Security Vulnerability Assessment

Regulatory Citation	6 CFR 27.215 - Security Vulnerability Assessments 49 CFR 172.802 - Components of a security plan
What It Is	Standards provide guidelines for conducting Security Vulnerability Assessments (SVA) and assessing transportation security risks.
Who It Applies To	Motor carriers who offer for transportation in commerce, or transport in commerce, certain hazardous materials and certain chemical facilities covered under the Chemical Facility Anti-Terrorism Standards (CFATS).
Origination Date	3-25-2003

6 CFR 27.215

If the Department of Homeland Security (DHS) determines that a chemical facility is high-risk, the facility must complete a Security Vulnerability Assessment (SVA). A SVA must 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 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.

Security Vulnerability Assessment

Continued

The SVA requires each facility to identify critical assets associated with each Chemical of Interest (COI) listed in the preliminary tier letter. The SVA website also requires that the facility inventory and describe their security equipment; their access control procedures and equipment; and their inventory, shipping and receiving procedures. The facility is then instructed to evaluate the response and consequence of each critical asset/COI combination against a series of DHS-defined adversarial attacks. The facility is asked to consider an adversary's ability to conduct a prescribed attack against the listed asset/COI combinations and provide DHS with an informed judgment as to the level of success of the attack. The facility is also required to provide their value judgment on the effectiveness of emergency response programs.

49 CFR 172.802

A written security plan must include an assessment of possible transportation security risks for shipments of the hazardous materials and appropriate measures to address the assessed risks. Specific measures put into place by the plan may vary commensurate with the level of threat at a particular time. At a minimum, a security plan must include the following elements:

1. Personnel security. Measures to confirm information provided by job applicants hired for positions that involve access to and handling of the hazardous materials covered by the security plan.
2. Unauthorized access. Measures to address the assessed risk that unauthorized persons may gain access to the hazardous materials covered by the security plan or transport conveyances being prepared for transportation of the hazardous materials covered by the security plan.
3. En route security. Measures to address the assessed security risks of shipments of hazardous materials covered by the security plan en route from origin to destination, including shipments stored incidental to movement.

The security plan must also include the following:

1. Identification by job title of the senior management official responsible for the overall development and implementation of the security plan;
2. Security duties for each position or department that is responsible for implementing the plan, or a portion of the plan, and the process of notifying employees when specific elements of the security plan must be implemented; and
3. A plan for training hazmat employees.

Security Vulnerability Assessment

Continued

Copies of the security plan must be available to the employees who are responsible for implementing it, consistent with personnel security clearance or background investigation restrictions and a demonstrated need to know. The security plan must be revised and updated as necessary to reflect changing circumstances. When the security plan is updated or revised, all copies of the plan must be maintained as of the date of the most recent revision.

FAQ & Interpretations

Follow these links:

http://www.phmsa.dot.gov/portal/site/PHMSA/menuitem.daf900ffe7cbb29970107210e90d8789/?vgnextoid=55b4e5f5e9494110VgnVCM1000009ed07898RCRD&vgnextchannel=55b4e5f5e9494110VgnVCM1000009ed07898RCRD&keyword=172.802

http://www.dhs.gov/csat-security-vulnerability-assessment