KERAMIDA
ENGINEERS • SCIENTISTS • PLANNERS
GLOBAL EHS & SUSTAINABILITY SERVICES

CHEMICAL FACILITY ANTI-TERRORISM STANDARDS (CFATS)

ANNUAL SECURITY PLAN AUDITING- STRATEGIES FOR SUCCESS

Agenda

- Overview
- Who is affected?
- What are the requirements?
- Benefits of a security plan?
- Audit framework
- Strategies for change
- Summary

Overview

- Chemical Facility Anti-Terrorism Standards (CFATS) Program
  - 2007 – Established to identify and regulate high-risk facilities that possess certain chemicals of interest (COI) at specific concentrations and quantities.
    - Overseen by the U.S. Department of Homeland Security through the Infrastructure Security Compliance Division (ISCD).
    - Protect and prevent chemicals from being released, stolen and/or sabotaged by terrorists.
  - 2014 – Program was amended through The Protecting and Securing Chemical Facilities from Terrorist Attacks Act.
  - January 2019 - Authorization for the program is set to expire. The necessary security measures need to be implemented by affected facilities.

Who is affected?

- CFATS applies to all facilities that meets or exceeds the screening threshold quantities for any listed chemical of interest.
  - Chemical manufacturing, storage and distribution
  - Energy and utilities
  - Agriculture and food
  - Mining
  - Universities and laboratories
  - Healthcare and pharmaceuticals
  - Electronics
  - Paint and coatings
  - Plastics

What are the requirements?

- Determine if your facility manufactures, stores or distributes any chemicals of interest (COI) above the screening threshold quantities. See Appendix A (www.dhs.gov/publication/appendix-final-rule).
- If your facility possesses COI at or above the screening threshold quantities then complete a Top-Screen (www.dhs.gov/csat-top-screen) about your chemical holdings via the Chemical Security Assessment Tool (CSAT).
  - Will determine if facility is high risk. Rankings are from 1 through 4.
- If determined to be high risk then a Security Vulnerability Assessment (SVA) and a Site Security Plan (SSP) – or an Alternative Security Plan (ASP) must be submitted. (www.dhs.gov/cfats-risk-based-performance-standards)
- The ISCD will perform an inspection of your facility prior to approving the security plan.
  - Once plan is approved compliance inspections will be conducted regularly to verify agreed-upon security measures are implemented.

What are the benefits of a security plan?

- Highlights where various security measures need to be strengthened. Evaluates the effectiveness of methodologies and promotes risk analysis.
- Increases compliance through improved accountability of personnel. Requires an evaluation of processes and methods.
- Establishes the institutionalization of security activities within the organization.
- Demonstrates continuous improvement through annual training and the incorporation of lessons learned from audits.
- It is an overall business enhancing byproduct. Provides a value-add back to the business.

Annual Audit Framework

1) **AREA PERIMETER – EFFECTIVE SECUREMENT AND MONITORING OF THE PERIMETER OF THE BUILDING**

- Perimeter barriers (fences, gates, bollards, walls, water, etc.)
  – controls vehicular and pedestrian access
  - provides channeling to facility entry
  - delays forced entry and protects critical assets
- Intrusion detection systems (electronic sensors, remote surveillance, human-based)
- Lighting
- Protective forces (proprietary or contracted out)
  - Armed or unarmed
  - Standing post, monitoring critical assets, roving patrols

2) SECURE SITE ASSETS – EFFECTIVE SECURMENT AND MONITORING OF RESTRICTED AREAS AND/OR CRITICAL ASSETS WITHIN THE FACILITY

- Secure with barriers (fencing, walls, man-made obstacles, natural obstacles, etc.)
- Monitoring and intrusion detection systems (electronic sensors, remote surveillance, human-based)
- Protective forces (proprietary or contracted out)
  - Armed or unarmed
  - Standing post, monitoring critical assets, roving patrols

3) SCREEN AND CONTROL ACCESS – THE IDENTIFICATION, SCREENING AND/OR INSPECTION OF INDIVIDUALS AND VEHICLES

- Personnel identification – photo IDs
- Hand-carried items inspection
- Vehicle identification and inspection – visual inspections, cargo inspection systems, under/over inspection systems, etc.
- Control point measures – road alignment, speed bumps, gates, etc.
- Parking security measures

4) DETER, DETECT AND DELAY – THE PREVENTION, RECOGNITION AND THE ABILITY TO CREAT SUFFICIENT TIME BEFORE AN ATTACK BECOMES SUCCESSFUL SO THAT RESPONSE MEASURES CAN BE ENACTED

- Measures implemented to discourage attackers from pursuing access into facility and/or restricted areas. Also, the ability to identify and delay unauthorized access.
  - Perimeter and/or restricted area barriers
  - Intrusion detection systems
  - Lighting
  - Protective forces
  - Response planning
  - Communication – cell phones, radios, PA/alarm systems

5) SHIPPING, RECEIPT AND STORAGE – SECUREMENT AND OVERSIGHT OF THE SHIPPING, RECEIPT AND STORAGE OF HAZARDOUS MATERIALS

- Product stewardship – knowing where product is located and ensuring the material is being delivered or received from a known entity
  - Control procedures are in place
  - Transactions are verified
- Inventory controls – lists of hazardous material, tracking procedures, monitoring and regular report generation
- Training on how to identify and report on suspicious activities

6) THEFT OR DIVERSION - PREVENTION OF THEFT OR DIVERSION OF HAZARDOUS CHEMICALS THAT COULD BE USED FOR MALICE ON OR OFF-SITE

- Restricted access to COI
- Know-your-customer provisions – verification of customer qualification criteria and confirmation of identity
- Background checks for employees and contractors involved with COI
- Monitoring of COI
- Physical security of COI – chains, locks, detection devices, etc.
- Limited vehicular access
- Vehicular inspections
- Inventory controls
- Tamper evident devices – seals for vehicle valves
- Cyber security for COI

7) SABOTAGE – PREVENTION OF THE INSIDE DESTRUCTION OR DAMAGING OF A FACILITY

- Procedures in place
- Tamper evident devices
- Visitor controls – escort and access controls, identification

8) CYBER SECURITY – PREVENTION OF UNAUTHORIZED ON-SITE OR REMOTE ACCESS TO CRITICAL PROCESS CONTROLS

- Security policies, plans and procedures
- Access control
- Personnel security
- Awareness and training
- Security controls, monitoring, response and reporting
- Disaster recovery and business continuity
- System development and acquisition
- Configuration management

9) RESPONSE – DEVELOPMENT AND TRAINING ON EMERGENCY PLANS TO RESPOND TO SECURITY INCIDENTS

- Crisis management plan
- Communication systems
- Process safeguards
- Outreach

10) MONITORING –MAINTENANCE OF EFFECTIVE MONITORING, COMMUNICATIONS AND WARNING SYSTEMS

- Inspection, testing and preventative maintenance procedures
- Outages
- Repairs
- Maintenance personnel surety

11) TRAINING – ASSURANCE OF PROPER SECURITTY TRAINING, EXERCISES AND DRILLS OF PERSONNEL

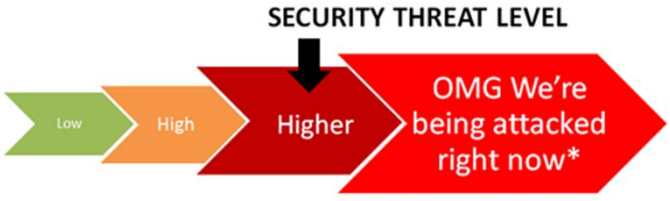
- Security training program for security and non-security personnel
  - Including drills and exercises

12) PERSONNEL SURETY – CONFIRMATION OF BACKGROUND CHECKS AND CREDENTIALS

- New/prospective employees and unescorted visitors
  - existing employees
  - contents of background checks
  - terrorist screening
  - annual audits

13) ELEVATED THREATS – CAPABILITY OF ESCALATING THE LEVEL OF PROTECTIVE MEASURES

- Procedures and time limits



14) SPECIFIC THREATS, VULNERABILITIES OR RISKS– ABILITY TO ADDRESS

- Documentation and training

15) SIGNIFICANT SECURITY INCIDENTS – ABILITY TO REPORT INTERNALLY AND TO LAW ENFORCEMENT

- Reporting procedures and knowing who to notify

16) SIGNIFICANT SECURITY INCIDENTS AND SUSPICIOUS ACTIVITIES – ABILITY TO IDENTIFY, INVESTIGATE, REPORT AND MAINTAIN RECORDS

- Investigative procedures and lessons learned

17) OFFICIALS AND ORGANIZATION – ESTABLISHMENT OF OFFICALS AND AN ORGANIZATION RESPONSIBLE FOR SECURITY

- Establish responsibilities for owner/operator, corporate security officer, facility security officer, cyber security officer and facility management

18) RECORDS – MAINTENANCE

- Maintain the following records:
  - training
  - drills and exercises
  - security incidents
  - maintenance
  - security threats
  - audits
  - letters of authorization
  - correspondence with the Department of Homeland Security
  - alternative security plan

Strategies To Implement Change

Control
- The ability to manage activities and assets.
- Have policies, procedures and technologies in place that establish rights, authorities and responsibilities.
- Provide monitoring and feedback.
- Control applies to nearly every aspect of security.

Detect
- The ability for a facility to identify the fact that it is under attack.
- Detection is the first step in response.
- The sooner the attack is detected, the sooner an appropriate response can be initiated.

Deter
- This is the perception on the part of the adversary that the effort required to mount a successful attack is greater than that required for an alternative target.
- Leads to reluctance on the part of the adversary to mount an attack or drives the adversary to select an alternative facility.
- The more protection that exists between an adversary and a targeted asset, the lower the likelihood that the adversarial attack will succeed.

Delay
- The ability of a facility's security program to keep an adversarial attack from succeeding long enough for an appropriate response plan to be deployed.

Questions?

KERAMIDA
ENGINEERS • SCIENTISTS • PLANNERS
GLOBAL EHS & SUSTAINABILITY SERVICES