

# EEI Security Committee Meeting

---

Austin, TX  
September 30, 2009

## CFATS Update

George T. Miserendino  
952-423-3457  
[solutions@tritonsecsol.com](mailto:solutions@tritonsecsol.com)

# Introduction to CFATS

---

- Its All About “Risk”
- **RISK = (Consequence) (Vulnerability) (Threat)**
  - Consequence
    - COI's + Proximity to a population center + precursor potential + perception
  - Vulnerability
    - The likelihood that an attack on a facility will be successful
    - Security Vulnerability Assessment
  - Threat
    - The intent and capability of an adversary with respect to attacking a facility
    - Defined by DHS

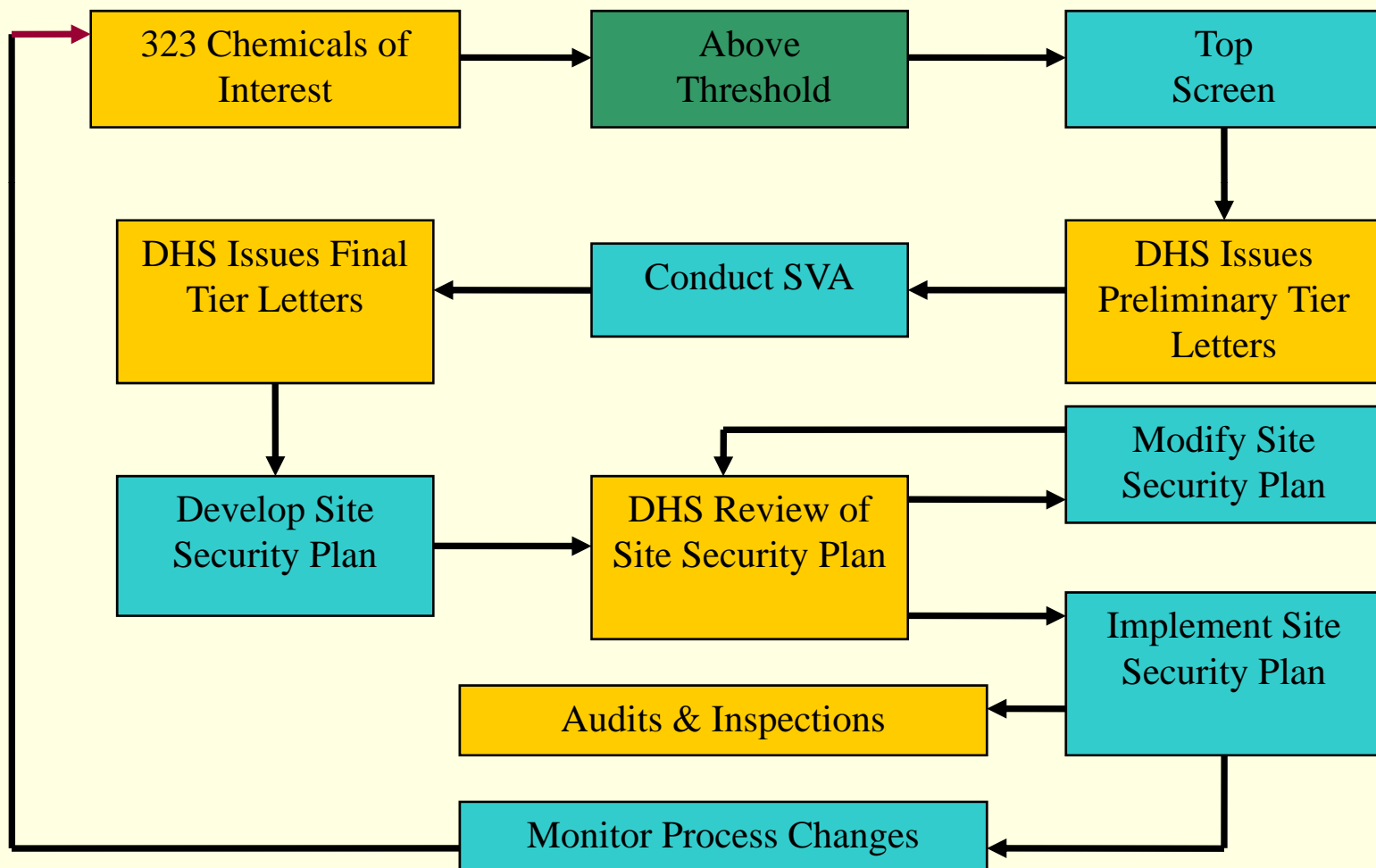
# Introduction to CFATS

---

## **Four Things to Remember**

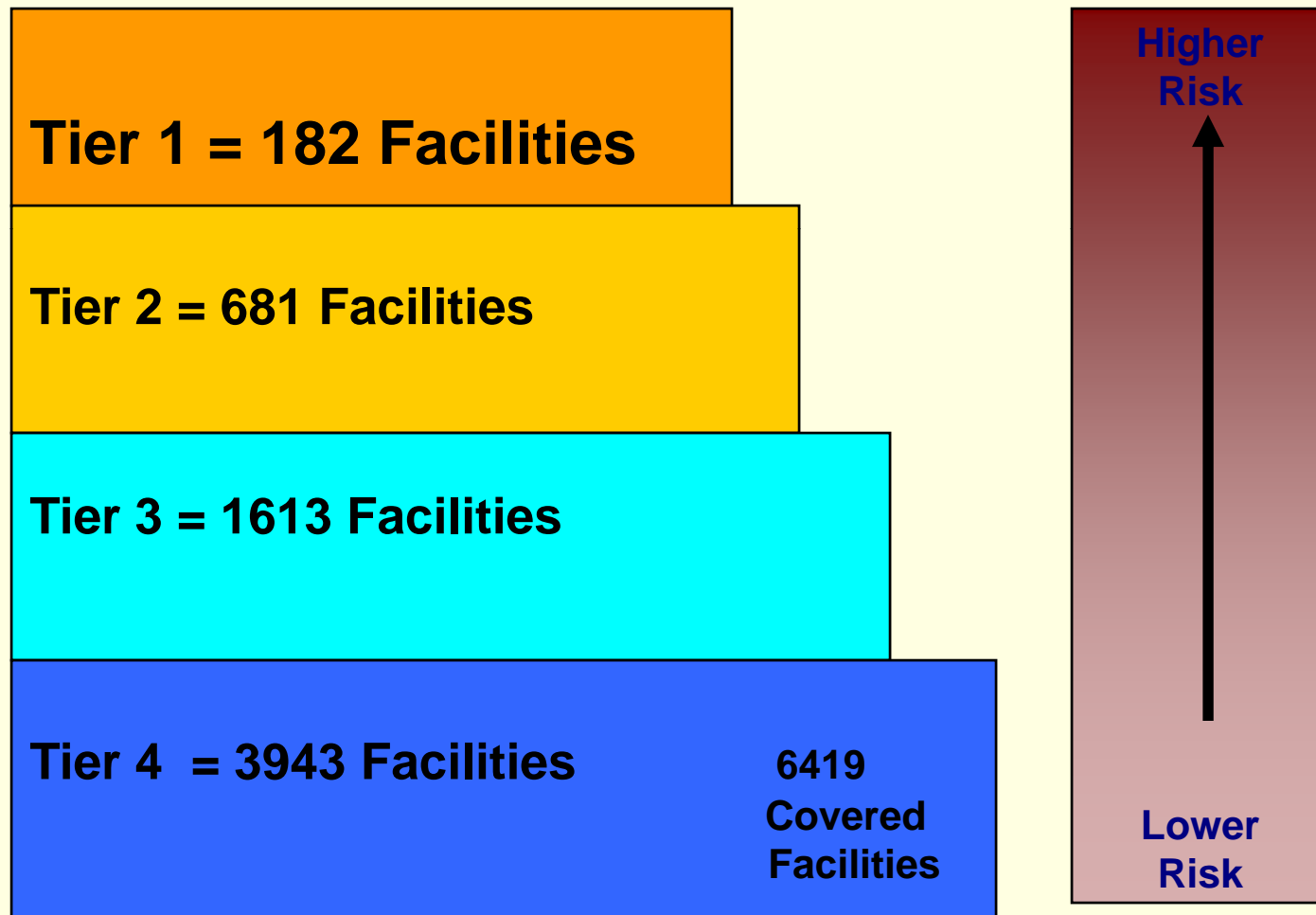
1. Federal Regulation 6 CFR 27
2. Facilities that use chemicals, not just chemical facilities
3. \$25,000 / Day and/or Closure
4. Ongoing inspections, audit, training

# DHS CFATS Process



# The CFATS Process

Top Screen= Who is Covered



# The CFATS Process

## Top Screen = Who is Covered

---

### **Chemical Security Assessment Tool (CSAT)**

#### ■ **Five secure, web based tools:**

1. Facility Registration
2. Top Screen (consequence screening)
3. Security Vulnerability Assessment Tool (SVA)
4. Site Security Plan Templates (SSP)
5. Personnel Surety (terrorist background checks)

#### ■ **Facility specific roles**

- Authorizer, Preparer, Submitter

# The CFATS Process

SVA = Likelihood of Success

---

- **SVA addresses COI's and "Security Issues"**
  - Release (Toxic Cloud, Explosion, Fire)
  - Theft/Diversion
  - Sabotage
- **Report on**
  - Security Equipment
  - Access Control
  - Inventory Control
  - Critical Assets
  - Cyber Security
  - Consequences of specified attacks

# The Eighteen CFATS Risk Based Performance Standards

---

- |                                  |  |
|----------------------------------|--|
| 1. Restrict Area Perimeter       | 11. Training   |
| 2. Secure Site Assets            | 12. Personnel Surety   |
| 3. Screen and Control Access     | 13. Elevated Threats   |
| 4. Deter, Detect and Delay       | 14. Specific Threats, Vulnerabilities or Risks               |
| 5. Shipping, Receipt and Storage | 15. Reporting of Significant Security Incidents              |
| 6. Theft Diversion               | 16. Significant Security Incidents and Suspicious Activities |
| 7. Sabotage                      | 17. Officials and Organization                               |
| 8. Cyber                         | 18. Records  |
| 9. Response                      |  |
| 10. Monitoring                   |  |

# The CFATS Process

SVA = Likelihood of Success

## CFATS Attack Scenarios

- **Aircraft Attack**
  - ❖ 737 crashes into storage tanks or processing areas
- **Vehicle Born Improved Explosive Device (VBIED)**
  - ❖ Adversary detonates BVIED outside perimeter near critical assets: gains entry by cutting gate during off-hours, crashing through the gate or by “piggy backing” through main gate.
- **Maritime/Boat Born IED Attack**
  - ❖ Adversary pilots boat IED onto or near critical assets and detonates.
- **Assault Team Attack**
  - ❖ Adversary climbs or cuts the facility perimeter fence.
  - ❖ Adversary attacks security assets at the access control point.
- **Standoff Attack**
  - ❖ Adversary fires light anti-tank weapon from outside the perimeter or gains entry and fires.
- **Theft**
  - ❖ Adversary enter the facility and steals COI.
- **Sabotage**
  - ❖ Adversary contaminates COI, result in an explosion or toxic release after shipment from facility.
- **Diversion**
  - ❖ Adversary arranges for shipment to address or picked-up at site. Not an authorized customer.

➤

# The CFATS Process

SVA = Likelihood of Success

---

## ■ SVA Likelihoods

- Access to critical assets
- Identifiability of critical assets
- Target hardness
- Effectiveness of response



# Facility Security Vulnerability Assessment Tool Results

---

- COI – Number of & their locations
- Threat – Types, Number & Understanding
- 120 days to submit Site Security Plan (SSP)
- SSP - On-line DHS tool: 3 year requirement
- SSP - it is a “reporting tool”, not a planning tool
- SSP - An analysis of the RBPS against what you has in place

# Facility Site “Conceptual” Security Plan

---

- **Conceptual “planning tool”**
- **Plan the facility program/plan before you submit the SSP**
  - Explain “how” security program/plan meets the performance requirements of the RBPS
  - Focus on COI threat
- **RBPS plan focus:**
  - Technologies
  - Policies
  - Procedures
  - Training

# CFATS Conceptual Plan Basis

---

- **18 RBPS organized into 6 basic criteria/characteristics:**

- Control
- Deterrence
- Detection
- Delay
- Response
- Management

# SSP Submittal for Tier 3

---

- Late November 09 - Online submittal
- Based on facility CFATS security plan/program - “**Conceptual Compliance Plan**”
- “**Situational Compliance Tool**” - no specific timeline to comply with submittal
- Identify
  - Applied Technologies
  - Procedures

# Conceptual Security Plan Recommendations

---

- Develop a “team approach” to gain consensus on:
  - Conceptual design for protection strategy
  - Fully integrated technologies
  - Procedure development
  - Design and location of SOC
  - Integration of the PACS

# CFATS Conceptual Plan

## Recommendations

---

- **Apply an integrated security systems approach consisting of:**
  - Delay and deterrence – barriers, fencing and walls
  - Detection - card readers, door alarms, and interior motion alarms
  - Assessment – interior/exterior video (MVD potential)
  - Response - onsite guards and local law enforcement

# Proposed Protection Strategy

---

## ■ **Defense in-depth at COI locations**

- Perimeter area fence and access control
- Building access control
- COI/CA rooms... IDS and assessment (video)

## ■ **Two levels of access control through applied technologies**

## ■ **COI protection**

- Card access control
- Video assessment
- IDS

# Consider a System Integrator

---

- Knowledge and experience on many PACS projects
- Knowledge of latest integration technologies
- Design and implementation experience
- Maintenance experience
- Equipment knowledge for the operating environment
- Integration experience for SOC design

# Path Forward

---

- Form a “team”
- Develop “**conceptual project plan**”
- ID Technology Application Approach
  - Select a “system integrator” - turn key approach
- ID final submittal schedule
- Develop (outline form) facility “CFATS Plan”
- Finalize list of **procedures** based on RBPS
- Establish **reasonable** end date in 2010
- Request a DHS assist visit to approve concept

# 10 Things to Remember about CFATS

---

## 1. **Regulatory**

- ❖ This is not optional
- ❖ Has real penalties (\$25,000/Day + Shut Down)

## 2. **Appendix A lists the Chemicals of Interest (COI's)**

## 3. **Appendix A lists the thresholds**

- ❖ Below = Out
- ❖ Above = In

## 4. **Tiers = 1 – 2 – 3 – 4**

- ❖ Tier 1 is highest risk, Tier 4 is lowest risk

## 5. **Security Vulnerability Assessment**

- ❖ First look at a facility's security program

# 10 Things to Remember about CFATS

---

## 6. **Site Security Plan**

- ❖ Facility tells DHS what its security plans are (now + future).

## 7. **Risk Based Performance Standards (RBPS)**

- ❖ 18 different characteristics of a security plan
- ❖ Level of performance varies based on Tier

## 8. **DHS will be on site to inspect**

- ❖ They will have done their homework.

## 9. **Facilities need to resubmit top screens**

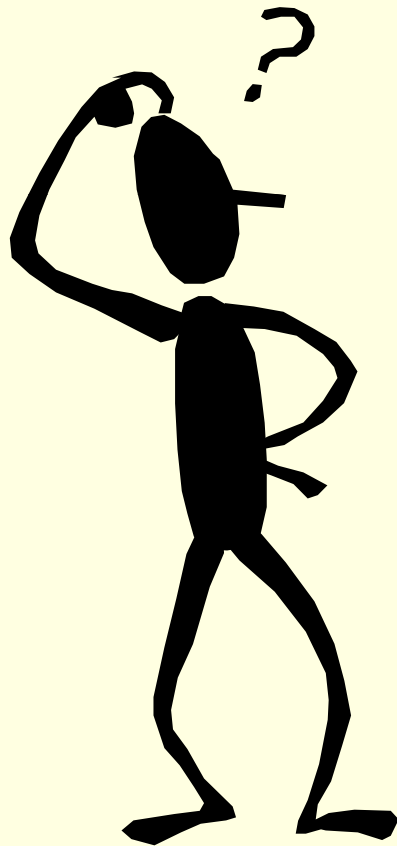
- ❖ Every 2 years for Tier 1 & 2; every 3 years for Tier 3 & 4 and anytime there is a change in the type or quantity of chemicals.

## 10. **Chemical-terrorism Vulnerability Information (CVI)**

- ❖ Provides information security

# Questions?

---



**George T. Miserendino**  
**Triton Security Solutions**  
**[solutions@tritonsecsol.com](mailto:solutions@tritonsecsol.com)**  
**952-423-3457**