

The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

Chemical Facility Anti-Terrorism Standards (CFATS)

June 2015



Homeland
Security

Why Chemical Facility Security?

- We face a persistent & evolving threat from terrorist groups & cells.
- Chemical facilities potentially are attractive targets as:
 - A successful attack on some chemical facilities could potentially cause a significant number of deaths and injuries.
 - Certain chemical facilities possess materials that could be stolen or diverted and used as or converted into weapons for use offsite.
- In 2007, Congress authorized the Department to regulate security at “high-risk” chemical facilities.
 - The Department developed the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, to implement this authority.
- In December 2014, Congress passed H.R. 4007: *Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014* (The CFATS Act of 2014).
 - The President signed The CFATS Act of 2014 into law on December 18, 2014

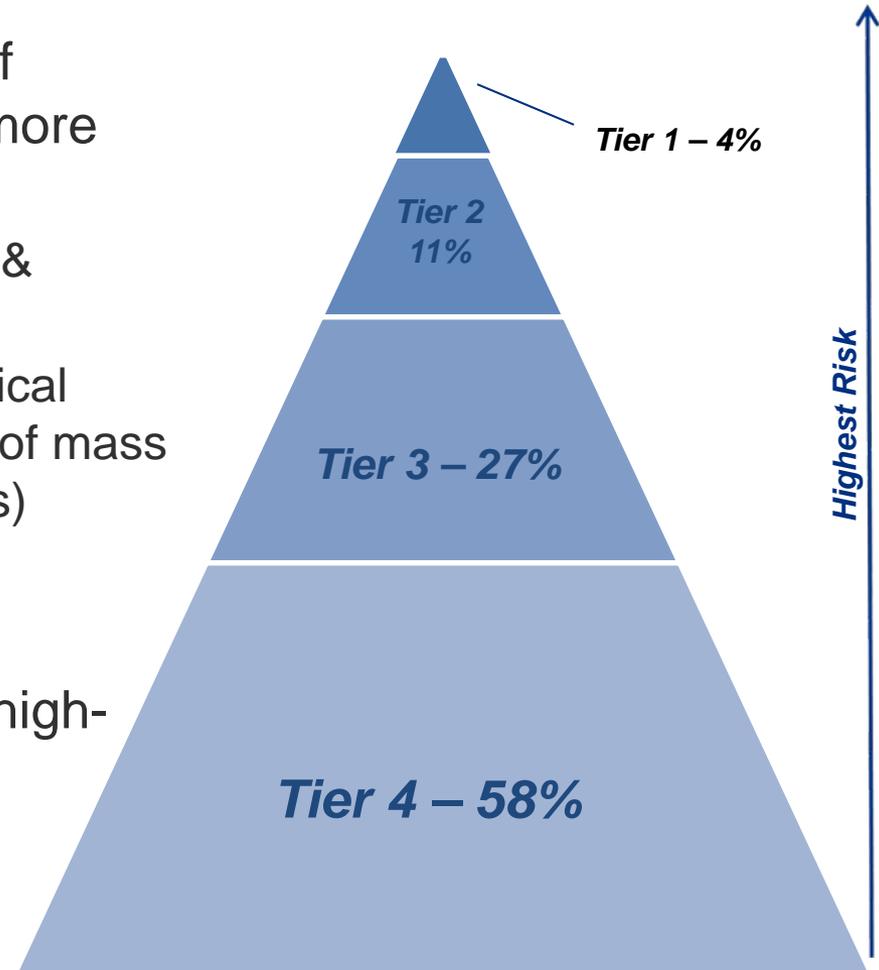
Who Is Regulated?

- To determine if a facility is subject to CFATS, DHS looks at the unique circumstances faced by the facility, starting with the quantities of Chemicals of Interest (COI) the facility possesses.
- Potential regulation is *not* based on the facility type, meaning that many different types of facilities may be subject to CFATS, including:
 - Chemical manufacturers
 - Warehouse and distributors
 - Chemical repackaging operations
 - Oil and gas operations
 - Hospitals
 - Semi-conductor manufacturers
 - Paint manufacturers
 - Colleges and universities



Essentials of the CFATS Program

- High-risk facilities contain chemicals of interest (COI) that give rise to one or more **security issues**, such as:
 - **Release chemicals** (toxic, flammable & explosive)
 - **Theft or diversion chemicals** (chemical weapons and/or precursors, weapons of mass effect, and explosive and/or precursors)
 - **Sabotage and contamination**
- Covered facilities are placed in 1 of 4 high-risk tiers



Stats current as of 1/26/15

Risk-Based Performance Standards (RBPS)

- RBPS are the foundation of the Site Security Plan (SSP) and Alternative Security Programs (ASP) of the CFATS program, where they drive the security performance at all tiered facilities.
- CFATS currently has 18 RBPS, addressing areas such as perimeter security; shipping, receipt, and storage; cybersecurity; personnel surety; training; and recordkeeping.
- RBPS provide facilities with substantial flexibility and allow for the use of existing or planned measures, ideas, and expertise where appropriate.
- A covered high-risk facility has to meet the applicable RBPS with measures appropriate for the facility's level (tier) of risk.
- Measures appropriate to meet the RBPS for one type of facility will not necessarily be appropriate for another type of facility.



Risk-Based Performance Standards (RBPS)

1. Restrict area perimeter
2. Secure site assets
3. Screen and control access
4. **Deter, detect, delay**
5. Shipping, receipt, and storage
6. Theft and diversion
7. Sabotage
8. Cyber
9. **Response**
10. Monitoring
11. **Training**
12. Personnel surety
13. Elevated threats
14. Specific threats, vulnerabilities, or risks
15. **Reporting of significant security incidents**
16. **Significant security incidents and suspicious activities**
17. Officials and organization
18. Records

First Responders and CFATS

- Collaboration between CFATS covered facilities and first responders is critical to ensuring a secure and resilient community.
- Compliance with several RBPSs may leverage the emergency response community, such as:
 - Detect, deter, delay (RBPS 4)
 - Response (RBPS 9)
 - Training (RBPS 11)
 - Reporting of significant security incidents (RBPS 15)
 - Significant security incidents and suspicious activities (RBPS 16)
- Facilities are encouraged to coordinate with the emergency response community as they develop these aspects of their SSPs/ASPs.

RBPS 4 – Deter, Detect, and Delay

- Purpose – Deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful. This includes measures to:
 - **Deter** vehicles from penetrating the facility, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets;
 - **Deter** attacks through visible, professional, well maintained security measures and systems, including security personnel, detection systems, barriers and barricades, and hardened or reduced value targets;
 - **Detect** attacks at early stages, through counter-surveillance, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers and barricades; and
 - **Delay** an attack for a sufficient period of time to allow appropriate response through onsite security response, barriers and barricades, hardened targets, and well-coordinated response planning.



RBPS 9 Response

- Purpose – Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders.
- In the context of this RBPS, “response” includes actions to mitigate the consequences of an adversary’s action.
- RBPS 9 typically focuses on the emergency response to a fire, aerial release, or other loss of containment of a COI as the result of a security incident.
- Activities performed in support of RBPS 9 may include:
 - The development of crisis management plans and procedures
 - Training, drills, and exercises, including drills with local first responders; and
 - The purchase of emergency response equipment, including radios or other backup communications systems, and the establishment of emergency notification systems.
 - Outreach and liaison with LEPC, FD and LE

RBPS 11 – Training

- Purpose – Facility must ensure that personnel have proper security training, exercises, and drills.
- A common, but not required, approach to satisfying this RBPS is the development of a Security Awareness and Training Program (SATP). SATP components may include:
 - Training, such as hands-on activities, seminars, workshops, etc.;
 - Exercises, such as tabletops, functional, and full-scale;
 - Drills;
 - Tests, such as static, dynamic ,or functional; and
 - Joint Initiatives with local law enforcement and first responders.

RBPS 15 – Reporting of Incidents

- Purpose – Report significant security incidents to DHS and to local law enforcement officials.
- This typically involves four steps:
 - (1) Identifying a security incident;
 - (2) Reporting it to facility security;
 - (3) Determining whether or not the incident is a significant security incident; and
 - (4) If it a significant security incident, reporting it to DHS and local law enforcement.
- Many facilities will also have procedures and related training on how they will accomplish those steps.
- Near Misses – Simply because an attack or other incident is not carried out successfully does not mean that the incident was insignificant and should not be reported.



RBPS 16 – Incidents and Suspicious Activities

- Purpose – Identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site.
- This RBPS complements RBPS 15, focusing on how a facility will identify, investigate, report, and maintain records on significant security incidents and suspicious activities. These activities may serve varied purposes, including:
 - Identifying if a security incident has occurred;
 - Gathering evidence for potential law enforcement investigation; and
 - Identifying gaps or weaknesses in a facility’s security posture so those gaps can be closed.
 - To comply with this RBPS, facilities often will demonstrate -
 - Written investigation and reporting procedures; and
 - A process for identifying, disseminating, and acting upon lessons learned.

CFATS SSP/ASP Process



Homeland Security

Initiate CFATS Process		Complete Top-Screen		Complete SVA or ASP	
Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Facility with Chemicals of Interest (COI) at or above the Screening Threshold Quantity (STQ) recognizes the need to submit a Top-Screen and completes CVI training and CSAT user registration.	CFATS Help Desk registers the facility and provides a user ID and password.	Facility completes Top-Screen, identifying chemicals and quantities and providing other relevant information.	DHS reviews Top-Screen information and determines the facility's Preliminary Tier status or determines that facility is not high-risk.	DHS sends facility a Preliminary Tier letter and deadline for completing a Security Vulnerability Assessment (SVA) or an Alternative Security Program (ASP for Tier 4 facilities, if they choose). If DHS has determined that the facility is not high-risk, the facility is sent a letter releasing it from further regulation.	Covered (high-risk) facility completes an SVA or ASP to provide more detailed information about COI and vulnerability to attack.
SVA/ASP Review		Complete SSP or ASP		Authorization	
Step 7	Step 8	Step 9	Step 10	Step 11	Step 12
DHS reviews SVA or ASP information provided and determines facility's Final Tier or that facility is not high-risk.	DHS notifies the facility of its final status and tiered facilities are provided deadlines for completing an Site Security Plan (SSP) or ASP.	Facility completes an SSP or ASP detailing site-specific security measures to satisfy applicable Risk-Based Performance Standards.	DHS reviews SSP or ASP and (a) issues authorization letter for SSP or ASP and schedules an inspection or (b) issues notice to resolve deficiencies. Failure to resolve deficiencies may result in disapproval.	DHS conducts authorization inspection, reviews all available information, and either issues a Letter of Approval for the SSP or ASP or issues notice to the facility to resolve deficiencies. Failure to resolve deficiencies may result in disapproval.	If SSP or ASP is approved, DHS conducts compliance inspections on a regular and recurring basis to verify continued compliance with the approved SSP or ASP. 

First Responders

Information on chemical facilities in your area.

- DHS and EPA resources are available to First Responders
 - Planning Right-to-Know Act
 - Risk Management Program
 - CFATS information
- Future Resource: Infrastructure Protection (IP) Gateway
 - Risk Analysis
 - Critical Infrastructure Vulnerability Assessments
 - Event and Incident Planning
- Access to Information is Protected
 - Contact your regional director for access



The screenshot shows a webpage with a blue header and a white main content area. The header includes the DHS logo and the text 'Homeland Security' and 'Law Enforcement and First Responders'. The main content area has a blue box with white text that reads: 'There are a number of avenues available for law enforcement and first responders to access information about chemical facilities in their area. The Environmental Protection Agency (EPA) and the Department of Homeland Security (DHS) have established databases by which law enforcement and first responder personnel with a need-to-know can access information pertaining to chemical facilities in their jurisdiction. The information available comes from EPA's Emergency Planning Right-to-Know Act (EPCRA) and Risk Management Program (RMP) as well as DHS's Chemical Facility Anti-Terrorism Standards.' Below this text is a photograph of an industrial facility with several tall chimneys. The page also contains sections for 'Emergency Planning Right-to-Know Act', 'Risk Management Program', and 'Additional information about State Tier II reporting requirements and procedures is available at: http://www2.epa.gov/epcra/state-tier-ii-reporting-requirements-and-procedures'.

Law Enforcement and First Responders

There are a number of avenues available for law enforcement and first responders to access information about chemical facilities in their area. The Environmental Protection Agency (EPA) and the Department of Homeland Security (DHS) have established databases by which law enforcement and first responder personnel with a need-to-know can access information pertaining to chemical facilities in their jurisdiction. The information available comes from EPA's Emergency Planning Right-to-Know Act (EPCRA) and Risk Management Program (RMP) as well as DHS's Chemical Facility Anti-Terrorism Standards.

Emergency Planning Right-to-Know Act

The Emergency Planning Right-to-Know Act (EPCRA) was established in 1986 to help communities plan for emergencies involving hazardous substances. EPCRA ensures that local communities and first responders have needed information on potential chemical hazards within their communities in order to develop community emergency response plans and respond appropriately to chemical emergencies that may occur. Under EPCRA, companies are required to disclose chemical activities that surpass a specified threshold.

Facilities holding any substance for which the facility must maintain a Safety Data Sheet (SDS) under the Occupational Safety and Health Administration's Hazard Communication standard above threshold quantities must submit an Emergency and Hazardous Chemical Inventory Form – called a "Tier II Report." This report must be submitted annually – by March 1 – to the State Emergency Response Commission (SERC), Local Emergency Planning Committee (LEPC), and the local fire department.

Additional information about State Tier II reporting requirements and procedures is available at: <http://www2.epa.gov/epcra/state-tier-ii-reporting-requirements-and-procedures>.

Risk Management Program

The Risk Management Program (RMP) was established in 1990 as a means of preventing and mitigating the consequences of chemical accidents. Owners and operators of facilities that manufacture, use, store, or otherwise handle any of the 140 listed flammable and toxic substances above threshold quantities in a process are required to submit a risk management plan to EPA. This plan must include information on the facility's hazard assessment, accident prevention mechanisms, and emergency response measures. Facilities must update the plan every five years (or sooner if major changes occur).

Additional information about accessing RMP information is available at: <http://www2.epa.gov/rmp/federal-reading-room-risk-management-plans-rmp>.

Chemical-terrorism Vulnerability Information

- CVI is an information protection regime authorized by Congress and created by CFATS to protect certain information developed or submitted as a result of the CFATS program from inappropriate public disclosure.
- Except in exigent or emergency circumstances, in order to possess CVI, individuals must complete the Department's CVI Authorized User Training and must have a "need to know."
 - For those who need to become CVI Authorized Users, DHS offers online training at <http://www.dhs.gov/chemicalsecurity>.
- Information needed by emergency responders is often not CVI. However, under exigent or emergency circumstances, CVI can be shared without all parties being CVI authorized.



Homeland Security

For more information visit:
www.dhs.gov/criticalinfrastructure

Paul Gilbreath

Infrastructure Security Compliance Division
Office of Infrastructure Protection
Paul.gilbreath@hq.dhs.gov