The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

Chemical Facility Anti-Terrorism Standards (CFATS):
Compliance Lessons Learned and Guideposts

DHSChemSecurityTalks - West

June 2018

Homeland Security

CFATS Trends and Developments

- DHS designed and released an enhanced risk tiering methodology and the new CSAT 2.0 in fall 2016, retiering is now near completion
- These new tools allowed DHS to refine our Site Security Plan (SSP) tool using one of our previous best practices to align the risk-based performance standards into overarching security objectives or “Guideposts”

Homeland Security

Overarching Security Objectives

As a best practice, DHS has now grouped these 18 RBPS into 5 Security Objectives:

Detection

- Covers portions of Risk-Based Performance Standard (RBPS) 1-7

Delay

- Covers portions of RBPS 1-7

Response

- Covers portions of RBPS 11 and RBPS 9, 13-14

Cybersecurity

- Covers RBPS 8

Security Management

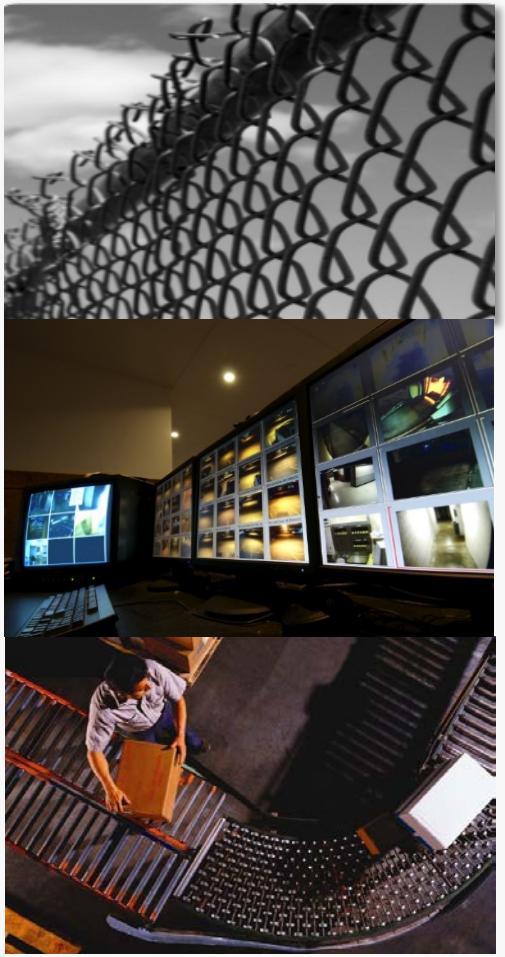
- Covers portions of RBPS 7 and 11 and RBPS 10, 12, and 15-18

Homeland Security

Detect and Delay RBPS

The first seven RBPS address the Detection and Delay objectives

- RBPS 1—Restrict Area Perimeter
- RBPS 2—Secure Site Assets
- RBPS 3—Screen and Control Access
- RBPS 4—Deter, Detect, and Delay
- RBPS 5—Shipping, Receipt, and Storage
- RBPS 6—Theft or Diversion
- RBPS 7—Sabotage



Homeland Security

Detection

- If a facility chooses to utilize systems (IDS, ACS, or CCTV) for detection, DHS seeks to ensure they:
  - Cover the appropriate areas and/or entry points.
  - Are activated at appropriate times.
  - Alarm to a responsible and trained individual(s) in order to initiate a response.
- If the facility utilizes employees or on-site security personnel, they must:
  - Be capable and trained to provide detection.
  - Be dedicated to or conduct patrols of the necessary areas.

Homeland Security

Detection (cont.)

Security Issue	Tier 1	Tier 2	Tier 3	Tier 4
Theft/Diversion	Maintain a high likelihood of detecting attacks at early stages resulting in the capability to continuously monitor the critical asset or facility perimeter; allow for the notification of intrusion to a continuously manned location. This may be achieved by physical security systems (such as IDs or CCTV) or personnel presence, or a combination thereof, with no gaps.		Maintain reasonable ability to detect and initiate a response in real time; for example, ensuring monitoring systems are checked multiple times a day, including weekends.	Maintain some ability to detect and initiate a response; for example, ensuring monitoring systems are checked at least once a day, including weekends.
Release			Maintain a high likelihood of detecting attacks at early stages resulting in the capability to continuously monitor the critical asset or facility perimeter; allow for the notification of intrusion in real time. This may be achieved by physical security systems or personnel presence, or a combination thereof, with no gaps, OR via process alarms with automatic mitigation measures.**	
Sabotage			Maintain ability to detect attempted tampering prior to shipment. This may include traditional detection methods or perimeter-based detection of incoming substances through ingress screening and inspections or shipping procedures requiring inspection prior to egress.	

Homeland Security

Additional Considerations for Release COI

- Release-Toxic facilities that have automatic mitigation measures—such as dikes or other containment measures—that would be successful in reducing the effects of the attack or slowing the release from impacting the targeted population may not require continuous intrusion detection if they have a detection capability at the moment of the release through process alarm or similar device.
- Release-Flammable facilities with strong mitigation measures—such as the use of an automatic deluge system that can provide fire suppression through the use of extinguishing materials such as water, foam, dry powder chemicals, or inert gases—that could prevent an attack from being successful may also not require continuous intrusion detection if they have a detection capability at the moment of the release such as a heat sensor or similar device.

Delay

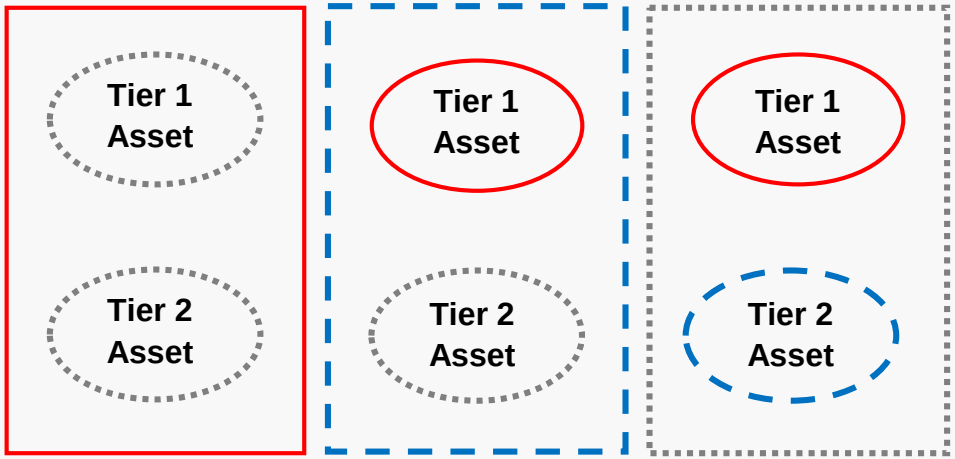
- A facility should be able to delay an attack for a sufficient period of time to allow appropriate response by security personnel via barriers and barricades—such as fencing, walls, locking mechanisms, bollards, etc.—and hardened targets.

- Delay measures should also take into account security issues, for example, a Release facility should also consider strong vehicle barriers and sufficient vehicle standoff distances around the COI. The required standoff distances will vary depending on the building components used in the construction of the facility.

Homeland Security

Facility vs Asset Protection

- Facilities may choose to deploy security measures at the perimeter, asset, or both.
- Defining assets and deploying security measures at specific assets is particularly important to facilities which require restriction to some employees, customers, etc., such as:
  - Universities/Colleges;
  - Hospitals;
  - Store Front operations; and
  - Co-located facilities.



Homeland Security

Tip: Access Control and Personnel Surety

- No matter which option is chosen, a facility must consider:
  - How is access controlled and validated?
  - Who at the facility has access?
    - Have these individuals been properly trained?
    - Have these individuals received the appropriate background checks?

Homeland Security

Response

Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders.

- Response focuses on the planning to mitigate, respond, and report incidents in a timely manner between facility personnel, first responders, and law enforcement
- Local Emergency Planning Committees (LEPC) may be contacted by local Chemical Security Inspectors to verify that facilities have developed plans for emergency notification, response, evacuation, etc.
- IP Gateway (EO Portal) – A DHS platform to share and coordinate CFATS information among Federal, State, local, territorial, and tribal (SLTT) agencies partners.

Homeland Security

Response (cont.)

What are some possible facility security components related to Response?

- Crisis Management Plan
- Communication Systems
- Process Safeguards
- Outreach

What are some activities a facility may want to include in its Crisis Management Plan?

- Contingency Plans
- Continuity of Operations Plan
- Emergency Response
- Post-incident Security
- Evacuation
- Notification Control
- Re-entry
- Security Response

Homeland Security

Cyber Security

RBPS 8 addresses the deterrence of cyber sabotage, including preventing unauthorized on-site or remote access to critical process controls, critical business systems, and other sensitive computerized systems.

- Computerized systems are replacing methods of business across numerous industries. As these methods change so do the vulnerabilities that chemical facilities face. Cyber intrusions to control systems and critical information are more common than ever which is why protecting against these cyber attacks is an essential component in managing overall risk for a facility.
- The goal of cybersecurity is to reduce the risk of attackers conducting malicious attacks on critical systems, which could result in theft, diversion, release, or sabotage of chemicals of interest (COI).

Homeland Security

Cyber Security Systems

- When considering what systems could impact the security of the COI, facilities should examine:
  - Physical security systems
    - Does the facility employ an intrusion detection system, cameras, or an access control system?
  - Inventory management
    - Does the facility utilize software to manage ordering, shipping, or inventory?
  - COI Processing
    - Does the facility employ any control systems (ICS, DCS, SCADA)?

Homeland Security

Cyber Security Considerations

- For all of the identified systems, the facility should identify measures to address:
  - Access control and password management
  - System boundaries and security controls
  - Cyber security training
  - Network monitoring
  - Incident response and reporting
  - Associated policies and procedures

Homeland Security

Security Management

Security Management is the capability to manage the SSP/ASP, including the development and implementation of policies, procedures and other processes that support Site Security Plan implementation and oversight.

Homeland Security

Security Management (cont.)

- To ensure your facility is effectively implementing all RBPS within the security management guidepost:
  - Clearly document and communicate all policies and procedures
  - Maintain all associated records
  - Be capable of presenting these to inspectors

Training and Exercise Policies and Records

Incident and Threat Policies and Records

Maintenance Program Records

Outreach with First Responders

Background Check Procedures

Inventory Records

Contractual Documents

Homeland Security

Annual Audit

- The required SSP/ASP annual audit is one way facilities should ensure they are staying in compliance with their approved SSP/ASP
- This audit could include:
  - Verification of Top-Screen and SVA data
  - Confirmation of all Chemical Security Assessment Tool (CSAT) user roles
  - Confirmation of all existing and planned measures from the SSP/ASP
  - Sampling of RBPS 18 records
  - Review of current policies, procedures, training, etc.

Homeland Security

Overarching Lessons Learned

- Over 75% of facilities require at least one planned measure in order to satisfy the Risk Based Performance Standards (RBPS). Make sure you are implementing these in accordance with your approved plan.
- Involving employees in the development and implementation of the SSP/ASP can greatly assist in maintaining its accuracy and identifying changes or issues early enough to resolve appropriately.
- Identify DHS, state, and local resources to assist in satisfaction of the RBPS such as training, exercises, response, recordkeeping, etc.

Homeland Security

Available Resources

Outreach: DHS outreach for CFATS is a continuous effort to educate stakeholders on the program.

- To request a CFATS presentation or a CAV, submit a request through the program website www.dhs.gov/chemicalsecurity, or email DHS at CFATS@hq.dhs.gov

CFATS Help Desk: Direct questions about the CFATS program to the CFATS Help Desk.

- Hours of Operation are Mon. – Fri. 8:30 AM – 5:00 PM (ET)
- CFATS Help Desk toll-free number 1-866-323-2957
- CFATS Help Desk email address csat@dhs.gov

CFATS Web Site: For CFATS Frequently Asked Questions (FAQs), CVI training, and other useful CFATS-related information, please go to www.dhs.gov/chemicalsecurity.

Homeland Security

Homeland Security

For more information, visit:
www.dhs.gov/critical-infrastructure

Kelly Rae Murray

ISCD, Deputy Branch Chief

Kelly.Murray@hq.dhs.gov