and submit a new Site Security Plan within 120 calendar days of written notification from the Department or within the time frame specified in any subsequent FEDERAL REGISTER notice.

(c) The Executive Assistant Director retains the authority to modify the schedule in this part as needed. The Executive Assistant Director may shorten or extend these time periods based on the operations at the facility, the nature of the covered facility's vulnerabilities, the level and immediacy of security risk, or for other reasons. If the Department alters the time periods for a specific facility, the Department will do so in written notice to the facility.

(d) If a covered facility makes material modifications to its operations or site, the covered facility must complete and submit a revised Top-Screen to the Department within 60 days of the material modification. In accordance with the resubmission requirements in § 27.210(b)(2) and (3), the Department will notify the covered facility as to whether the covered facility must submit a revised Security Vulnerability Assessment, Site Security Plan, or both.

[72 FR 17729, Apr. 9, 2007, as amended at 72 FR 65420, Nov. 20, 2007; 86 FR 41891, Aug. 4, 2021]

§ 27.215 Security vulnerability assessments.

(a) *Initial assessment.* If the Executive Assistant Director determines that a chemical facility is high risk, the facility must complete a Security Vulnerability Assessment. A Security Vulnerability Assessment shall include:

(1) Asset Characterization, which includes the identification and characterization of potential critical assets; identification of hazards and consequences of concern for the facility, its surroundings, its identified critical asset(s), and its supporting infrastructure; and identification of existing layers of protection;

(2) Threat Assessment, which includes a description of possible internal threats, external threats, and internally-assisted threats;

(3) Security Vulnerability Analysis, which includes the identification of potential security vulnerabilities and the identification of existing countermeasures and their level of effectiveness in both reducing identified vulnerabilities and in meeting the applicable risk-based performance standards;

(4) Risk Assessment, including a determination of the relative degree of risk to the facility in terms of the expected effect on each critical asset and the likelihood of a success of an attack; and

(5) Countermeasures Analysis, including strategies that reduce the probability of a successful attack or reduce the probable degree of success, strategies that enhance the degree of risk reduction, the reliability and maintainability of the options, the capabilities and effectiveness of mitigation options, and the feasibility of the options.

(b) Except as provided in § 27.235, a covered facility must complete the Security Vulnerability Assessment through the CSAT process, or through any other methodology or process identified or issued by the Executive Assistant Director.

(c) Covered facilities must submit a Security Vulnerability Assessment to the Department in accordance with the schedule provided in § 27.210.

(d) *Updates and revisions.* (1) A covered facility must update and revise its

Security Vulnerability Assessment in accordance with the schedule provided in § 27.210.

(2) Notwithstanding paragraph (d)(1) of this section, a covered facility must update, revise, or otherwise alter its Security Vulnerability Assessment to account for new or differing modes of potential terrorist attack or for other security-related reasons, if requested by the Executive Assistant Director.

[72 FR 17729, Apr. 9, 2007, as amended at 86 FR 41891, Aug. 4, 2021]

§ 27.220 Tiering.

(a) *Preliminary determination of risk-based tiering*. Based on the information the Department receives in accordance with §§ 27.200 and 27.205 (including information submitted through the Top-Screen process) and following its initial determination in § 27.205(a) that a facility presents a high level of security risk, the Department shall notify a facility of the Department's preliminary determination of the facility's placement in a risk-based tier.

(b) *Confirmation or alteration of risk-based tiering*. Following review of a covered facility's Security Vulnerability Assessment, the Executive Assistant Director shall notify the covered facility of its final placement within a risk-based tier, or for covered facilities previously notified of a preliminary tiering, confirm or alter such tiering.

(c) The Department shall place covered facilities in one of four risk-based tiers, ranging from highest risk facilities in Tier 1 to lowest risk facilities in Tier 4.

(d) The Executive Assistant Director may provide the facility with guidance regarding the risk-based performance standards and any other necessary guidance materials applicable to its assigned tier.

[72 FR 17729, Apr. 9, 2007, as amended at 86 FR 41892, Aug. 4, 2021]

§ 27.225 Site security plans.

(a) The Site Security Plan must meet the following standards:

(1) Address each vulnerability identified in the facility's Security Vulnerability Assessment, and identify and describe the security measures to address each such vulnerability;

(2) Identify and describe how security measures selected by the facility will address the applicable risk-based performance standards and potential modes of terrorist attack including, as applicable, vehicle-borne explosive devices, water-borne explosive devices, ground assault, or other modes or potential modes identified by the Department;

(3) Identify and describe how security measures selected and utilized by the facility will meet or exceed each applicable performance standard for the appropriate risk-based tier for the facility; and

(4) Specify other information the Executive Assistant Director deems necessary regarding chemical facility security.

(b) Except as provided in § 27.235, a covered facility must complete the Site Security Plan through the CSAT process, or through any other methodology or process identified or issued by the Executive Assistant Director.

(c) Covered facilities must submit a Site Security Plan to the Department in accordance with the schedule provided in § 27.210.

(d) *Updates and revisions*. (1) When a covered facility updates, revises, or otherwise alters its Security Vulnerability Assessment pursuant to § 27.215(d), the covered facility shall make corresponding changes to its Site Security Plan.

(2) A covered facility must also update and revise its Site Security Plan in accordance with the schedule in § 27.210.

(e) A covered facility must conduct an annual audit of its compliance with its Site Security Plan.

[72 FR 17729, Apr. 9, 2007, as amended at 86 FR 41892, Aug. 4, 2021]

§ 27.230 Risk-based performance standards.

(a) Covered facilities must satisfy the performance standards identified in this section. The Executive Assistant Director will issue guidance on the application of these standards to risk-based tiers of covered facilities, and the acceptable layering of measures used to meet these standards will vary by risk-based tier. Each covered facility must select, develop in their Site