

***Chemical Facility  
Anti-Terrorism Standards  
(CFATS)  
Security Vulnerability Assessments***

**“Telling the Story about Your  
Facility’s Risk”**

# CFATS Implementation Schedule

## DHS Appropriations Act of 2007

- Identify Covered Facilities
  - Facilities that store or process Chemicals of Interest (COI) in quantities that meet or exceed the Screening Threshold Quantities (STQ)
- Required Initial Top-Screen
- Security Vulnerability Assessments (SVA's)
  - Determine the overall level of risk
- Site Security Plans (SSP's)
  - A comprehensive plan on how the risk to the facility will be mitigated
  - Alternate Security Program (ASP) accepted as well

# CFATS Top-Screen Process

## DHS Appropriations Act of 2007

- ◆ Required Top-Screen submissions for initial tiering
  - ◆ Based upon type and quantity of chemicals and consequences of concern
  - ◆ Provided DHS a rough order of magnitude for the number of facilities and their respective level of risk
  - ◆ Provides the facility owner with an idea of the level of risk and requisite security measures
- ◆ Results Published the Week of 24 June 08
  - ◆ Provides facilities with a start point for managing their risk
  - ◆ Starts the clock for the SVA
  - ◆ Is not the “Final Rule”; tiering may be changed

# CFATS Implementation Schedule

## DHS Appropriations Act of 2007

- ◆ Security Vulnerability Assessments (SVA's)
  - ◆ Purpose is twofold:
    - ◆ Validates the DHS tiering decision
    - ◆ ***Tells the story about the risk to the facility***
  - ◆ An automated process that conducts analysis via risk engine in the database.
  - ◆ Analyzes the risk to the facility by determining the end result of a an attack from a specific threat against a specific COI given specific consequences of concern.
  - ◆ Utilizes pre-determined modes of attack to represent the Threat
  - ◆ Consequence is assessed by considering three factors:
    - ◆ The chemical of interest
    - ◆ The type of hazard
    - ◆ The consequences of concern

# Facility Compliance Dates

Now that initial tiering decisions are made, facilities can calculate SVA due dates from the week of 24 June 08:

◆ Tier 1	219 Facilities	90 Days
◆ Tier 2	756 Facilities	120 Days
◆ Tier 3	1,712 Facilities	150 Days
◆ Tier 4	4,319 Facilities	180 Days

# SVA's: Telling your Story of Risk

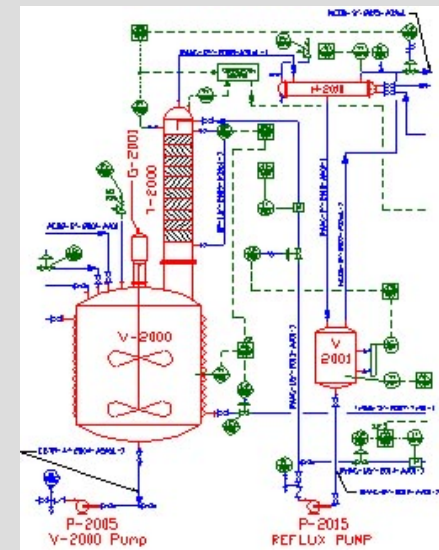
- ◆ Asset Characterization
- ◆ Threat Assessment
- ◆ Security Vulnerability Analysis
- ◆ Cyber Controls
- ◆ Countermeasure Analysis



# Asset Characterization

- ◆ What do I need to protect?
- ◆ General information about the facility
- ◆ Should pre-populate from Top-Screen input
- ◆ If you disagree with Top-Screen or believe data is inaccurate, call the help desk.
- ◆ Points to Consider:
  - ◆ The COI
  - ◆ The Security Issue
  - ◆ Consequences of Concern
  - ◆ Critical Assets
  - ◆ Existing layers of protection

***“I have 50 lbs of aluminum powder, that if stolen can be used to significantly raise the power of an explosive device used against the 300k people in the nearby city.”***



# Threat Assessment

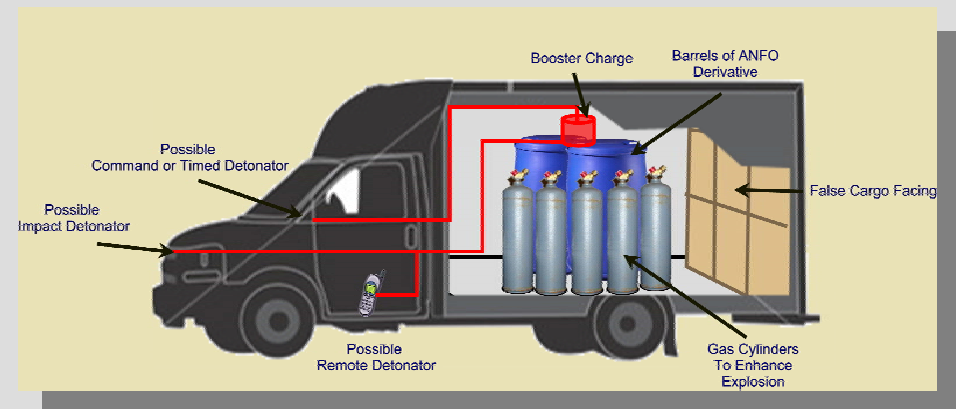
## What do I need to protect it from?

### The tool utilizes modes of attack, all may not apply

- Vehicle
- Maritime
- Aircraft
- Sabotage
- Theft
- Diversion
- Assault team
- Stand off (RPG or 50 cal etc)

### Types of Threats

- Internal
- Internal-Assisted
- External



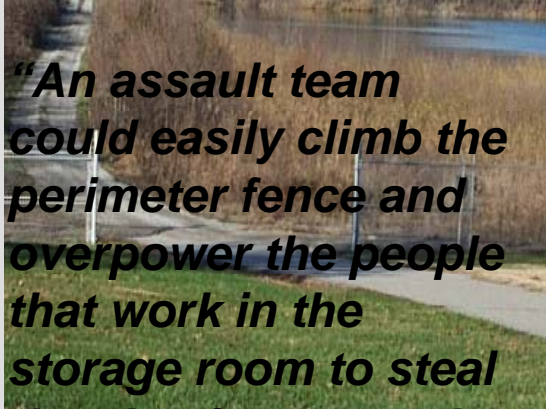
***“An assault team could attack the facility and steal the aluminum powder that can be used to significantly raise the power of an explosive device used against the 300k people in the nearby city.”***

# Security Vulnerability Assessments

◆ How can the threat exploit my critical assets?

◆ Points to Consider:

- ◆ What happens when the threat exploits my critical assets?
- ◆ Consider mode of attack and the security issue for the COI
- ◆ Discuss the existing counter measures and their level or degree of effectiveness as well as the vulnerabilities they are designed to mitigate.
- ◆ Discuss the degree to which the countermeasures meet or exceed the RBPS



***“An assault team could easily climb the perimeter fence and overpower the people that work in the storage room to steal the aluminum powder. The fence has no barbed wire and there are no locked doors or cabinets in the storage room. These security measures are highly insufficient to meet RBPS 1 and 4.*”**

# Countermeasure Analysis

- ◆ The facility must be able to describe how the countermeasure reduces the risk.
- ◆ Points to Consider:
  - ◆ What happens when the threat exploits my critical assets?
  - ◆ Consider mode of attack and the security issue for the COI
  - ◆ Discuss the existing counter measures and their level or degree of effectiveness as well as the vulnerabilities they are designed to mitigate.



# Cyber Control

- ◆ Considers Two Types of Systems
  - ◆ Cyber Control that control chemical processing tasks
  - ◆ Business Control Systems that facilitate the business but do not control the manufacturing
- ◆ Requirements or questions are in line with ISO 27001-2005 and 27002-2005 Standards



Questions?