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 Assistant Secretary.

(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 Assistant Secretary.

§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 Assistant Secretary 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 Assistant Secretary may provide the facility with guidance regarding the risk-based performance standards and any other necessary guidance materials applicable to its assigned tier.

§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