CONCENTRIC SECURITY UNIVERSITY

Chemical Facility Anti-Terrorism Standards (CFATS) Briefing

INTENT/PURPOSE

In Section 550 of the Homeland Security Appropriations Act of 2007 (P.L. 109-295) (Act), Congress gave the Department of Homeland Security (DHS or the Department) regulatory authority over security at high-risk chemical facilities. In the Act, Congress instructed DHS to require all high-risk chemical facilities to complete security vulnerability assessments, develop site security plans, and implement protective measures necessary to meet DHS-defined risk-based performance standards.

GENERAL SUMMARY STATEMENT

Among other things, CFATS establishes eighteen Risk-Based Performance Standards (RBPSs) that identify the areas for which a facility's security posture will be examined, such as perimeter security, access control, personnel surety, and cyber security. To meet the RBPSs, covered facilities2 are free to choose whatever security programs or processes they deem appropriate, so long as they achieve the requisite level of performance in each applicable area.

MAJOR TOPICS ADDRESSED

The guideline addresses the following 18 Risk Based Performance Standards:

1. Restrict Area Perimeter-Secure and monitor the perimeter of the facility.
2. Secure Site Assets - Secure and monitor restricted areas or potentially critical targets within the facility.
3. Screen and Control Access - Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter.
4. Deter, Detect, and Delay - Deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful.
5. Shipping, Receipt, and Storage - Secure and monitor the shipping, receipt, and storage of hazardous materials for the facility.
6. Theft and Diversion - Deter theft or diversion of potentially dangerous chemicals.
7. Sabotage - Deter insider sabotage.
8. Cyber – Deter cyber sabotage, including preventing unauthorized on-site or remote access to critical process controls.
9. Response – Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders.
10. Monitoring - Maintain effective monitoring, communications and warning systems.

© 2011 Concentric Security - All Rights Reserved

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.
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. RBPS 18 – Records addresses the creation, maintenance, protection, storage, and disposal of appropriate security-related records pursuant to 6 CFR § 27.255 and the activities required to make these records available to DHS upon request.

CONCENTRIC SECURITY
UNIVERSITY

Concentric Security University
7560 Main Street, Sykesville, MD 21784
P 410.552.9950 F 410.552.9939
Website: www.ConcentricU.com
Email: info@ConcentricU.com

11/2011
© 2011 Concentric Security - All Rights Reserved